МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

Кафедра комп’ютерних систем та мереж

Конспект лекцій

з дисципліни

Захист інформації у комп’ютерних системах

для студентів денної та заочної форми навчання
спеціальності
123 "Комп'ютерна інженерія"

Тернопіль -2019

Конспект лекцій з дисципліни «Захист інформації у комп’ютерних системах» розроблені у відповідності з навчальним планом за спеціальністю 123 “Комп’ютерна інженерія”

УКЛАДАЧ: ст. викл. каф. КС Жаровський Р.О.

Конспект лекцій розглянуто і затверджено на засіданні кафедри комп’ютерних систем та мереж, протокол №7 від 07.02.2019 року.

Зміст

Лекція 1. ОСНОВНІ ПОНЯТТЯ І АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Нові ІТ активно впроваджуються в усі сфери народного господарства. Поява локальних і глобальних мереж передачі даних надала користувачам комп'ютерів нові можливості для оперативного обміну інформацією. Розвиток Internet привів до використання глобальних мереж передачі даних в повсякденному житті практично кожної людини. У міру розвитку і ускладнення засобів, методів і форм автоматизації процесів обробки інформації підвищується залежність суспільства від міри безпеки використовуваних їм ІТ.

1.1. Основні поняття захисту інформації і інформаційної безпеки

Сучасні методи обробки, передачі і накопичення інформації сприяли появі загроз, пов'язаних з можливістю втрати, спотворення і розкриття даних, що адресованих або належать кінцевим користувачам. Тому забезпечення інформаційної безпеки комп'ютерних систем і мереж є одним з провідних напрямів розвитку ІТ.

Розглянемо основні поняття захисту інформації і інформаційної безпеки комп'ютерних систем і мереж.

Захист інформації — це діяльність по запобіганню просочуванню інформації, що захищається, несанкціонованих і неумисних дій на інформацію, що захищається.

Об'єкт захисту — інформація, носій інформації або інформаційний процес, відносно яких необхідно забезпечувати захист відповідно до поставленої мети захисту інформації.

Мета захисту інформації — це бажаний результат захисту інформації. Метою захисту інформації може бути запобігання збитку власникові, власникові, користувачеві інформації в результаті можливого просочування інформації і/або несанкціонованої і неумисної дії на інформацію.

Ефективність захисту інформації — міра відповідності результатів захисту інформації поставленої мети.

Захист інформації від витоку — діяльність по запобіганню неконтрольованому поширенню інформації, що захищається, від її розголошування, несанкціонованого доступу (НСД) до інформації, що захищається, і отримання інформації, що захищається, зловмисниками.

Захист інформації від розголошування — діяльність по запобіганню несанкціонованому доведенню інформації, що захищається, до неконтрольованої кількості одержувачів інформації.

Захист інформації від НСД — діяльність по запобіганню отриманню інформації, що захищається, зацікавленим суб'єктом з порушенням встановлених правовими документами або власником або власником інформації прав або правил доступу до інформації, що захищається. Зацікавленим суб'єктом, що здійснює НСД до інформації, що захищається, може виступати держава, юридична особа, група фізичних осіб, в т. ч. громадська організація, окрема фізична особа.

Система захисту інформації — сукупність органів і/або виконавців, використовувана ними техніка захисту інформації, а також об'єкти захисту,

організовані і функціонуючі за правилами, встановленими відповідними правовими, організаційно-розпорядчими і нормативними документами по захисту інформації.

Під інформаційною безпекою розуміють захищеність інформації від незаконного ознайомлення, перетворення і знищення, а також захищеність інформаційних ресурсів від дій, спрямованих на порушення їх працездатності. Природа цих дій може бути найрізноманітнішою.

Це і спроби проникнення зловмисників, і помилки персоналу, і вихід з ладу апаратних і програмних засобів, і стихійні лиха(землетрус, ураган, пожежа) і т. п.

Сучасна автоматизована система (АС) обробки інформації є складною системою, що складається з великого числа компонентів різної міри автономності, які пов'язані між собою і обмінюються даними. Практично кожен компонент може піддатися зовнішній дії або вийти з ладу. Компоненти АС можна розбити на наступні групи:

- апаратні засоби — комп'ютери і їх складові частини(процесори, монітори, термінали, периферійні пристрої — дисководи, принтери, контроллери, кабелі, лінії зв'язку і т. д.);
- програмне забезпечення — придбані програми, початкові, об'єктні, завантажувальні модулі; ОС і системні програми(компілятори, компонувальники та ін.), утиліти, діагностичні програми і т. д.;
- дані — що зберігаються тимчасово і постійно, на магнітних носіях, друкарські, архіви, системні журнали і т. д.;
- персонал — обслуговуючий персонал і користувачі.

Одній з особливостей забезпечення інформаційної безпеки в АС являється те, що таким абстрактним поняттям, як інформація, об'єкти і суб'єкти системи, відповідають фізичні представлення в комп'ютерному середовищі:

- для представлення інформації — машинні носії інформації у вигляді зовнішніх облаштувань комп'ютерних систем (терміналів, друкуючих пристроїв, різних накопичувачів, ліній і каналів зв'язку), оперативної пам'яті, файлів, записів і т. д.;
- об'єктам системи — пасивні компоненти системи, що зберігають, приймають або передавальні інформацію. Доступ до об'єкту означає доступ до інформації, що міститься в нім;
- суб'єктам системи — активні компоненти системи, які можуть стати причиною потоку інформації від об'єкту до суб'єкта або зміни стану системи. Суб'єктами можуть виступати користувачі, активні програми і процеси.

Інформаційна безпека комп'ютерних систем досягається забезпеченням конфіденційності, цілісності і достовірності оброблюваних даних, а також доступності і цілісності інформаційних компонентів і ресурсів системи. Перелічені вище базові властивості інформації потребують повнішого тлумачення.

Конфіденційність даних — це статус, наданий даним і що визначає необхідну міру їх захисту. До конфіденційних даних можна віднести, наприклад, наступні: особисту інформацію користувачів; облікові записи(імена і паролі); дані про кредитні карти; дані про розробки і різні внутрішні документи; бухгалтерські відомості. Конфіденційна інформація має бути відома тільки допущеним суб'єктам системи(користувачам, процесам, програмам), що пройшли перевірку (авторизованим). Для інших суб'єктів системи ця інформація має бути невідомою.

Встановлення градацій важливості захисту інформації (об'єкту захисту), що захищається, називають категоруванням інформації, що захищається.

Під цілісністю інформації розуміється властивість інформації зберігати свою структуру і/або зміст в процесі передачі і зберігання. Цілісність інформації забезпечується у тому випадку, якщо дані в системі не відрізняються в семантичному відношенні від даних в початкових документах, т. е. якщо не сталося їх випадкового або умисного спотворення або руйнування. Забезпечення цілісності даних є одним із складних завдань захисту інформації.

Достовірність інформації — властивість інформації, що виражається в строгій приналежності суб'єктові, який є її джерелом, або тому суб'єктові, від якого ця інформація прийнята.

Юридична значущість інформації означає, що документ, що є носієм інформації, має юридичну силу.

Доступність даних. Робота користувача з даними можлива тільки у тому випадку, якщо він має до них доступ.

Доступ до інформації — отримання суб'єктом можливості ознайомлення з інформацією, у тому числі за допомогою технічних засобів. Суб'єкт доступу до інформації — учасник правовідносин в інформаційних процесах.

Оперативність доступу до інформації — це здатність інформації або деякого інформаційного ресурсу бути доступною для кінцевого користувача відповідно до його оперативних потреб.

Власник інформації — суб'єкт, в повному об'ємі що реалізовує повноваження володіння, користування, розпорядження інформацією відповідно до законодавчих актів.

Власник інформації — суб'єкт, що здійснює володіння і користування інформацією і що реалізовує повноваження розпорядження в межах прав, встановлених законом і/або власником інформації.

Користувач(споживач) інформації — суб'єкт, що користується інформацією, отриманою від її власника, власника або посередника відповідно до встановлених прав і правил доступу до інформації або з їх порушенням.

Право доступу до інформації — сукупність правил доступу до інформації, встановлених правовими документами або власником або власником інформації.

Правило доступу до інформації — сукупність правил, що регламентують порядок і умови доступу суб'єкта до інформації і її носіїв.

Розрізняють санкціонований і несанкціонований доступ до інформації.

Санкціонований доступ до інформації — це доступ до інформації, що не порушує встановлені правила розмежування доступу. Правила розмежування доступу служать для регламентації права доступу до компонент системи.

Несанкціонований доступ до інформації — порушення встановлених правил розмежування доступу. Обличчя або процес, здійснюючі НСД, до інформації є порушниками правил розмежування доступу. НСД є найбільш поширеним видом комп'ютерних порушень.

Відповідальним за захист комп'ютерної системи від НСД до інформації являється адміністратор захисту.

Доступність інформації має на увазі також доступність компонента або ресурсу комп'ютерної системи, т. е. властивість компонента або ресурсу бути доступним для законних суб'єктів системи. Зразковий перелік ресурсів, які можуть

бути доступні, включає: принтери, сервери, робочі станції, дані користувачів, будь-які критичні дані, необхідні для роботи.

Цілісність ресурсу або компонента системи — ця властивість ресурсу або компонента бути незмінною в семантичному сенсі при функціонуванні системи в умовах випадкових або умисних спотворень або руйнівних дій.

З допуском до інформації і ресурсів системи пов'язана група таких важливих понять, як ідентифікація, аутентифікація, авторизація. З кожним суб'єктом системи(мережі) зв'язують деяку інформацію(число, рядок символів), що ідентифікує суб'єкт. Ця інформація є ідентифікатором суб'єкта системи(мережі). Суб'єкт, що має зареєстрований ідентифікатор, є законним(легальним) суб'єктом. Ідентифікація суб'єкта — це процедура розпізнавання суб'єкта по його ідентифікатору. Ідентифікація виконується при спробі суб'єкта увійти до системи(мережа). Наступним кроком взаємодії системи з суб'єктом є аутентифікація суб'єкта. Аутентифікація суб'єкта — це перевірка достовірності суб'єкта з цим ідентифікатором. Процедура аутентифікації встановлює, чи являється суб'єкт саме тим, ким він себе оголосив. Після ідентифікації і аутентифікації суб'єкта виконують процедуру авторизації. Авторизація суб'єкта — це процедура надання законному суб'єктові, що успішно пройшов ідентифікацію і аутентифікацію, відповідних повноважень і доступних ресурсів системи(мережі).

Під загрозою безпеки АС розуміються можливі дії, здатні прямо або побічно завдати збитку її безпеки. Збиток безпеки має на увазі порушення стану захищеності інформації, що міститься і обробляється в системі(мережі). З поняттям загрози безпеки тісно пов'язано поняття уразливості комп'ютерної системи(мережі). Уразливість комп'ютерної системи — ця властива системі невдала властивість, яка може привести до реалізації загрози. Атака на комп'ютерну систему — це пошук і/або використання зловмисником тієї або іншої уразливості системи. Іншими словами, атака — це реалізація загрози безпеки.

Протидія загрозам безпеки є метою засобів захисту комп'ютерних систем і мереж.

Захищена система — це система із засобами захисту, які успішно і ефективно протистоять загрозам безпеки.

Спосіб захисту інформації — порядок і правила застосування певних принципів і засобів захисту інформації.

Засіб захисту інформації — технічний, програмний засіб, речовина і/або матеріал, призначені або використовувані для захисту інформації

Комплекс засобів захисту(КСЗ) — сукупність програмних і технічних засобів, що створюються і підтримуваних для забезпечення інформаційної безпеки системи(мережі). КСЗ створюється і підтримується відповідно до прийнятої в цій організації політики безпеки.

Техніка захисту інформації — засоби захисту інформації, засобу контролю ефективності захисту інформації, засобу і системи управління, призначені для забезпечення захисту інформації.

Корпоративні мережі відносяться до розподілених автоматизованих систем(АС), що здійснюють обробку інформації. Забезпечення безпеки АС припускає організацію протидії будь-якому несанкціонованому вторгненню в процес функціонування АС, а також спробам модифікації, розкрадання, виведення з ладу або руйнування її компонентів, т. е. захист усіх компонентів АС — апаратних

засобів, програмного забезпечення(ПЗ), даних і персоналу. Конкретний підхід до проблеми забезпечення безпеки заснований на розробленій для АС політиці безпеки [30, 63].

Політика безпеки — це сукупність норм, правил і практичних рекомендацій, що регламентують роботу засобів захисту комп'ютерної системи від заданої безлічі загроз. Детальніші відомості про види політики безпеки і процес її розробки наводяться в л. 3.

1.2. Аналіз загроз інформаційної безпеки

Під загрозою(у загальному сенсі) зазвичай розуміють потенційно можливу подію(дія, процес або явище), яка може привести до нанесення збитку чиїм-небудь інтересам. Надалі під загрозою безпеки АС обробки інформації розумітимемо можливість дії на АС, яке пряме або побічно може завдати збитку її безпеки.

Нині відомий великий перелік загроз інформаційної безпеки АС, що містить сотні позицій.

Розгляд можливих загроз інформаційної безпеки проводиться з метою визначення повного набору вимог до системи, що розробляється, зашиті.

Перелік загроз, оцінки вірогідності їх реалізації, а також модель порушника служать основою для аналізу ризику реалізації загроз і формулювання вимог до системи захисту АС. Окрім виявлення можливих загроз, доцільне проведення аналізу цих загроз на основі їх класифікації за рядом ознак. Кожна з ознак класифікації відбиває одну з узагальнених вимог до системи захисту. Загрози, що відповідають кожній ознаці класифікації, дозволяють деталізувати відбиване цією ознакою вимога.

Необхідність класифікації загроз інформаційної безпеки АС обумовлена тим, що інформація, що зберігається і оброблювана, в сучасних АС схильна до дії надзвичайно великого числа чинників, в силу чого стає неможливим формалізувати завдання опису повної безлічі загроз. Тому для системи, що захищається, зазвичай визначають не повний перелік загроз, а перелік класів загроз.

Класифікація можливих загроз інформаційної безпеки АС може бути проведений за наступними базовими ознаками [63].

1. За природою виникнення:
   - природні загрози, викликані діями на АС об'єктивних фізичних процесів або стихійних природних явищ;
   - штучні загрози безпеки АС, викликані діяльністю людини.
2. По мірі навмисності прояву:
   - загрози, викликані помилками або халатністю персоналу, наприклад некомпетентне використання засобів захисту, введення помилкових даних і т. п.;
   - загрози умисної дії, наприклад дії зловмисників.
3. По безпосередньому джерелу загроз:
   - природне середовище, наприклад стихійні лиха, магнітні бурі і ін.;
   - людина, наприклад вербування шляхом підкупу персоналу, розголошування конфіденційних даних і т. п.;
   - санкціоновані програмно-апаратні засоби, наприклад видалення даних, відмова в роботі ОС;

• несанкціоновані програмно-апаратні засоби, наприклад зараження комп'ютера вірусами з деструктивними функціями.

4. По положенню джерела загроз:

• поза контрольованою зоною АС, наприклад перехоплення даних, що передаються по каналах зв'язку, перехоплення побічних електромагнітних, акустичних і інших випромінювань пристроїв;

• в межах контрольованої зони АС, наприклад застосування підслуховуючих пристроїв, розкрадання записів, носіїв інформації і т. п.;

• безпосередньо у АС, наприклад некоректне використання ресурсів АС.

5. По мірі залежності від активності АС:

• незалежно від активності АС, наприклад розкриття шифрів криптозахисту інформації;

• тільки в процесі обробки даних, наприклад загрози виконання і поширення програмних вірусів.

6. По мірі дії на АС:

• пасивні загрози, які при реалізації нічого не міняють в структурі і змісті АС, наприклад загроза копіювання секретних даних;

• активні загрози, які при дії вносять зміни в структуру і зміст АС, наприклад впровадження троянських коней і вірусів.

7. По етапах доступу користувачів або програм до ресурсів АС:

• загрози, що проявляються на етапі доступу до ресурсів АС, наприклад загрози несанкціонованого доступу в АС;

• загрози, що проявляються після дозволу доступу до ресурсів АС, наприклад загрози несанкціонованого або некоректного використання ресурсів АС.

8. За способом доступу до ресурсів АС:

• загрози, здійснювані з використанням стандартного шляху доступу до ресурсів АС, наприклад незаконне отримання паролів і інших реквізитів розмежування доступу з подальшим маскуванням під зареєстрованого користувача;

• загрози, здійснювані з використанням прихованого нестандартного шляху доступу до ресурсів АС, наприклад несанкціонований доступ до ресурсів АС шляхом використання недокументованих можливостей ОС.

9. За поточним місцем розташування інформації, що зберігається і оброблюваної в АС:

• загрози доступу до інформації, що знаходиться на зовнішніх пристроях, що запам'ятовують, наприклад несанкціоноване копіювання секретної інформації з жорсткого диска;

• загрози доступу до інформації, що знаходиться в оперативній пам'яті, наприклад читання залишкової інформації з оперативної пам'яті, доступ до системної області оперативної пам'яті з боку застосовних програм;

• загрози доступу до інформації, циркулюючої в лініях зв'язку, наприклад незаконне підключення до ліній зв'язку з подальшим введенням неправдивих повідомлень або модифікацією передаваних повідомлень, незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача з подальшим введенням дизінформації і нав'язуванням неправдивих повідомлень;

- загрози доступу до інформації, що відображається на терміналі або друкованій на принтері, наприклад запис інформації, що відображається, на приховану відеокамеру.

Як вже відзначалося, небезпечні дії на АС підрозділяють на випадкові і умисні. Аналіз досвіду проектування, виготовлення і експлуатації АС показує, що інформація піддається різним випадковим діям на усіх етапах циклу життя і функціонування АС.

Причинами випадкових дій при експлуатації АС можуть бути:

- аварійні ситуації із-за стихійних лих і відключень електроживлення;
- відмови і збої апаратури;
- помилки в програмному забезпеченні;
- помилки в роботі обслуговуючого персоналу і користувачів;
- перешкоди в лініях зв'язку із-за дій зовнішнього середовища.

Помилки в ПЗ є поширеним видом комп'ютерних порушень. ПЗ серверів, робочих станцій, маршрутизаторів і т. д. написано людьми, тому воно практично завжди містить помилки. Чим вище складність подібного ПЗ, тим більше вірогідності виявлення в нім помилок і вразливостей. Більшість з них не представляють ніякій небезпеці, деякі ж можуть привести до серйозних наслідків, таким як отримання зловмисником контролю над сервером, непрацездатність сервера, несанкціоноване використання ресурсів(використання комп'ютера як плацдарму для атаки і т. п.). Зазвичай подібні помилки усуваються за допомогою пакетів оновлень, що регулярно випускаються виробником ПЗ. Своєчасна установка таких пакетів є необхідною умовою безпеки інформації.

Умисні загрози пов'язані з цілеспрямованими діями порушника. В якості порушника може бути службовець, відвідувач, конкурент, найманець і т. д. Дії порушника можуть бути обумовлені різними мотивами: невдоволенням службовця своєю кар'єрою, суто матеріальним інтересом(хабар), цікавістю, конкурентною боротьбою, прагненням самоствердитися за всяку ціну і т. п.

Виходячи з можливості виникнення найбільш небезпечної ситуації, обумовленої діями порушника, можна скласти гіпотетичну модель потенційного порушника [40]:

- кваліфікація порушника може бути на рівні розробника цієї системи;
- порушником може бути як стороння особа, так і законний користувач системи;
- порушникові відома інформація про принципи роботи системи;
- порушник вибере найбільш слабку ланку в захисті.

Зокрема, для банківських АС можна виділити наступні умисні загрози:

- НСД осіб, що не належать до числа банківських службовців, і ознайомлення з конфіденційною інформацією, що зберігається;
- ознайомлення банківських службовців з інформацією, до якої вони не повинні мати доступу;
- несанкціоноване копіювання програм і даних;
- крадіжка магнітних носіїв, що містять конфіденційну інформацію;
- крадіжка роздрукованих банківських документів;
- умисне знищення інформації;
- несанкціонована модифікація банківськими службовцями фінансових документів, звітності і баз даних;

- фальсифікація повідомлень, що передаються по каналах зв'язку;
- відмова від авторства повідомлення, переданого по каналах зв'язку;
- відмова від факту отримання інформації;
- нав'язування раніше переданого повідомлення;
- руйнування інформації, викликане вірусними діями;
- руйнування архівної банківської інформації, що зберігається на магнітних носіях;
- крадіжка устаткування.

Несанкціонований доступ — найбільш поширений і різноманітний вид комп'ютерних порушень. Суть НСД полягає в отриманні користувачем(порушником) доступу до об'єкту порушуючи правила розмежування доступу, встановлені відповідно до прийнятої в організації політики безпеки. НСД використовує будь-яку помилку в системі захисту і можливий при нераціональному виборі засобів захисту, їх некоректній установці і налаштуванні. НСД може бути здійснений як штатними засобами АС, так і спеціально створеними апаратними і програмними засобами.

Основні канали НСД, через які порушник може отримати доступ до компонент АС і здійснити розкрадання, модифікацію і/або руйнування інформації:

- штатні канали доступу до інформації (термінали користувачів, оператора, адміністратора системи; засоби відображення і документування інформації; канали зв'язку) при їх використанні порушниками, а також законними користувачами поза межами їх повноважень;
- технологічні пульти управління;
- лінії зв'язку між апаратними засобами АС;
- побічні електромагнітні випромінювання від апаратури, ліній зв'язку, мереж електроживлення і заземлення та ін.

З усієї різноманітності способів і прийомів НСД зупинимося на наступних поширених і пов'язаних між собою порушеннях:

- перехоплення паролів;
- «маскарад»;
- незаконне використання привілеїв.

Перехоплення паролів здійснюється спеціально розробленими програмами. При спробі законного користувача увійти до системи програма-перехоплювач імітує на екрані дисплея введення імені і пароля користувача, які відразу пересилаються власникові програми-перехоплювача, після чого на екран виводиться повідомлення про помилку і управління повертається ОС.

Користувач припускає, що припустимо помилку при введенні пароля. Він повторює введення і дістає доступ в систему. Власник програми-перехоплювача, що отримав ім'я і пароль законного користувача, може тепер використати їх у своїх цілях. Існують і інші способи перехоплення паролів.

«Маскарад» — це виконання яких-небудь дій одним користувачем від імені іншого користувача, що має відповідні повноваження. Метою «маскараду» є приписування яких-небудь дій іншому користувачеві або привласнення повноважень і привілеїв іншого користувача. Прикладами реалізації «маскараду» є:

- вхід в систему під ім'ям і паролем іншого користувача (цьому «маскараду» передує перехоплення пароля);

- передача повідомлень в мережі від імені іншого користувача.

«Маскарад» особливо небезпечний у банківських системах електронних платежів, де неправильна ідентифікація клієнта із-за «маскараду» зловмисника може привести до великих збитків законного клієнта банку.

Незаконне використання привілеїв. Більшість систем захисту встановлюють певні набори привілеїв для виконання заданих функцій. Кожен користувач отримує свій набір привілеїв: звичайні користувачі — мінімальний, адміністратори — максимальний. Несанкціоноване захоплення привілеїв, наприклад за допомогою «маскараду», призводить до можливості виконання порушником певних дій в обхід системи захисту. Слід зазначити, що незаконне захоплення привілеїв можливе або за наявності помилок в системі захисту, або через халатність адміністратора при управлінні системою і призначенні привілеїв.

Прийнято вважати, що незалежно від конкретних видів загроз або їх проблемно-орієнтованої класифікації АС задовольняє потреби осіб, що експлуатують її, якщо забезпечуються наступні важливі властивості інформації і систем її обробки: конфіденційність, цілісність і доступність.

Іншими словами, відповідно до існуючих підходів вважають, що інформаційна безпека АС забезпечена у разі, якщо для інформаційних ресурсів в системі підтримуються певні рівні:

- конфіденційності (неможливості несанкціонованого отримання якої-небудь інформації);
- цілісності (неможливості несанкціонованої або випадкової її модифікації);
- доступності (можливості за розумний час отримати необхідну інформацію).

Відповідно для АС розглядають три основні види загроз.

Загрози порушення конфіденційності, спрямовані на розголошування конфіденційної або секретної інформації. При реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступу. В термінах комп'ютерної безпеки загроза порушення конфіденційності має місце всякий раз, коли отриманий НСД до деякої закритої інформації, що зберігається в комп'ютерній системі або передається від однієї системи до іншої.

Загрози порушення цілісності інформації, що зберігається в комп'ютерній системі або передається по каналу зв'язку, які спрямовані на її зміну або спотворення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена умисне, а також в результаті об'єктивних дій з боку середовища, що оточує систему. Ця загроза особливо актуальна для систем передачі інформації — комп'ютерних мереж і систем телекомунікацій. Умисні порушення цілісності інформації не слід плутати з її санкціонованою зміною, яка виконується повноважними особами з обґрунтованою метою(такою зміною, наприклад, являється періодична корекція деякої БД).

Загрози порушення працездатності (відмова в обслуговуванні), спрямовані на створення таких ситуацій, коли певні умисні дії або знижують працездатність АС, або блокують доступ до деяких її ресурсів. Наприклад, якщо один користувач системи просить доступ до деякої служби, а інший робить дії з блокування цього доступу, то перший користувач дістає відмову в обслуговуванні. Блокування доступу до ресурсу може бути постійним або тимчасовим.

Ці види загроз можна вважати первинними або безпосередніми, оскільки реалізація цих загроз веде до безпосередньої дії на інформацію, що захищається.

Для сучасних ІТ підсистеми захисту є невід'ємною частиною АС обробки інформації. Атакуюча сторона повинна здолати цю підсистему захисту, щоб порушити, наприклад, конфіденційність АС. Проте треба усвідомлювати, що не існує абсолютно стійкої системи захисту, питання лише в часі і засобах, що вимагаються на її подолання. Виходячи з цих умов, розглянемо наступну модель: захист інформаційної системи вважається здоланим, якщо в ході дослідження цієї системи визначені усе її уразливості.

Подолання захисту також є загрозою, тому для захищених систем можна розглядати четвертий вид загрози — загрозу розкриття параметрів АС, що включає підсистему захисту. На практиці будь-який захід, що проводиться, упереджається етапом розвідки, в ході якого визначаються основні параметри системи, її характеристики і т. п. Результатом цього етапу є уточнення поставленого завдання, а також вибирання найбільш оптимального технічного засобу.

Загрозу розкриття параметрів АС можна вважати опосередкованою загрозою. Наслідки її реалізації не заподіюють який-небудь збиток оброблюваній інформації, але дають можливість реалізувати первинні або безпосередні загрози, перелічені вище.

При розгляді питань захисту АС доцільно використати чотирьохрівневу градацію доступу до тієї, що зберігається, оброблюваній і такій, що захищається АС інформації. Така градація доступу допоможе систематизувати як можливі загрози, так і заходи по їх нейтралізації і парируванню, т. е. допоможе систематизувати увесь спектр методів забезпечення захисту, що відносяться до інформаційної безпеки. Це наступні рівні доступу:

- рівень носіїв інформації;
- рівень засобів взаємодії з носієм;
- рівень представлення інформації;
- рівень змісту інформації.

Введення цих рівнів обумовлене наступними міркуваннями.

По-перше, інформація для зручності маніпулювання найчастіше фіксується на деякому матеріальному носії, яким може бути дискета або що-небудь подібне.

По-друге, якщо спосіб представлення інформації такий, що вона не може бути безпосередньо сприйнята людиною, виникає необхідність в перетворювачах інформації в доступний для людини спосіб представлення. Наприклад, для читання інформації з дискети потрібний комп'ютер, обладнаний дисководом відповідного типу.

По-третє, як вже було відмічено, інформація може бути охарактеризована способом свого представлення: мовою символів, мовою жестів і т. д.

По-четверте, людині має бути доступний сенс представленої інформації, її семантика.

До основних напрямів реалізації зловмисником інформаційних загроз відносяться:

- безпосереднє звернення до об'єктів доступу;
- створення програмних і технічних засобів, що виконують звернення до об'єктів доступу в обхід засобів захисту;

• модифікація засобів захисту, що дозволяє реалізувати загрози інформаційної безпеки;

• впровадження в технічні засоби АС програмних або технічних механізмів, що порушують передбачувану структуру і функції АС.

У таблиці. 1.1 перераховані основні методи реалізації загроз інформаційної безпеки.

Таблиця 1.1. Основні методи реалізації загроз інформаційної безпеки

Рівень доступу до інформації в АС	Загроза розкриття параметрів системи	Загроза порушення конфіденційності	Загроза порушення цілісності	Загроза відмови служб(відмови доступу до інформації)
Рівень носіїв інформації	Визначення типу і параметрів носіїв інформації	Розкрадання (копіювання) носіїв інформації Перехоплення	Знищення машинних носіїв інформації	Виведення з ладу машинних носіїв інформації
Рівень засобів взаємодії з носієм	Отримання інформації про програмно-апаратне середовище Отримання детальної інформації про функції, що виконуються АС Отримання даних про використання системи захисту	Несанкціонований доступ до ресурсів АС Здійснення користувачем несанкціонованих дій Несанкціоноване копіювання програмного забезпечення Перехоплення даних, передаваних по каналах зв'язку	Внесення користувачем несанкціонованих змін в програми і дані Установка і використання нештатного програмного забезпечення Зараження програмними вірусами	Прояв помилок проектування і розробки програмно-апаратних компонентів АС Обхід механізмів захисту АС
Рівень представлення інформації	Визначення способу представлення інформації	Візуальне спостереження Розкриття представлення інформації (дешифрування)	Внесення спотворень в представлення даних; знищення даних	Спотворення відповідності синтаксичних і семантичних конструкцій мови
Рівень змісту інформації	Визначення змісту даних на якісному рівні	Розкриття змісту інформації	Впровадження дезінформації	Заборона на використання інформації

Для досягнення необхідного рівня інформаційної безпеки АС необхідно забезпечити протидію різним технічним загрозам і мінімізувати можливий вплив «людського чинника».

Лекція 2 ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МЕРЕЖ

Основною властивістю, що відрізняє комп'ютерні мережі від автономних комп'ютерів, є наявність обміну інформацією між мережевими вузлами, пов'язаними лініями передачі даних.

Об'єднання комп'ютерів в комп'ютерні мережі дозволяє значно підвищити ефективність використання комп'ютерної системи в цілому. Підвищення ефективності при цьому досягається за рахунок можливості обміну інформацією між комп'ютерами мережі, а також за рахунок можливості використання на кожному комп'ютері загальних мережевих ресурсів (інформації, зовнішньої пам'яті, програмних застосувань, зовнішніх пристроїв).

Однією з основних ознак корпоративної мережі є застосування глобальних зв'язків для об'єднання окремих локальних мереж філій підприємства і комп'ютерів його видалених співробітників з центральною локальною мережею. Останніми роками інтенсивно розвиваються безпровідні комп'ютерні мережі, і зокрема безпровідні локальні мережі WLAN (Wireless Local Area Network).

2.1. Введення в мережевий інформаційний обмін

Стрімкий розвиток ИТ привів до появи і швидкого зростання глобальної мережі Internet. Розвиток комп'ютерних мереж немислимий без суворого дотримання принципів стандартизації апаратного і ПЗ. Днем народження Інтернету в сучасному розумінні цього слова стала дата стандартизації в 1983 р. стека

комунікаційних протоколів TCP/IP, що лежить в основі Всесвітньої мережі Інтернет. Інтернет є сукупністю сполучених між собою комп'ютерних мереж, в яких використовуються єдині погоджені правила обміну даними між комп'ютерами.

2.1.1. Використання мережі Інтернет

Розвиток глобальної мережі Internet сприяв використанню для побудови глобальних корпоративних зв'язків дешевшого і доступнішого (в порівнянні з виділеними каналами) транспорту Internet. Мережа Internet пропонує різноманітні методи комунікації і способи доступу до інформації, тому для багатьох компаній вона стала невід'ємною частиною їх ІС.

Вплив Internet на корпоративні мережі сприяв появі нового поняття — intranet (інтранет, інтрамережі), при якому способи доставки і обробки інформації, властиві Internet, переносяться в корпоративну мережу.

Відмітимо основні можливості, що надаються мережею Internet для побудови корпоративних мереж [5, 9].

Дешеві і доступні комунікаційні канали Internet. На початок XXI ст. у зв'язку з бурхливим розвитком Internet і мереж колективного доступу у світі стався якісний стрибок в поширенні і доступності інформації. Користувачі отримали дешеві і доступні комунікаційні канали Internet. Прагнучи до економії коштів, підприємства стали активно використовувати ці канали для передачі критичної комерційної і управлінської інформації.

Універсальність. Глобальна мережа Internet була створена для забезпечення обміну інформацією між видаленими користувачами. Розвиток Internet- технологій

привів до виникнення популярної глобальної служби World Wide Web (WWW), що дозволило користувачам працювати з інформацією в режимі прямого підключення. Ця технологія має на увазі підключення користувача до глобальної мережі і використання WWW- браузерів для перегляду інформації. Стандартизація інтерфейсів обміну даними між утилітами перегляду інформації і інформаційними серверами дозволила організувати однаковий інтерфейс з користувачем для різних платформ.

Доступ до різноманітної інформації і послуга Internet. Окрім транспортних послуг з транзитної передачі даних для абонентів будь-яких типів, мережу Інтернет забезпечує також досить широкий набір високорівневих Інтернет-сервісів:

- всесвітня павутина World Wide Web;
- сервіс імен доменів DNS;
- доступ до файлових архівів FTP;
- електронна пошта (e — mail);
- телеконференції (Usenet);
- сервіси спілкування ICQ, IRC;
- сервіс Telnet;
- пошук інформації в Інтернеті.

Комп'ютери, що надають ці послуги, називаються серверами, відповідно комп'ютери, що користуються послугами, називаються клієнтами. Ці ж терміни відносяться і до ПЗ, використовуваному на комп'ютерах-серверах і комп'ютерах-клієнтах. Мережа Internet забезпечує доступ до великої і різноманітної інформації за допомогою величезного числа підключених до неї хост-вузлів.

Хост — це комп'ютер або група комп'ютерів, що мають пряме мережеве з'єднання з Internet і надають користувачам доступ до своїх засобів і служб. Багато хто з цих комп'ютерів виконує роль серверів, що пропонують будь-якому користувачеві, що має вихід в Internet, доступ до електронних ресурсів — даних, застосувань і послуг. Зв'язавши свої мережі із зовнішніми ресурсами, компанії можуть реалізувати постійні комунікації і організувати ефективний потік інформації між людьми. З'єднання внутрішніх мереж із зовнішніми організаціями і ресурсами дозволяє компаніям скористатися перевагами цих мереж — зниженням витрат і підвищенням ефективності.

Простота використання. При використанні Інтернет-технологій не потрібно спеціальне навчання персоналу.

Для об'єднання локальних мереж в глобальні використовуються спеціалізовані комп'ютери (маршрутизатори і шлюзи), за допомогою яких локальні мережі підключаються до міжмережевих каналів зв'язку. Маршрутизатори і шлюзи фізично сполучають локальні мережі один з одним і, використовуючи спеціальне ПЗ, передають дані з однієї мережі в іншу. Глобальні мережі мають складну розгалужену структуру і надмірні зв'язки. Маршрутизатори і шлюзи забезпечують пошук оптимального маршруту при передачі даних в глобальних мережах, завдяки чому досягається максимальна швидкість потоку повідомлень. Високошвидкісні канали зв'язку між локальними мережами можуть бути реалізовані на основі волоконно-оптичних кабелів або за допомогою супутникового зв'язку. Як повільні міжмережеві канали зв'язку використовуються різні види телефонних ліній.

Побудова корпоративних комп'ютерних мереж із застосуванням технології інтрамереж означає передусім використання стека TCP/IP для транспортування даних і технології Web для їх представлення.

2.1.2. Модель ISO/OSI і стек протоколів TCP/IP

Основне завдання, що вирішується при створенні комп'ютерних мереж, — забезпечення сумісності устаткування за електричними і механічними характеристиками і сумісністю інформаційного забезпечення (програм і даних) по системах кодування і форматі даних. Рішення цієї задачі відноситься до області стандартизації. Методологічною основою стандартизації в комп'ютерних мережах є багаторівневий підхід до розробки засобів мережевої взаємодії. На основі цього підходу і технічних пропозицій Міжнародної організації стандартів ISO (International Standards Organization) на початку 1980-х рр. була розроблена стандартна модель взаємодії відкритих систем OSI (Open Systems Interconnection). Модель ISO/OSI зіграла важливу роль в розвитку комп'ютерних мереж.

Модель OSI визначає різні рівні взаємодії систем і вказує, які функції повинен виконувати кожен рівень. У моделі OSI засобу взаємодії діляться на сім рівнів:

1. прикладного (Application),
2. представницького (Presentation),
3. сеансового (Session),
4. транспортного (Transport),
5. мережевого (Network),
6. канального (Data Link),
7. фізичного (Physical).

Самий верхній рівень — прикладний. На цьому рівні користувач взаємодіє із застосуваннями. Самий нижній рівень — фізичний. Цей рівень забезпечує обмін сигналами між пристроями.

Обмін даними через канали зв'язку відбувається шляхом переміщення даних з верхнього рівня на нижній, потім транспортування по лініях зв'язку і, нарешті, зворотним відтворенням даних в комп'ютері клієнта в результаті їх переміщення з нижнього рівня на верхній.

Для забезпечення необхідної сумісності на кожному з рівнів архітектури комп'ютерної мережі діють спеціальні стандартні протоколи. Вони є формалізованими правилами, що визначають послідовність і формат повідомлень, якими обмінюються мережеві компоненти, що лежать на одному рівні, але в різних вузлах мережі.

Ієрархічно організований набір протоколів, достатній для організації взаємодії вузлів в мережі, називається стеком комунікаційних протоколів. Слід чітко розрізняти модель ISO/OSI і стек протоколів ISO/OSI. Модель ISO/OSI є концептуальною схемою взаємодії відкритих систем, а стек протоколів ISO/OSI є набором цілком конкретних специфікацій протоколів для семи рівнів взаємодії, які визначені в моделі ISO/OSI.

Комунікаційні протоколи можуть бути реалізовані як програмно, так і апаратно. Протоколи нижніх рівнів часто реалізуються комбінацією програмних і

апаратних засобів, а протоколи верхніх рівнів — як правило, чисто програмними засобами.

Модулі, що реалізовують протоколи сусідніх рівнів і мережі, що знаходяться в одному вузлі, повинні взаємодіяти один з одним також відповідно до чітко певних правил і за допомогою стандартизованих форматів повідомлень. Ці правила прийнято називати міжрівневим інтерфейсом. Міжрівневий інтерфейс визначає набір сервісів, що надаються цим рівнем сусідньому рівню. По суті, протокол і інтерфейс є близькими поняттями, але традиційно в мережах за ними закріплені різні зони дії: протоколи визначають правила взаємодії модулів одного рівня в різних вузлах мережі, а інтерфейси визначають правила взаємодії модулів сусідніх рівнів в одному вузлі.

Стек протоколів TCP/IP (Transmission Control Protocol/ Internet Protocol) є промисловим стандартом стека комунікаційних протоколів, розробленим для глобальних мереж. Стандарти TCP/IP опубліковані в серії документів, названих Request for Comment (RFC). Документи RFC описують внутрішню роботу мережі Internet. Деякі RFC описують мережеві сервіси або протоколи і їх реалізацію, тоді як інші узагальнюють умови застосування.

Стек TCP/IP об'єднує набір протоколів, що взаємодіють між собою. Найважливішими з них є протокол IP, що відповідає за пошук маршруту (чи маршрутів) в Інтернеті від одного комп'ютера до іншого через безліч проміжних мереж, шлюзів і маршрутизаторів і передачу блоків даних по цих маршрутах, і протокол TCP, що забезпечує надійну доставку, безпомилковість і правильний порядок прийому передаваних даних.

Великий внесок у розвиток стека TCP/IP вніс Каліфорнійський університет у Берклі (США), який реалізував протоколи стека у своїй версії ОС UNIX, зробивши як самі програми, так і їх початкові тексти безкоштовними і загальнодоступними. Популярність цієї ОС привела до широкого поширення протоколів IP, TCP і інших протоколів стека. Сьогодні цей стек використовується для зв'язку комп'ютерів всесвітньої інформаційної мережі Internet, а також у величезному числі корпоративних мереж. Стек TCP/IP є найпоширенішим засобом організації складених комп'ютерних мереж.

Широке поширення стека TCP/IP пояснюється наступним:

- це найбільш завершений стандартний і в той же час популярний стек мережевих протоколів, що має багаторічну історію;
- майже все більші мережі передають основну частину свого трафіку за допомогою протоколу TCP/IP;
- усі сучасні ОС підтримують стек TCP/IP.

Крім того, це:

- метод діставання доступу до мережі Internet;
- гнучка технологія для з'єднання різнорідних систем як на рівні транспортних підсистем, так і на рівні прикладних сервісів;
- основа для створення intranet — корпоративної мережі, що використовує транспортні послуги Internet і гіпертекстову технологію WWW, розроблену в Internet;
- стійке масштабоване міжплатформене середовище для застосувань клієнт-сервер [46].

Структура і функціональність стека протоколів TCP/IP

Стек TCP/IP був розроблений до появи моделі взаємодії відкритих систем OSI і також має багаторівневу структуру. Структура протоколів TCP/IP приведена на Рис. 2.1.

Стек протоколів TCP/IP має чотири рівні —

1. прикладний (Application),
2. транспортний (Transport),
3. рівень міжмережевої взаємодії (Internet)
4. рівень мережевих інтерфейсів (Network).

Для порівняння на Рис. 2.1 показані також сім рівнів моделі OSI. Слід зазначити, що відповідність рівнів стека TCP/IP рівням моделі OSI досить умовно.

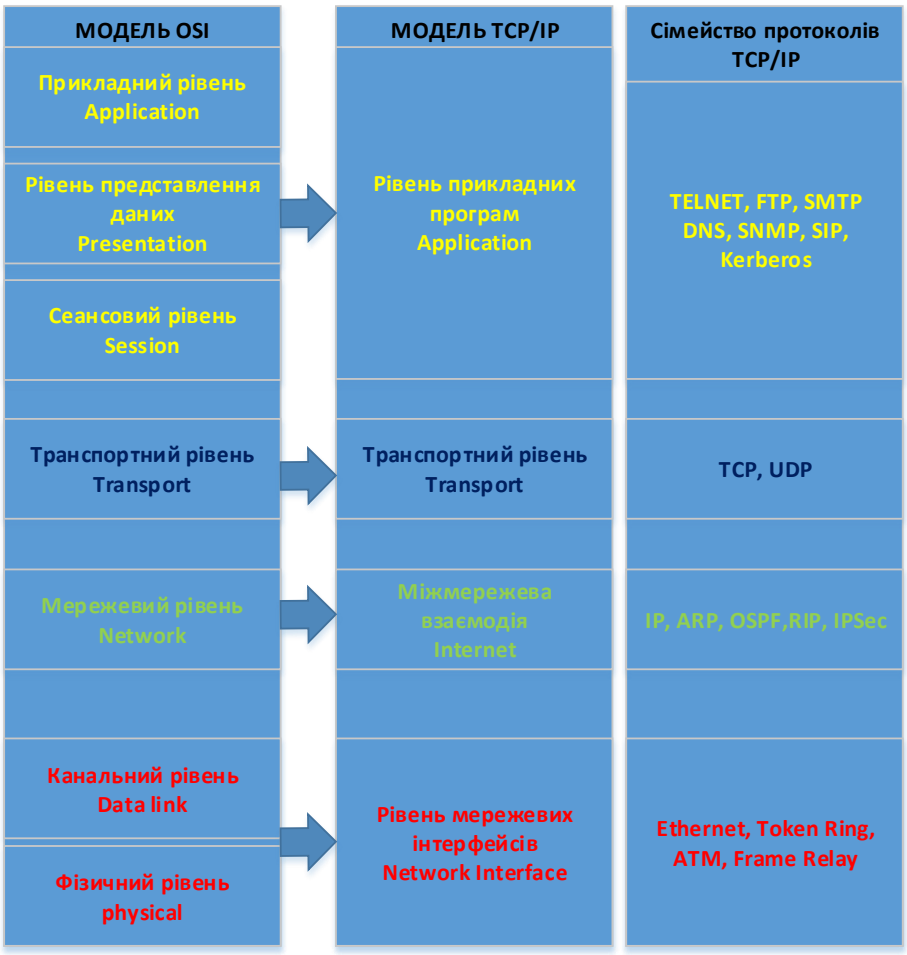

Рис. 2.1. Рівні стека протоколів TCP/IP

Прикладний рівень (Application) включає велике число прикладних протоколів і сервісів. До них відносяться такі популярні протоколи, як протокол копіювання файлів FTP, протокол емуляції терміналу Telnet, поштовий протокол SMPT, використовуваний в електронній пошті мережі Internet, гіпертекстові сервіси доступу до видаленої інформації, такі як WWW, і багато інших. Розглянемо детальніше деякі з цих протоколів [46].

Протокол пересилки файлів FTP (File Transfer Protocol) реалізує видалений доступ до файлу. Для того, щоб забезпечити надійну передачу, FTP використовує як транспорт протокол зі встановленням з'єднань — TCP. Окрім пересилки файлів, протокол FTP пропонує і інші послуги. Наприклад, користувачеві надається можливість інтерактивної роботи з видаленою машиною, зокрема, він може

роздрукувати вміст її каталогів. Нарешті, FTP виконує аутентифікацію користувачів. Перш ніж отримати доступ до файлу, відповідно до протоколу користувачі повинні повідомити своє ім'я і пароль. Для доступу до публічних каталогів FTP— архівом.

Internet не потрібно парольна аутентифікація, і її можна обійти шляхом використання для такого доступу зумовленого імені користувача Anonymous.

Протокол Telnet забезпечує передачу потоку байтів між процесами, а також між процесом і терміналом. Найчастіше цей протокол використовується для емуляції терміналу видаленого комп'ютера. При використанні сервісу Telnet користувач фактично управляє видаленим комп'ютером так само, як і локальний користувач, тому такий вид доступу вимагає хорошого захисту. Сервери Telnet завжди використовують, як мінімум, аутентифікацію по паролю, а іноді і потужніші засоби захисту, наприклад систему Kerberos.

Протокол SNMP (Simple Network Management Protocol) використовується для організації мережевого управління. Спочатку протокол SNMP був розроблений для видаленого контролю і управління маршрутизаторами Internet. Із зростанням популярності протокол SNMP стали застосовувати для управління різним комунікаційним устаткуванням — концентраторами, мостами, мережевими адаптерами та ін. В стандарті SNMP визначена специфікація інформаційної бази даних управління мережею. Ця специфікація, відома як база даних MIB (Management Information Base), визначає ті елементи даних, які керований пристрій повинен зберігати, і допустимі операції над ними.

На транспортному рівні (Transport) стека TCP/IP, що називається також основним рівнем, функціонують протокол TCP і протокол UDP.

Протокол управління передачею TCP (Transport Control Protocol) вирішує задачу забезпечення надійного інформаційного зв'язку між двома кінцевими вузлами. Цей протокол називають протоколом «зі встановленням з'єднання». Це означає, що два вузли, що зв'язуються за допомогою цього протоколу, «домовляються» про те, що вони обмінюватимуться потоком даних і приймають деякі угоди про управління цим потоком. Згідно з протоколом TCP, дані «нарізаються», що відправляються, на невеликі стандартні пакети, після чого кожен пакет маркірується так, щоб в нім були дані для правильного складання документу на комп'ютері одержувача.

Протокол дейтаграм користувача UDP (User Datagram Protocol) забезпечує передачу прикладних пакетів дейтаграмним способом, т. е. кожен блок передаваної інформації (пакет) обробляється і поширюється від вузла до вузла

як незалежна одиниця інформації — дейтаграма. При цьому протокол UDP виконує тільки функції сполучної ланки між мережевим протоколом і численними прикладними процесами. Необхідність в протоколі UDP обумовлена тим, що UDP «уміє» розрізняти застосування і доставляє інформацію від додатка до застосування.

Рівень міжмережевої взаємодії (Internet) реалізує концепцію комутації пакетів без встановлення з'єднань. Основним протоколом цього рівня є адресний протокол IP. Цей протокол спочатку проектувався як протокол передачі пакетів в складених мережах, що складаються з великого числа локальних мереж, об'єднаних як локальними, так і глобальними зв'язками.

Суть протоколу IP полягає в тому, що у кожного користувача Всесвітньої мережі Internet має бути своя унікальна адреса (IP— адреса). Без цього не можна говорити про точну доставку TCP-пакетів в потрібне робоче місце. Ця адреса виражається дуже просто — чотирма байтами, наприклад: 185.47.39.14. Структура IP— адреси організована таким чином, що кожен комп'ютер, через який проходить який-небудь TCP— пакет, може по цих чотирьох числах визначити, кому з найближчих «сусідів» потрібно переслати пакет, щоб він виявився «ближчий» до одержувача. В результаті кінцевого числа перекидань TCP— пакет досягає адресата. В даному випадку оцінюється не географічна «близькість». Враховуються умови зв'язку і пропускна спроможність лінії. Два комп'ютери, що знаходяться на різних континентах, але пов'язані високопродуктивною лінією космічного зв'язку, вважаються ближчими один одному, ніж два комп'ютери з сусідніх міст, пов'язаних звичайним телефонним зв'язком. Вирішенням питань, що вважати «ближче», а що «далі» займаються спеціальні засоби — маршрутизатори. Роль маршрутизатора в мережі може виконувати як спеціалізований комп'ютер, так і спеціалізована програма, працююча на вузловому сервері мережі.

До рівня міжмережевої взаємодії відносяться і протоколи, пов'язані із складанням і модифікацією таблиць маршрутизації, такі як протоколи збору маршрутної інформації RIP (Routing Internet Protocol) і OSPF (Open Shortest Path First), а також протокол міжмережевих повідомлень ICMP (Internet Control Message Protocol), що управляють. Останній протокол призначений

для обміну інформацією про помилки між маршрутизаторами мережі і вузлом — джерелом пакету.

Рівень мережевого інтерфейсу (Network) відповідає фізичному і канальному рівням моделі OSI. Цей рівень в протоколах TCP/IP не регламентується, але підтримує усі популярні стандарти фізичного і канального рівня: для локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet, для глобальних мереж — протоколи з'єднань «точка-точка» SLIP і PPP, протоколи територіальних мереж з комутацією пакетів X. 25, frame relay. Розроблена специфікація, що визначає використання технології ATM як транспорт канального рівня.

Розділені на рівні протоколи стека TCP/IP спроектовані таким чином, що конкретний рівень хоста призначення отримує саме той об'єкт, який був відправлений еквівалентним рівнем хоста джерела. Кожен рівень стека одного хоста утворює логічне з'єднання з однойменним рівнем стека іншого хоста. При реалізації фізичного з'єднання рівень передає свої дані інтерфейсу рівня, розташованого вище або нижче в тому ж хості (Рис. 2.2). Вертикальні стрілки показують фізичне з'єднання у рамках одного хоста, а горизонтальні стрілки показують логічне з'єднання між однойменними рівнями в різних хостах.

Слід звернути увагу на термінологію, традиційно використовувану для позначення інформаційних об'єктів, що поширюються на інтерфейсах між різними рівнями управління стека протоколів TCP/IP.

Застосування передає транспортному рівню повідомлення (message), яке має те, що відповідає цьому застосуванню розмір і семантику. Транспортний рівень «розрізає» це повідомлення (якщо воно досить велике) на пакети (packets), які передаються рівню міжмережевої взаємодії (т. е. протоколу IP). Протокол IP формує свої IP— пакети (ще говорять — IP— дейтаграми) і потім упаковує їх у

формат, прийнятний для цього фізичного середовища передачі інформації. Ці, вже апаратно-залежні, пакети зазвичай називають кадрами (frame).

Коли дані передаються від прикладного рівня до транспортного рівня, потім рівню міжмережевої взаємодії і далі через рівень мережевого інтерфейсу в мережу, кожен протокол виконує відповідну обробку і інкапсулює результат цієї обробки, приєднуючи спереду свій заголовок (Рис. 2.3).

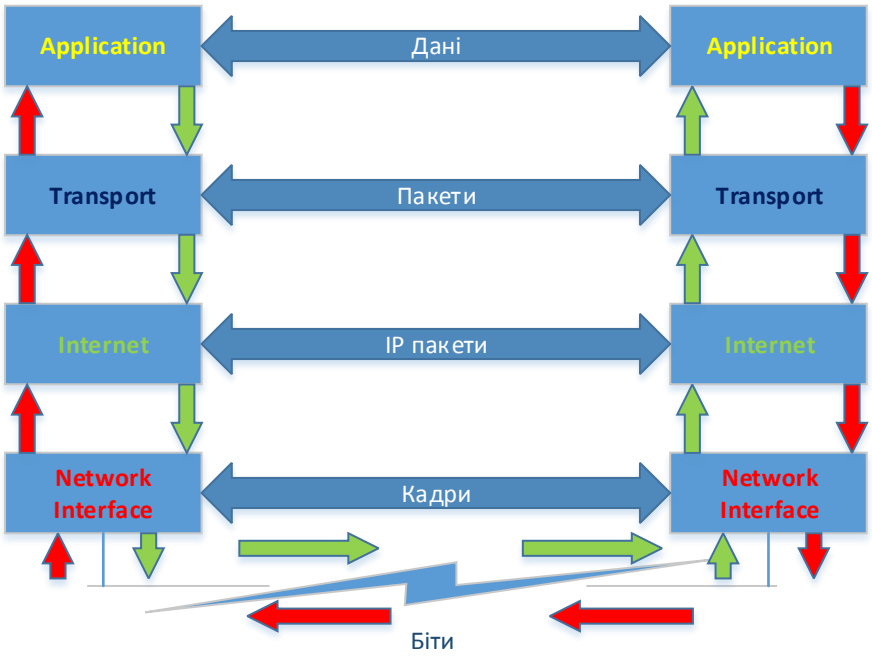

Рис. 2.2. Логічні і фізичні з'єднання між рівнями стека TCP/IP

У системі, що приймає цей потік інформації, ці заголовки послідовно віддаляються у міру обробки даних і передачі їх вгору по стеку. Такий підхід забезпечує необхідну гнучкість в обробці передаваних даних, оскільки верхнім рівням зовсім не треба торкатися технології, використовуваної в нижніх рівнях. Наприклад, якщо шифруються дані на рівні IP, рівень TCP і прикладний рівень залишаються незмінними.

Що стосується безпеки протоколів TCP/IP, т. е. безпеці передачі даних в Інтернеті в цілому, користувачам необхідно мати на увазі, що якщо не вжиті спеціальні заходи, то усі дані передаються протоколами TCP/IP у відкритому виді. Це означає, що будь-який вузол (і відповідно до його оператор), що знаходиться на шляху дотримання даних від відправника до одержувача, може скопіювати собі усі передавані дані і використати їх надалі у своїх цілях. В рівній мірі дані можуть бути спотворені або знищені.

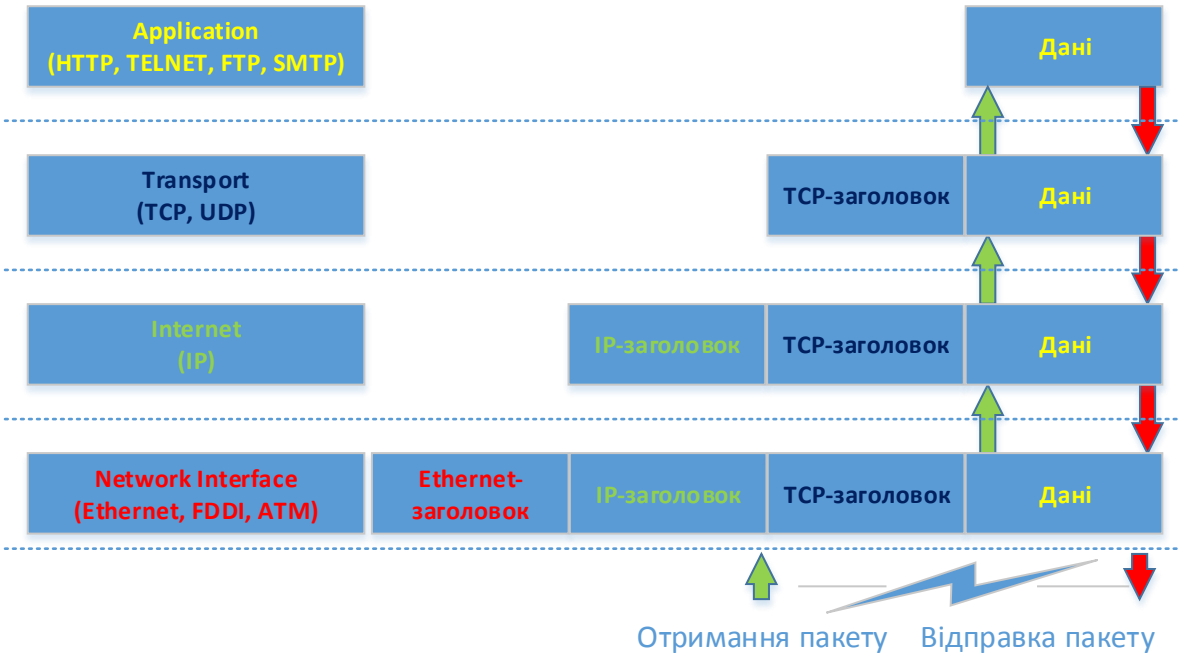

Рис. 2.3. Схема інкапсуляції даних в стеку протоколів TCP/IP

2.2. Аналіз загроз мережевої безпеки

Для організації комунікацій в неоднорідному мережевому середовищі застосовується набір протоколів TCP/IP, забезпечуючи сумісність між комп'ютерами різних типів. Сумісність — одна з основних переваг TCP/IP, тому більшість комп'ютерних мереж підтримують ці протоколи. Крім того, протоколи TCP/IP надають доступ до ресурсів глобальної мережі Інтернет.

Завдяки своїй популярності TCP/IP став стандартом де-факто для міжмережевої взаємодії. Проте повсюдне поширення стека протоколів TCP/IP оголило і його слабкі сторони. Створюючи своє дітище, архітектори стека TCP/IP не бачили причин для занепокоєння про захист мереж, що будуються на його основі. Тому в специфікаціях ранніх версій протоколу IP були відсутні вимоги безпеки, що привело до первинної уразливості реалізації цього протоколу.

2.2.1. Проблеми безпеки IP- мереж

Зростання популярності Інтернет-технологій супроводжується зростанням серйозних загроз розголошування персональних даних, критично важливих корпоративних ресурсів, державних таємниць і т. д. Хакери і інші зловмисники піддають загрозам мережеві інформаційні ресурси, намагаючись отримати до них доступ за допомогою спеціальних атак. Ці атаки стають усе більш витонченими по дії і нескладними у виконанні. Цьому сприяють два основні чинники.

По-перше, це повсюдне проникнення Інтернету. До цієї мережі підключені мільйони комп'ютерів. В найближчому майбутньому їх число у багато разів зросте, тому вірогідність доступу хакерів до уразливих комп'ютерів і комп'ютерних мереж також постійно зростає. Крім того, широке поширення Інтернету дозволяє хакерам обмінюватися інформацією в глобальному масштабі.

По-друге, це загальне поширення простих у використанні ОС і середовищ розробки. Цей чинник різко знижує вимоги до рівня знань зловмисника. Раніше від

хакера були потрібні хороші знання і навички програмування, щоб створювати і поширювати шкідливі програми. Тепер, для того, щоб отримати доступ до хакерського засобу, треба просто знати IP- адреса потрібного сайту, а для проведення атаки досить клацнути мишкою.

Проблеми забезпечення інформаційної безпеки в корпоративних комп'ютерних мережах обумовлені загрозами безпеки для локальних робітників станцій, локальних мереж і атаками на корпоративні мережі, що мають вихід в загальнодоступні мережі передачі даних.

Мережеві атаки такі ж різноманітні, як і системи, проти яких вони спрямовані. Одні атаки відрізняються великою складністю, інші може здійснити звичайний оператор, що навіть не припускає, які наслідки матиме його діяльність.

Цілі порушника, що здійснює атаку:

- порушення конфіденційності передаваної інформації;
- порушення цілісності і достовірності передаваної інформації;
- порушення працездатності усієї системи або окремих її частин.

Розподілені системи схильні до передусім видалених атак, оскільки компоненти розподілених систем зазвичай використовують відкриті канали передачі даних, і порушник може не лише проводити пасивне прослуховування передаваної інформації, але і модифікувати передаваний трафік (активна дія). І якщо активна дія на трафік може бути зафіксована, то пасивна дія практично не піддається виявленню. Але оскільки в ході функціонування розподілених систем обмін службовою інформацією між компонентами системи здійснюється теж по відкритих каналах передачі даних, то службова інформація стає таким же об'єктом атаки, як і дані користувача.

Трудність виявлення факту проведення видаленої атаки виводить цей вид неправомірних дій на перше місце по мірі небезпеки і перешкоджає своєчасному реагуванню на здійснену загрозу, внаслідок чого у порушника збільшуються шанси успішної реалізації атаки.

Безпека локальної мережі відрізняється від безпеки міжмережевої взаємодії тим, що на перше за значимістю місце виходять порушення зареєстрованих користувачів, оскільки в цьому випадку канали передачі даних локальної мережі знаходяться на контрольованій території і захист від несанкціонованого підключення до яких реалізується адміністративними методами.

На практиці IP- мережі уразливі для багатьох способів несанкціонованого вторгнення в процес обміну даними. У міру розвитку комп'ютерних і мережевих технологій (наприклад з появою мобільних Java- застосувань і елементів ActiveX) список можливих типів мережевих атак на IP- мережі постійно розширюється [9].

Найбільш поширені наступні атаки.

Підслуховування (sniffing). В основному дані по комп'ютерних мережах передаються в незахищеному форматі (відкритим текстом), що дозволяє зловмисникові, що отримав доступ до ліній передачі даних в мережі підслуховувати або прочитувати трафік. Для підслуховування в комп'ютерних мережах використовують сніффер. Сніффер пакетів є застосовною програмою, яка перехоплює усі мережеві пакети, що передаються через певний домен.

Нині сніффери працюють в мережах на цілком законній підставі. Вони використовуються для діагностики несправностей і аналізу трафіку. Проте з огляду на те, що деякі мережеві застосування передають дані в текстовому форматі (Telnet,

FTP, SMTP, POP3 і т. д.), за допомогою сніффера можна дізнатися корисну, а іноді і конфіденційну інформацію (наприклад, імена користувачів і паролі).

Перехоплення пароля, що передається по мережі в незашифрованій формі, шляхом «підслуховування» каналу є різновидом атаки підслуховування, яку називають password sniffing. Перехоплення імен і паролів створює велику небезпеку, оскільки користувачі часто застосовують один і той же логін і пароль для безлічі застосувань і систем. Багато користувачів взагалі мають один пароль для доступу до усіх ресурсів і застосувань. Якщо застосування працює в режимі клієнт/сервер, а аутентифікаційні дані передаються по мережі в читаному текстовому форматі, цю інформацію з великою вірогідністю можна використати для доступу до інших корпоративних або зовнішніх ресурсів.

Запобігти загрозі сніффінга пакетів можна за допомогою застосування для аутентифікації одноразових паролів, установки апаратних або програмних засобів, сніффери, що розпізнають, застосування криптографічного захисту каналів зв'язку.

Зміна даних. Зловмисник, що отримав можливість прочитати ваші дані, зможе зробити і наступний крок — змінити їх. Дані в пакеті можуть бути змінені, навіть якщо зловмисник нічого не знає ні про відправника, ні про одержувача. Навіть якщо ви не потребуєте строгої конфіденційності усіх передаваних даних, то напевно не захочете, щоб вони були змінені по дорозі.

Аналіз мережевого трафіку. Метою атак подібного типу є прослуховування каналів зв'язку і аналіз передаваних даних і службової інформації для вивчення топології і архітектури побудови системи, отримання критичної призначеної для користувача інформації (наприклад, паролів користувачів або номерів кредитних карт, що передаються у відкритому виді). До атак цього типу схильні такі протоколи, як FTP або Telnet, особливістю яких є те, що ім'я і пароль користувача передаються у рамках цих протоколів у відкритому виді.

Підміна довіреного суб'єкта. Велика частина мереж і ОС використовують IP-адресу комп'ютера, для того, щоб визначати, чи той це адресат, який потрібний. В деяких випадках можливе некоректне привласнення IP- адреси (підміна IP- адреси відправника іншою адресою). Такий спосіб атаки називають фальсифікацією адреси (IP - spoofing).

IP- спуфінг має місце, коли зловмисник, що знаходиться усередині корпорації або поза нею, видає себе за законного користувача. Він може скористатися IP-адресою, що знаходиться в межах діапазону санкціонованих IP- адрес, або авторизованою зовнішньою адресою, якій дозволяється доступ до певних мережевих ресурсів. Зловмисник може також використати спеціальні програми, що формують 1P-пакеты так, щоб вони виглядали як вихідні з дозволених внутрішніх адрес корпоративної мережі.

Атаки IP- спуфінга часто стають відправною точкою для інших атак. Класичним прикладом є атака типу «відмова в обслуговуванні» (DoS), яка розпочинається з чужої адреси, що приховує істинну особу хакера.

Загрозу спуфінга можна ослабити (але не усунути) за допомогою правильного налаштування управління доступом із зовнішньої мережі, припинення спроб спуфінга чужих мереж користувачами своєї мережі.

Слід мати на увазі, що IP- спуфінг може бути здійснений за умови, що аутентифікація користувачів проводиться на базі IP- адрес, тому атаки IP- спуфінга

можна запобігти шляхом введення додаткових методів аутентифікації користувачів (на основі одноразових паролів або інших методів криптографії).

Посередництво. Ця атака має на увазі активне підслуховування, перехоплення і управління передаваними даними невидимим проміжним вузлом. Коли комп'ютери взаємодіють на низьких мережевих рівнях, вони не завжди можуть визначити, з ким саме вони обмінюються даними.

Посередництво в обміні незашифрованими ключами (атака man - in - the - middle). Для проведення атаки man - in - the - middle (людина-в-середині) зловмисникові потрібний доступ до пакетів, що передаються по мережі. Такий доступ до усіх пакетів, що передаються від провайдера ISP у будь-яку іншу мережу, може, наприклад, отримати співробітник цього провайдера. Для атак цього типу часто використовуються сніффери пакетів, транспортні протоколи і протоколи маршрутизації.

Атаки man - in - the - middle проводяться з метою крадіжки інформації, перехоплення поточної сесії і діставання доступу до приватних мережевих ресурсів, для аналізу трафіку і отримання інформації про мережу і її користувачів, для проведення атак типу DoS, спотворення передаваних даних і введення несанкціонованої інформації в мережеві сесії.

Ефективно боротися з атаками типу man — in — the — middle можна тільки за допомогою криптографії. Для протидії атакам цього типу використовується інфраструктура управління відкритими ключами — PKI (Public Key Infrastructure).

Перехоплення сеансу (session hijacking). Після закінчення початкової процедури аутентифікації з'єднання, встановлене законним користувачем, наприклад з поштовим сервером, перемикається зловмисником на новий хост, а початковому серверу видається команда розірвати з'єднання. В результаті «співрозмовник» законного користувача виявляється непомітно підміненим.

Після діставання доступу до мережі атакуючий зловмисник може:

- посилати некоректні дані застосуванням і мережевим службам, що призводить до їх аварійного завершення або неправильного функціонування;
- наводнити комп'ютер або усю мережу трафіком, поки не станеться зупинки системи в результаті перевантаження;
- блокувати трафік, що приведе до втрати доступу авторизованих користувачів до мережевих ресурсів.

Відмова в обслуговуванні (Denial of Service, DoS). Ця атака відрізняється від атак інших типів: вона не націлена на діставання доступу до мережі або на отримання з цієї мережі якої-небудь інформації. Атака DoS робить мережу організації недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, ОС або застосування. По суті, вона позбавляє звичайних користувачів доступу до ресурсів або комп'ютерів мережі організації.

Більшість атак DoS спираються на загальні слабкості системної архітектури. У разі використання деяких серверних застосувань (таких як web - сереер або FTP-сервер) атаки DoS можуть полягати в тому, щоб зайняти усі з'єднання, доступні для цих застосувань, і тримати їх в зайнятому стані, не допускаючи обслуговування звичайних користувачів. В ході атак

DoS можуть використовуватися звичайні Інтернет-протоколи, такі як TCP і ICMP (Internet Control Message Protocol).

Атаки DoS важко запобігти, оскільки для цього потрібно координацію дій з провайдером. Якщо трафік, призначений для переповнювання мережі, не зупинити у провайдера, то на вході в мережу це зробити вже не можна, тому що уся смуга пропускання буде зайнята.

Якщо атака цього типу проводиться одночасно через безліч пристроїв, то говорять про розподілену атаку відмови в обслуговуванні DDoS (distributed DoS). Простота реалізації атак DoS і величезна шкода, що заподіюється ними організаціям і користувачам, залучають до них пильну увагу адміністраторів мережевій безпеці.

Парольні атаки. Їх мета — заволодіння паролем і логіном законного користувача. Зловмисники можуть проводити парольні атаки, використовуючи такі методи, як:

- підміна IP- адреси (1P-спуфінг);
- підслуховування (сніффінг);
- простий перебір.

IP- спуфінг і сніффінг пакетів були розглянуті вище. Ці методи дозволяють оволодіти паролем і логіном користувача, якщо вони передаються відкритим текстом по незахищеному каналу.

Часто хакери намагаються підібрати пароль і логін, використовуючи для цього численні спроби доступу. Такий метод носить назву атака повного перебору (brute force attack). Для цієї атаки використовується спеціальна програма, яка намагається отримати доступ до ресурсу загального користування (наприклад, до сервера). Якщо в результаті зловмисникові вдається підібрати пароль, він дістає доступ до ресурсів на правах звичайного користувача.

Парольних атак можна уникнути, якщо не користуватися паролями в текстовій формі. Використання одноразових паролів і криптографічної аутентифікації може практично звести нанівець загрозу таких атак. На жаль, не усі застосування, хости і пристрої підтримують вказані методи аутентифікації.

При використанні звичайних паролів необхідно придумати такий пароль, який було б важко підібрати. Мінімальна довжина пароля має бути не менше 8 символів. Пароль повинен включати символи верхнього регістра, цифри і спеціальні символи (# і т. д.).

Вгадування ключа. Криптографічний ключ є кодом або числом, необхідним для розшифровки захищеної інформації. Хоча упізнати ключ доступу не просто і вимагає великих витрат ресурсів, проте це можливо. Зокрема, для визначення значення ключа може бути використана спеціальна програма, що реалізовує метод повного перебору. Ключ, до якого дістає доступ що атакує, називається скомпрометованим. Той, що атакує використовує скомпрометований ключ для діставання доступу до захищених передаваних даних без відома відправника і одержувача. Ключ дає можливість розшифровувати і змінювати дані.

Атаки на рівні застосувань можуть проводитися декількома способами.

Найпоширеніший з них полягає у використанні відомих слабкостей серверного ПЗ (FTP, HTTP, web - сервера).

Головна проблема з атаками на рівні застосувань полягає в тому, що вони часто користуються портами, яким дозволений прохід через міжмережевий екран. Відомості про атаки на рівні застосувань широко публікуються, щоб дати можливість адміністраторам виправити проблему за допомогою корекційних

модулів (патчів). На жаль, багато хакерів також мають доступ до цих відомостей, що дозволяє їм вчитися.

Неможливо повністю виключити атаки на рівні застосувань. Хакери постійно відкривають і публікують на своїх сайтах в Інтернеті усі нові вразливі місця застосовних програм.

Тут важливо здійснювати хороше системне адміністрування. Щоб понизити уразливість від атак цього типу, можна зробити наступні заходи:

- аналізувати log- файли ОС і мережеві log- файли за допомогою спеціальних аналітичних застосувань;
- відстежувати дані CERT про слабкі місця застосовних програм;
- користуватися найсвіжішими версіями ОС і застосувань і самими останніми корекційними модулями (патчами);
- використати системи розпізнавання атак IDS (Intrusion Detection Systems).

Мережева розвідка — це збір інформації про мережу за допомогою загальнодоступних даних і застосувань. При підготовці атаки проти якої-небудь мережі хакер, як правило, намагається отримати про неї якомога більше інформації.

Мережева розвідка проводиться у формі запитів DNS, ехо-тестування (ping sweep) і сканування портів. Запити DNS допомагають зрозуміти, хто володіє тим або іншим доменом і які адреси цьому домену присвоєні. Луна-тестування адрес, розкритих за допомогою DNS, дозволяє побачити, які хости реально працюють в цьому середовищі. Отримавши список хостів, хакер використовує засоби сканування портів, щоб скласти повний список послуг, підтримуваних цими хостами. В результаті добувається інформація, яку можна використати для злому.

Системи IDS на рівні мережі і хостів зазвичай добре справляються із завданням повідомлення адміністратора про мережеву розвідку, що ведеться, що дозволяє краще підготуватися до майбутньої атаки і оповістити провайдера (ISP), в мережі якого встановлена система, що проявляє надмірну цікавість.

Зловживання довірою. Цей тип дій не є атакою в повному розумінні цього слова. Він є зловмисним використанням стосунків довіри, існуючих в мережі. Типовий приклад такого зловживання — ситуація в периферійній частині корпоративної мережі. У цьому сегменті зазвичай розташовуються сервери DNS, SMTP і HTTP. Оскільки усі вони належать одному і тому ж сегменту, злом одного з них призводить до злому і усіх інших, оскільки ці сервери довіряють іншим системам своєї мережі.

Ризик зловживання довірою можна понизити за рахунок суворішого контролю рівнів довіри в межах своєї мережі. Системи, розташовані із зовнішнього боку міжмережевого екрану, ніколи не повинні користуватися абсолютною довірою з боку систем, захищених міжмережевим екраном.

Стосунки довіри повинні обмежуватися певними протоколами і аутентифікуватися не лише по 1Р-адресам, але і за іншими параметрами.

Комп'ютерні віруси, мережеві «черв'яки», програма «Троянський кінь». Віруси є шкідливими програмами, які впроваджуються в інші програми для виконання певної небажаної функції на робочій станції кінцевого користувача. Вірус зазвичай розробляється зловмисниками так, щоб як можна довше залишатися невиявленим в комп'ютерній системі. Початковий період «дрімоти» вірусів є механізмом їх виживання. Вірус проявляється повною мірою в конкретний момент

часу, коли відбувається деяка подія виклику, наприклад п'ятниця 13-і, відома дата і т. п.

Різновидом програми-вірусу є мережевий «черв'як», який поширюється по глобальній мережі і не залишає своїй копії на магнітному носії. Цей термін використовується для іменування програм, які подібно до стрічкових черв'яків переміщаються по комп'ютерній мережі від однієї системи до іншої. «Черв'як» використовує механізми підтримки мережі для визначення вузла, який може бути уражений. Потім за допомогою цих же механізмів передає своє тіло в цей вузол і або активізується, або чекає відповідних умов для активізації. Мережеві «черв'яки» є небезпечним видом шкідливих програм, оскільки об'єктом їх атаки може стати будь-який з мільйонів комп'ютерів, підключених до глобальної мережі Internet. Для захисту від «черв'яка» необхідно вжити запобіжні заходи проти несанкціонованого доступу до внутрішньої мережі.

До комп'ютерних вірусів примикають так звані «троянські коні» (троянські програми). «Троянський кінь» — це програма, яка має вигляд корисного застосування, а на ділі виконує шкідливі функції (руйнування ПЗ, копіювання і пересилка зловмисникові файлів з конфіденційними даними і т. п.). Термін «троянський кінь» був уперше використаний хакером Даном Едварсом, співробітником Агентства національної безпеки США, що пізніше став. Небезпека «троянського коня» полягає в додатковому блоці команд, вставленому в початкову нешкідливу програму, яка потім надається користувачам АС. Цей блок команд може спрацьовувати при настанні якої-небудь умови (дати, стани системи) або по команді ззовні. Користувач, що запустив таку програму, наражає на небезпеку як свої файли, так і усю АС в цілому. Робочі станції кінцевих користувачів дуже уразливі для вірусів, мережевих «черв'яків» і «троянських коней».

Для захисту від вказаних шкідливих програм необхідно:

- виключення несанкціонованого доступу до виконуваних файлів;
- тестування програмних засобів, що придбавалися;
- контроль цілісності виконуваних файлів і системних областей;
- створення замкнутого середовища виконання програм.

Боротьба з вірусами, «черв'яками» і «троянськими кіньми» ведеться за допомогою ефективного антивірусного програмного забезпечення, працюючого на призначеному для користувача рівні і, можливо, на рівні мережі. Антивірусні засоби виявляють більшість вірусів, «черв'яків» і «троянських коней» і присікають їх поширення. Отримання найсвіжішої інформації про віруси допомагає ефективніше боротися з ними. У міру появи нових вірусів, «черв'яків» і «троянських коней» треба оновлювати бази цих антивірусних засобів і застосувань.

Перераховані атаки на IP- мережі можливі в результаті:

- використання загальнодоступних каналів передачі даних. Найважливіші дані, передаються по мережі в незашифрованому виді;
- уразливості в процедурах ідентифікації, реалізованих в стеку TCP/IP. Ідентифікуюча інформація на рівні IP передається у відкритому виді;
- відсутності у базовій версії стека протоколів TCP/IP механізмів, що забезпечують конфіденційність і цілісність передаваних повідомлень;
- аутентифікації відправника по його IP- адресі. Процедура аутентифікації виконується тільки на стадії встановлення з'єднання, а надалі достовірність пакетів, що приймаються, не перевіряється;

- відсутності контролю за маршрутом проходження повідомлень в мережі Internet, що робить видалені мережеві атаки практично безкарними

Перші засоби захисту передаваних даних з'явилися практично відразу після того, як уразливість IP- мереж дала про себе знати з практики. Характерними прикладами розробок в цій області можуть служити: PGP/Web - of - Trust для шифрування повідомлень електронної пошти, Secure Sockets Layer (SSL) для захисту Web- трафіку, Secure SHell (SSH) для захисту сеансів Telnet і процедур передачі файлів.

Загальним недоліком подібних широко поширених рішень є їх «прихильність» до певного типу застосувань, тобто нездатність задовольняти тим різноманітним вимогам до систем мережевого захисту, які пред'являють великі корпорації або Internet- провайдери.

Найрадикальніший спосіб подолання вказаного обмеження зводиться до побудови системи захисту не для окремих класів застосувань (хай і дуже популярних), а для мережі в цілому. Стосовно IP- мережам це означає, що системи захисту повинні діяти на мережевому рівні моделі OSI.

У 1993 р. у складі консорціуму 1ETF була створена робоча група IP Security Working Group, що зайнялася розробкою архітектури і протоколів для шифрування даних, що передаються по мережах IP. В результаті з'явився набір протоколів IPSec, заснованих на сучасних технологіях шифрування і електронного цифрового підпису даних. Оскільки архітектура протоколів IPSec сумісна з протоколом IPv4, її підтримку досить забезпечувати на обох кінцях з'єднання; проміжні мережеві вузли можуть взагалі нічого «не знати» про застосування IPSec.

Архітектура стека протоколів IPSec і його застосування для побудови захищених віртуальних каналів і мереж VPN (Virtual Private Networks) детально розглядаються в л. 12.

2.2.2. Загрози і уразливості дротяних корпоративних мереж

На початковому етапі розвитку мережевих технологій збиток від вірусних і інших типів комп'ютерних атак був невеликий, оскільки залежність світової економіки від інформаційних технологій була мала. Нині в умовах значної залежності бізнесу від електронних засобів доступу і обміну інформацією і постійно зростаючого числа атак збиток від самих незначних атак, що призводять до втрат машинного часу, обчислюється мільйонами доларів, а сукупний річний збиток світовій економіці складає десятки мільярдів доларів [9].

Інформація, що обробляється в корпоративних мережах, є особливо уразливою, чому сприяють:

- збільшення об'ємів оброблюваної, передаваної і такої, що зберігається в комп'ютерах інформації;
- зосередження у базах даних інформації різного рівня важливості і конфіденційності;
- розширення доступу круга користувачів до інформації, що зберігається у базах даних, і до ресурсів обчислювальної мережі;
- збільшення числа видалених робочих місць;
- широке використання глобальної мережі Internet і різних каналів зв'язку;

- автоматизація обміну інформацією між комп'ютерами користувачів.

Аналіз найбільш поширених загроз, до яких схильні сучасні дротяні корпоративні мережі, показує, що джерела загроз можуть змінюватися від неавторизованих вторгнень зловмисників до комп'ютерних вірусів, при цьому дуже істотною загрозою безпеки є людські помилки. Необхідно враховувати, що джерела загроз безпеки можуть знаходитися як усередині КІС — внутрішні джерела, так і поза нею — зовнішні джерела. Таке ділення цілком виправдане тому, що для однієї і тієї ж загрози (наприклад крадіжки) методи протидії для зовнішніх і внутрішніх джерел різні. Знання можливих загроз, а також вразливих місць КІС необхідно для вибирання найбільш ефективних засобів забезпечення безпеки.

Найчастішими і не безпечнішими (з точки зору розміру збитку) є неумисні помилки користувачів, операторів і системних адміністраторів, обслуговуючих КІС. Іноді такі помилки призводять до прямого збитку (неправильно введені дані, помилка в програмі, що викликала зупинку або руйнування системи), а іноді створюють слабкі місця, якими можуть скористатися зловмисники (такі зазвичай помилки адміністрування) [43].

Згідно з даними Національного інституту стандартів і технологій США (NIST), 55 % випадків порушення безпеки ІС — наслідок неумисних помилок. Робота в глобальній ІС робить цей чинник досить актуальним, причому джерелом збитку можуть бути як дії користувачів організації, так і користувачів глобальної мережі, що особливо небезпечно. На Рис. 2.4 приведена кругова діаграма, що ілюструє статистичні дані за джерелами порушень безпеки в КІС.

На другому місці по розмірах збитку розташовуються крадіжки і підробки. У більшості розслідуваних випадків винуватцями виявлялися штатні співробітники організацій, відмінно знайомі з режимом роботи і захисними заходами. Наявність потужного інформаційного каналу зв'язку з глобальними мережами за відсутності належного контролю за його роботою може додатково сприяти такій діяльності.

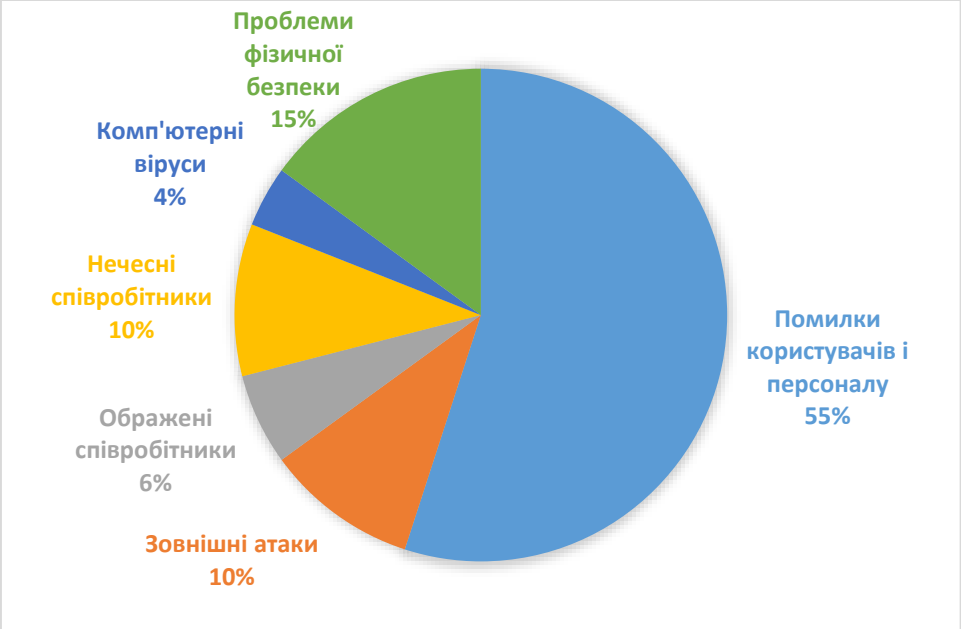

Рис. 2.4. Джерела порушень безпеки

Скривджені співробітники, що навіть були, знайомі з порядками в організації і здатні шкодити дуже ефективно. Тому при звільненні співробітника його права доступу до інформаційних ресурсів повинні анулюватися.

Умисні спроби отримання НСД через зовнішні комунікації займають близько 10 % усіх можливих порушень. Хоча ця величина здається не такою значною, досвід роботи в Internet показує, що майже кожен Intemet - сереер по декілька раз на день піддається спробам проникнення. Тести Агентства захисту інформаційних систем (США) показали, що 88 % комп'ютерів мають слабкі місця з точки зору інформаційної безпеки, які можуть активно використовуватися для отримання НСД. Окремо слід розглядати випадки видаленого доступу до інформаційних структур організацій.

До побудови політики безпеки необхідно оцінити риски, яким піддається комп'ютерне середовище організації і зробити відповідні дії. Очевидно, що витрати організації на контроль і запобігання загрозам безпеки не повинні перевищувати очікуваних втрат.

Приведені статистичні дані можуть підказати адміністрації і персоналу організації, куди слід направити зусилля для ефективного зниження загроз безпеки корпоративній мережі і системи. Звичайно, треба займатися проблемами фізичної безпеки і заходами по зниженню негативної дії на безпеку помилок людини, але в те ж

час необхідно приділяти найсерйозніша увага рішенню завдань мережевої безпеки по запобіганню атакам на корпоративну мережу і систему як ззовні, так і зсередини системи.

2.2.3. Загрози і уразливості безпровідних мереж

При побудові безпровідних мереж також стоїть проблема забезпечення їх безпеки. Якщо в звичайних мережах інформація передається по дротах, то радіохвилі, використовувані для безпровідних рішень, досить легко перехопити за наявності відповідного устаткування. Принцип дії безпровідної мережі призводить до виникнення великого числа можливих вразливостей для атак і проникнень.

Устаткування безпровідних локальних мереж WLAN (Wireless Local Area Network) включає точки безпровідного доступу і робочі станції для кожного абонента.

Точки доступу AP (Access Point) виконують роль концентраторів, що забезпечують зв'язок між абонентами і між собою, а також функцію мостів, що здійснюють зв'язок з кабельною локальною мережею і з Інтернет. Кожна точка доступу може обслуговувати декілька абонентів. Декілька близько розташованих точок доступу утворюють зону доступу Wi - Fi, в межах якої усі абоненти, забезпечені безпровідними адаптерами, дістають доступ до мережі. Такі зони доступу створюються в місцях масового скупчення людей: в аеропортах, студентських городках, бібліотеках, магазинах, бізнес-центрах і т. д.

У точки доступу є ідентифікатор набору сервісів SSID (Service Set Identifier). SSID — це 32-бітовий рядок, що використовується як ім'я безпровідної мережі, з якою асоціюються усі вузли. Ідентифікатор SSID потрібний для підключення робочої станції до мережі. Щоб зв'язати робочу станцію з точкою доступу, обидві

системи повинні мати один і той же SSID. Якщо робоча станція не має потрібного SSID, то вона не зможе зв'язатися з точкою доступу і з'єднатися з мережею.

Головна відмінність між дротяними і безпровідними мережами — наявність неконтрольованої області між кінцевими точками безпровідної мережі. Це дозволяє тим, що атакують, знаходяться у безпосередній близькості від безпровідних структур, проводити ряд нападів, які неможливі в дротом світі.

При використанні безпровідного доступу до локальної мережі загрози безпеки істотно зростають (Рис. 2.5).

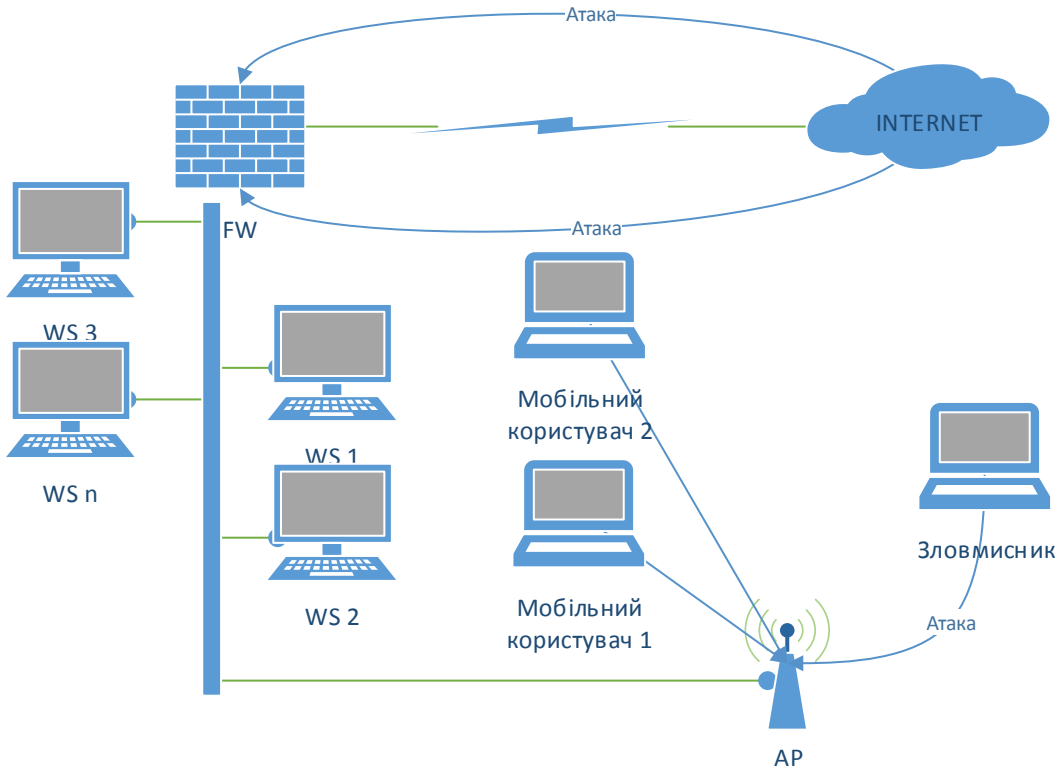

Рис. 2.5. Загрози при безпровідному доступі до локальної мережі

Перерахуємо основні уразливості і загрози безпровідних мереж.

Мовлення радіомаяка. Точка доступу включає з певною частотою широкомовний радіомаяк, щоб оповіщати навколишні безпровідні вузли про свою присутність. Ці широкомовні сигнали містять основну інформацію про точку безпровідного доступу, включаючи, як правило, SSID, і запрошують безпровідні вузли зареєструватися в цій області. Будь-яка робоча станція, що знаходиться в режимі очікування, може отримати SSID і додати себе у відповідну мережу. Мовлення радіомаяка є «природженою патологією» безпровідних мереж. Багато моделей дозволяють відключати SSID частину цього мовлення, що містить, щоб дещо утруднити безпровідне підслуховування, але SSID, проте, посилається при підключенні, тому все одно існує невелике вікно уразливості.

Виявлення WLAN. Для виявлення безпровідних мереж WLAN використовується, наприклад, утиліта NetStumber спільно з супутниковим навігатором глобальної системи позиціонування GPS. Ця утиліта ідентифікує SSID мережі WLAN, а також визначає, чи використовується в ній система шифрування WEP. Застосування зовнішньої антени на портативному комп'ютері робить можливим виявлення мереж WLAN під час обходу потрібного району або поїздки

по місту. Надійним методом виявлення WLAN є обстеження офісної будівлі з переносним комп'ютером в руках.

Підслуховування. Підслуховування ведуть для збору інформації про мережу, яку передбачається атакувати згодом. Перехоплювач може використати здобуті дані для того, щоб отримати доступ до мережевих ресурсів. Устаткування, використовуване для підслуховування в мережі, може бути не складніше того, яке використовується для звичайного доступу до цієї мережі. Безпровідні мережі за своєю природою дозволяють сполучати з фізичною мережею комп'ютери, що знаходяться на деякій відстані від неї, начебто ці комп'ютери знаходилися безпосередньо в мережі. Наприклад, підключитися до безпровідної мережі, розташованої у будівлі, може людина, що сидить в машині на стоянці поруч. Атаку за допомогою пасивного прослуховування практично неможливо виявити.

Неправдиві точки доступу в мережу. Досвідчений той, що атакує може організувати неправдиву точку доступу з імітацією мережевих ресурсів. Абоненти, нічого не підозрюючи, звертаються до цієї неправдивої точки доступу і повідомляють їй свої важливі реквізити, наприклад аутентифікаційну інформацію. Цей тип атак іноді застосовують у поєднанні з прямим «глушенням» істинної точки доступу в мережу.

Відмова в обслуговуванні. Повну паралізацію мережі може викликати атака типу DoS (Denial of Service) — відмова в обслуговуванні. Її мета полягає в створенні перешкоди при доступі користувача до мережевих ресурсів. Безпровідні системи особливо сприйнятливі до таких атак. Фізичний рівень у безпровідній мережі — абстрактний простір навколо точки доступу. Зловмисник може включити пристрій, що заповнює увесь спектр на робочій частоті перешкодами і нелегальним трафіком, — таке завдання не викликає особливих труднощів. Сам факт проведення DoS— атаки на фізичному рівні у безпровідній мережі важко довести.

Атаки типу «людина-в-середині». Атаки цього типу виконуються на безпровідних мережах набагато простіше, ніж на дротяних, оскільки у разі дротяної мережі вимагається реалізувати певний вид доступу до неї. Зазвичай атаки «людина-в-середині» використовуються для руйнування конфіденційності і цілісності сеансу зв'язку. Атаки MITM складніші, ніж більшість інших атак: для їх проведення потрібно детальну інформацію про мережу. Зловмисник зазвичай підміняє ідентифікацію одного з мережевих ресурсів. Він використовує можливість прослуховування і нелегального захоплення потоку даних з метою зміни його вмісту, необхідного для задоволення деяких своїх цілей, наприклад для спуфінга IP- адрес, зміни MAC-адреси для імітування іншого хоста і т. д.

Анонімний доступ в Інтернет. Незахищені безпровідні ЛВС забезпечують хакерам найкращий анонімний доступ для атак через Інтернет. Хакери можуть використати незахищену безпровідну ЛВС організації для виходу через неї в Інтернет, де вони здійснюватимуть протиправні дії, не залишаючи при цьому своїх слідів. Організація з незахищеною ЛВС формально стає джерелом атакуючого трафіку, націленого на іншу комп'ютерну систему, що пов'язано з потенційним ризиком правової відповідальності за заподіяний збиток жертві атаки хакерів.

Описані вище атаки не є єдиними атаками, використовуваними хакерами для злому безпровідних мереж.

2.3. Забезпечення інформаційної безпеки мереж

2.3.1. Способи забезпечення інформаційної безпеки

Існує два підходи до проблеми забезпечення безпеки комп'ютерних систем і мереж (КС): «фрагментарний» і комплексний [4, 62].

«Фрагментарний» підхід спрямований на протидію чітко певним загрозам в заданих умовах. В якості прикладів реалізації такого підходу можна вказати окремі засоби управління доступом, автономні засоби шифрування, спеціалізовані антивірусні програми і т. п.

Гідністю такого підходу є висока вибірковість до конкретної загрози. Істотний недолік — відсутність єдиного захищеного середовища обробки інформації. Фрагментарні заходи захисту інформації забезпечують захист конкретних об'єктів КС тільки від конкретної загрози. Навіть невелика видозміна загрози веде до втрати ефективності захисту.

Комплексний підхід орієнтований на створення захищеного середовища обробки інформації в КС, що об'єднує в єдиний комплекс різнорідні заходи протидії загрозам. Організація захищеного середовища обробки інформації дозволяє гарантувати певний рівень безпеки КС, що є безперечною гідністю комплексного підходу. До недоліків цього підходу відносяться: обмеження на свободу дій користувачів КС, чутливість до помилок установки і налаштування засобів захисту, складність управління.

Комплексний підхід застосовують для захисту КС великих організацій або невеликих КС, що виконують відповідальні завдання або оброблювальних особливо важливу інформацію. Порушення безпеки інформації в КС великих організацій може завдати величезного матеріального збитку як самим організаціям, так і їх клієнтам. Тому такі організації вимушені приділяти особливу увагу гарантіям безпеки і реалізовувати комплексний захист. Комплексного підходу дотримуються більшість державних і великих комерційних підприємств і установ. Цей підхід знайшов своє відображення в різних стандартах.

Комплексний підхід до проблеми забезпечення безпеки заснований на розробленій для конкретній КС політиці безпеки. Політика безпеки регламентує ефективну роботу засобів захисту КС. Вона охоплює усі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях. Надійна система безпеки мережі не може бути створена без ефективної політики мережевої безпеки. Політики безпеки детально розглядаються в Лек. 3.

Для захисту інтересів суб'єктів інформаційних стосунків необхідно поєднувати заходи наступних рівнів:

- законодавчого (стандарти, закони, нормативні акти і т. п.);
- адміністративно-організаційного (дії загального характеру, організації, що робляться керівництвом, і конкретні заходи безпеки, що мають справу з людьми);
- програмно-технічного (конкретні технічні заходи).

Заходи законодавчого рівня дуже важливі для забезпечення інформаційної безпеки. До цього рівня відноситься комплекс заходів, спрямованих на створення і підтримку в суспільстві негативного (у тому числі карального) відношення до порушень і порушників інформаційної безпеки.

Інформаційна безпека — це нова область діяльності, тут важливо не лише забороняти і карати, але і учити, роз'яснювати, допомагати. Суспільство повинне усвідомити важливість цієї проблематики, зрозуміти основні шляхи рішення відповідних проблем. Держава може зробити це оптимальним чином. Тут не треба великих матеріальних витрат, потрібно інтелектуальні вкладення.

Заходи адміністративно-організаційного рівня. Адміністрація організації повинна усвідомлювати необхідність підтримки режиму безпеки і виділяти на ці цілі відповідні ресурси. Основою заходів захисту адміністративно-організаційного рівня є політика безпеки (див. л. 3) і комплекс організаційних заходів.

До комплексу організаційних заходів відносяться заходи безпеки, що реалізовуються людьми. Виділяють наступні групи організаційних заходів:

- управління персоналом;
- фізичний захист;
- підтримка працездатності;
- реагування на порушення режиму безпеки;
- планування відновних робіт.

Для кожної групи в кожній організації повинен існувати набір регламентів, що визначають дії персоналу.

Заходи і засоби програмно-технічного рівня. Для підтримки режиму інформаційної безпеки особливо важливі заходи програмно-технічного рівня, оскільки основна загроза комп'ютерним системам виходить від них самих: збої устаткування, помилки програмного забезпечення, промахи користувачів і адміністраторів і т. п. У рамках сучасних інформаційних систем мають бути доступні наступні механізми безпеки:

- ідентифікація і перевірка достовірності користувачів;
- управління доступом;
- протоколювання і аудит;
- криптографія;
- екранування;
- забезпечення високої доступності.

Необхідність застосування стандартів.

Інформаційні системи (ІС) компаній майже завжди побудовані на основі програмних і апаратних продуктів різних виробників. Поки немає жодної компанії-розробника, яка надала б споживачеві повний перелік засобів (від апаратних до програмних) для побудови сучасної ІС. Щоб забезпечити в різнорідній ІС надійний захист інформації потрібно фахівців високої кваліфікації, які повинні відповідати за безпеку кожного компонента ІС: правильно їх настроювати, постійно відстежувати зміни, що відбуваються, контролювати роботу користувачів. Очевидно, що чим різнорідніше ІС, тим складніше забезпечити її безпеку. Достаток в корпоративних мережах і системах пристроїв зашиті, міжмережевих екранів (МЕ), шлюзів і VPN, а також зростаючий попит на доступ до корпоративних даних з боку співробітників, партнерів і замовників призводять до створення складного середовища захисту, важкого для управління, а іноді і несумісною.

Інтероперацийність продуктів захисту є невід'ємною вимогою для КІС. Для більшості гетерогенних середовищ важливо забезпечити погоджену взаємодію з продуктами інших виробників. Прийняте організацією рішення безпеки повинне гарантувати захист на усіх платформах у рамках цієї організації. Тому цілком

очевидна потреба в застосуванні єдиного набору стандартів як постачальниками засобів захисту, так і компаніями — системними інтеграторами і організаціями, що виступають замовниками систем безпеки для своїх корпоративних мереж і систем.

Стандарти утворюють понятійний базис, на якому будуються усі роботи по забезпеченню інформаційної безпеки, і визначають критерії, яким повинне слідувати управління безпекою. Стандарти є необхідною основою, що забезпечує сумісність продуктів різних виробників, що надзвичайно важливо при створенні систем мережевої безпеки в гетерогенних середовищах. Міжнародні і вітчизняні стандарти інформаційної безпеки розглядаються в л. 4.

Комплексний підхід до вирішення проблеми забезпечення безпеки, раціональне поєднанні законодавчих, адміністративно-організаційних і програмно-технічних заходів і обов'язкове наслідування промислових, національних і міжнародних стандартів — це той фундамент, на якому будується уся система захисту корпоративних мереж.

2.3.2. Шляхи рішення проблем захисту інформації в мережах

Для пошуку рішень проблем інформаційної безпеки при роботі в мережі Інтернет був створений незалежний консорціум ISTF (Internet Security Task Force) — громадська організація, що складається з представників і експертів компаній-постачальників засобів інформаційній безпеці, електронних бізнесів і провайдерів Internet— інфраструктури. Мета консорціуму — розробка технічного, організаційного і операційного керівництва по безпеці роботи в Internet.

Консорціум ISTF виділив 12 областей інформаційної безпеки, на яких в першу чергу повинні сконцентрувати свою увагу творці електронного бізнесу, щоб забезпечити його працездатність. Цей список, зокрема, включає:

- аутентифікацію (механізм об'єктивного підтвердження ідентифікуючої інформації);
- право на приватну, персональну інформацію (забезпечення конфіденційності інформації);
- визначення подій безпеки (Security Events);
- захист корпоративного периметра;
- визначення атак;
- контроль за потенційно небезпечним вмістом;
- контроль доступу;
- адміністрування;
- реакцію на події (Incident Response).

Рекомендації ISTF призначені для існуючих або

знову утворюваних компаній електронної комерції і електронного бізнесу.

Їх реалізація означає, що захист інформації в системі електронного бізнесу має бути комплексним.

Для комплексної зашиті від загроз і гарантії економічно вигідного і безпечного використання комунікаційних ресурсів для електронного бізнесу необхідно:

- проаналізувати загрози безпеки для системи електронного бізнесу;
- розробити політику інформаційної безпеки;

- захистити зовнішні канали передачі інформації, забезпечивши конфіденційність, цілісність і достовірність передаваної по них інформації;
- гарантувати можливість безпечного доступу до відкритих ресурсів зовнішніх мереж і Internet, а також спілкування з користувачами цих мереж;
- захистити окремі найбільш комерційно значимі ІС незалежно від використовуваних ними каналів передачі даних;
- надати персоналу захищений видалений доступ до інформаційних ресурсів корпоративної мережі;
- забезпечити надійне централізоване управління засобами мережевого захисту.

Згідно з рекомендаціями ISTF, першим і найважливішим етапом розробки системи інформаційної безпеки електронного бізнесу є механізми управління доступом до мереж загального користування і доступом з них, а також механізми безпечних комунікацій, МЕ, що реалізовуються, і продуктами захищених віртуальних мереж VPN.

Супроводжуючи їх засобами інтеграції і управління усією ключовою інформацією системи захисту (PKI — інфраструктура відкритих ключів), можна отримати цілісну, централізовану керовану систему інформаційної безпеки.

Наступний етап включає засоби контролю доступу користувачів, що інтегруються до загальної структури, в систему разом з системою одноразового входу і авторизації (Single Sign On).

Антивірусний захист, засоби аудиту і виявлення атак, по суті, завершують створення інтегрованої цілісної системи безпеки, якщо не йдеться про роботу з конфіденційними даними. В цьому випадку потрібно засоби криптографічного захисту даних і електронно-цифрового підпису.

Для реалізації основних функціональних компонентів системи безпеки для електронного бізнесу застосовуються різні методи і засоби захисту інформації:

- захищені комунікаційні протоколи;
- засоби криптографії;
- механізми аутентифікації і авторизації;
- засоби контролю доступу до робочих місць мережі і з мереж загального користування;
- антивірусні комплекси;
- програми виявлення атак і аудиту;
- засоби централізованого управління контролем доступу користувачів, а також безпечного обміну пакетами даних і повідомленнями будь-яких застосувань по відкритих IP-мережах.

Застосування комплексу засобів захисту на усіх рівнях корпоративної системи дозволяє побудувати ефективну і надійну систему забезпечення інформаційної безпеки.

Перелічені вище методи і засоби захисту інформації детально розглядаються в подальших лекціях.

Лекція 3 ПОЛІТИКИ БЕЗПЕКИ

Під політикою безпеки організації розуміють сукупність документованих управлінських рішень, спрямованих на захист інформації і асоційованих з нею ресурсів. Політика безпеки є тим засобом, за допомогою якого реалізується діяльність в комп'ютерній інформаційній системі організації. Взагалі політика безпеки визначається використовуваним комп'ютерним середовищем і відбиває специфічні потреби організації.

Зазвичай КІС є складним комплексом різнорідного, такого, що іноді погано узгоджується між собою апаратного і програмного забезпечення: комп'ютерів, ОС, мережевих засобів, СУБД, різноманітних застосувань. Усі ці компоненти зазвичай мають власні засоби захисту, які треба погоджувати між собою. Тому в якості погодженої платформи по забезпеченню безпеки корпоративної системи дуже важлива ефективна політика безпеки. У міру зростання комп'ютерної системи і інтеграції її в глобальну мережу, необхідно забезпечити відсутність в системі слабких місць, оскільки усі зусилля із захисту інформації можуть бути знецінені лише однією помилкою.

Політику безпеки можна побудувати так, щоб вона встановлювала, хто має доступ до конкретних активів і застосувань, які ролі і обов'язки матимуть конкретних осіб, а також передбачити процедури безпеки, які чітко пропонують, як повинні виконуватися конкретні завдання безпеки. Особливості роботи конкретного співробітника можуть зажадати доступу до інформації, яка не має бути доступна іншим працівникам. Наприклад, менеджер по персоналу може мати доступ до приватної інформації будь-якого співробітника, тоді як фахівець із звітності може мати доступ тільки до фінансових даних цих співробітників, а рядовий співробітник матиме доступ тільки до своєї власної персональної інформації.

Політика безпеки визначає позицію організації по раціональному використанню комп'ютерів і мережі, а також процедури по запобіганню і реагуванню на інциденти безпеки. У великій корпоративній системі може застосовуватися широкий діапазон різних політик — від бізнес-політик до специфічних правил доступу до наборів даних. Ці політики повністю визначаються конкретними потребами організації.

3.1. Основні поняття політики безпеки

Політика безпеки визначає стратегію управління в області інформаційної безпеки, а також міру уваги і кількість ресурсів, які вважає за доцільне виділити керівництво.

Політика безпеки будується на основі аналізу ризиків, які визнаються реальними для ІС організації. Коли проведений аналіз ризиків і визначена стратегія захисту, складається програма, реалізація якої повинна забезпечити інформаційну безпеку. Під цю програму виділяються ресурси, призначаються відповідальні, визначається порядок контролю виконання програми і т. п.

Політика безпеки організації повинна мати структуру короткого, легко такого, що розуміється документу високорівневої політики, підтримуваного конкретними документами спеціалізованих політик і процедур безпеки.

Високорівнева політика безпеки повинна періодично переглядатися, гарантуючи тим самим облік поточних потреб організації. Документ політики складають так, щоб політика була відносно незалежною від конкретних технологій, в цьому випадку документ не потрібно буде змінювати занадто часто.

Для того, щоб познайомитися з основними поняттями політики безпеки розглянемо в якості конкретного прикладу гіпотетичну локальну мережу, що належить деякій організації, і асоційовану з нею політику безпеки [5, 63].

Політика безпеки зазвичай оформляється у вигляді документу, що включає такі розділи, як опис проблеми, сфера застосування, позиція організації, розподіл ролей і обов'язків, санкції та ін.

Опис проблеми. Інформація, циркулююча у рамках локальної мережі, є критично важливою. Локальна мережа дозволяє користувачам спільно використати програми і дані, що збільшує загрозу безпеки. Тому кожен з комп'ютерів, що входять в мережу, потребує сильнішого захисту. Ці підвищені заходи безпеки і є темою цього документу, який покликаний продемонструвати співробітникам організації важливість захисту мережевого середовища, описати їх роль в забезпеченні безпеки, а також розподілити конкретні обов'язки по захисту інформації, циркулюючої в мережі.

Сфера застосування. У сферу дії цієї політики потрапляють усі апаратні, програмні і інформаційні ресурси, що входять в локальну мережу підприємства. Політика орієнтована також на людей, працюючих з мережею, у тому числі на користувачів, субпідрядників і постачальників.

Позиція організації. Основні цілі — забезпечення цілісності, доступності і конфіденційності даних, а також їх повноти і актуальності. До приватних цілей відносяться:

- забезпечення рівня безпеки, що відповідає нормативним документам;
- дотримання економічної доцільності у виборі захисних заходів(витрати на захист не повинні перевершувати передбачуваний збиток від порушення інформаційної безпеки);
- забезпечення безпеки в кожній функціональній області локальної мережі;
- забезпечення підзвітності усіх дій користувачів з інформацією і ресурсами;
- забезпечення аналізу реєстраційної інформації;
- надання користувачам достатньої інформації для свідомої підтримки режиму безпеки;
- вироблення планів відновлення після аварій і інших критичних ситуацій для усіх функціональних областей з метою забезпечення безперервності роботи мережі;
- забезпечення відповідності з наявними законами і загальноорганізаційною політикою безпеки.

Розподіл ролей і обов'язків. За реалізацію сформульованих вище цілей відповідають відповідні посадовці і користувачі мережі.

Керівники підрозділів відповідають за доведення положень політики безпеки до користувачів і за контакти з ними.

Адміністратори локальної мережі забезпечують безперервне функціонування мережі і відповідають за реалізацію технічних заходів, необхідних для проведення в життя політики безпеки. Вони зобов'язані:

- забезпечувати захист устаткування локальної мережі, у тому числі інтерфейсів з іншими мережами;
- оперативно і ефективно реагувати на події, що таять загрозу, інформувати адміністраторів сервісів про спроби порушення захисту;
- використати перевірені засоби аудиту і виявлення підозрілих ситуацій, щодня аналізувати реєстраційну інформацію, що відноситься до мережі в цілому і до файлових серверів особливо;
- не зловживати своїми повноваженнями, оскільки користувачі мають право на таємницю;
- розробляти процедури і готувати інструкції для захисту локальної мережі від шкідливого програмного забезпечення, надавати допомогу у виявленні і ліквідації шкідливого коду;
- регулярно виконувати резервне копіювання інформації, що зберігається на файлових серверах;
- виконувати усі зміни мережевої апаратно-програмної конфігурації;
- гарантувати обов'язковість процедури ідентифікації і аутентифікації для доступу до мережевих ресурсів, виділяти користувачам вхідні імена і початкові паролі тільки після заповнення реєстраційних форм;
- періодично проводити перевірку надійності захисту локальної мережі, не допускати отримання привілеїв неавторизованими користувачами.

Адміністратори сервісів відповідають за конкретні сервіси, і зокрема за побудову захисту відповідно до загальної політики безпеки. Вони зобов'язані:

- управляти правами доступу користувачів до обслуговуваних об'єктів;
- оперативно і ефективно реагувати на події, що таять загрозу, надавати допомогу у відображенні загрози, виявленні порушників і наданні інформації для їх покарання;
- регулярно виконувати резервне копіювання інформації, що обробляється сервісом;
- виділяти користувачам вхідні імена і початкові паролі тільки після заповнення реєстраційних форм;
- щодня аналізувати реєстраційну інформацію, що відноситься до сервісу, регулярно контролювати сервіс на предмет шкідливого програмного забезпечення;
- періодично проводити перевірку надійності захисту сервісу, не допускати отримання привілеїв неавторизованими користувачами.

Користувачі працюють з локальною мережею відповідно до політики безпеки, підкоряються розпорядженням осіб, що відповідають за окремі аспекти безпеки, повідомляють керівництво про усі підозрілі ситуації. Вони зобов'язані:

- знати і дотримуватися законів, правила, прийняті в цій організації, політику безпеки, процедури безпеки, використати доступні захисні механізми для забезпечення конфіденційності і цілісності своєї інформації;
- використати механізм захисту файлів і належним чином задавати права доступу;

- вибирати якісні паролі, регулярно міняти їх, не записувати паролі на папері, не повідомляти їх іншим особам;
- інформувати адміністраторів або керівництво про порушення безпеки і інші підозрілі ситуації;
- не використати слабкості в захисті сервісів і локальної мережі в цілому, не здійснювати неавторизованої роботи з даними, не створювати перешкод іншим користувачам;
- завжди повідомляти коректну ідентифікаційну і аутентифікаційну інформацію, не намагатися працювати від імені інших користувачів;
- забезпечувати резервне копіювання інформації з жорсткого диска свого комп'ютера;
- знати принципи роботи шкідливого програмного забезпечення, шляху його проникнення і поширення, знати і дотримуватися процедур для попередження проникнення шкідливого коду, його виявлення і знищення;
- знати і дотримуватися правил поведінки в екстрених ситуаціях, послідовність дій при ліквідації наслідків аварій.

Санкції. Порушення політики безпеки може піддати локальну мережу і циркулюючу в ній інформацію неприпустимому ризику. Випадки порушення безпеки з боку персоналу повинні оперативно розглядатися керівництвом для вжиття дисциплінарних заходів аж до звільнення.

Додаткова інформація. Конкретним групам виконавців можуть знадобитися для ознайомлення додаткові документи, зокрема, документи спеціалізованих політик і процедур безпеки, а також інші керівні вказівки. Необхідність в додаткових документах політик безпеки значною мірою залежить від розмірів і складності організації. Для досить великої організації можуть знадобитися на додаток до базової політики спеціалізовані політики безпеки. Організації меншого розміру потребують тільки деякої підмножини спеціалізованих політик. Багато хто з цих документів підтримки може бути коротким — об'ємом в одну-дві сторінки.

Управлінські заходи забезпечення інформаційної безпеки

Головною метою заходів, що робляться на управлінському рівні, є формування програми робіт в області інформаційної безпеки і забезпечення її виконання шляхом виділення необхідних ресурсів і здійснення регулярного контролю стану справ. Основою цієї програми є багаторівнева політика безпеки, що відбиває комплексний підхід організації до захисту своїх ресурсів і інформаційних активів.

З практичної точки зору політики безпеки можна розділити на три рівні: верхній, середній і нижній [5, 6].

Верхній рівень політики безпеки визначає рішення, що зачіпають організацію в цілому. Ці рішення носять дуже загальний характер і виходять, як правило, від керівництва організації.

Такі рішення можуть включати наступні елементи:

- формулювання цілей, які переслідує організація в області інформаційної безпеки, визначення загальних напрямів в досягненні цих цілей;
- формування або перегляд комплексної програми забезпечення інформаційної безпеки, визначення відповідальних осіб за просування програми;
- забезпечення матеріальної бази для дотримання законів і правил;

- формулювання управлінських рішень з питань реалізації програми безпеки, які повинні розглядатися на рівні організації в цілому.

Політика безпеки верхнього рівня формулює цілі організації в області інформаційної безпеки в термінах цілісності, доступності і конфіденційності. Якщо організація відповідає за підтримку критично важливих баз даних, на першому плані повинна стояти цілісність даних. Для організації, що займається продажами, важлива актуальність інформації про послуги, що надаються, і ціни, а також її доступність максимальному числу потенційних покупців. Режимна організація в першу чергу піклуватиметься про конфіденційність інформації, т. е. про її захист від НСД.

На верхній рівень виноситься управління ресурсами безпеки і координація використання цих ресурсів, виділення спеціального персоналу для захисту критично важливих систем, підтримка контактів з іншими організаціями, що забезпечують або контролюючими режим безпеки.

Політика верхнього рівня повинна чітко визначати сферу свого впливу. У неї можуть бути включені не лише усі комп'ютерні системи організації, але і домашні комп'ютери співробітників, якщо політика регламентує деякі аспекти їх використання. Можлива і така ситуація, коли в сферу впливу включаються лише найбільш важливі системи.

У політиці мають бути визначені обов'язки посадовців по виробленню програми безпеки і по проведенню її в життя, т. е. політика може служити основою підзвітності персоналу.

Політика верхнього рівня має справу з трьома аспектами законослухняної і виконавської дисципліни. По-перше, організація повинна дотримуватися існуючих законів. По-друге, слід контролювати дії осіб, відповідальних за розробку програми безпеки. По-третє, необхідно забезпечити виконавську дисципліну персоналу за допомогою системи заохочень і покарань.

Середній рівень політики безпеки визначає вирішення питань, що стосуються окремих аспектів інформаційної безпеки, але важливих для різних систем, експлуатованих організацією. Приклади таких питань — відношення до доступу в Internet(проблема поєднання свободи отримання інформації із захистом від зовнішніх загроз), використання домашніх комп'ютерів і т. д.

Політика безпеки середнього рівня повинна визначати для кожного аспекту інформаційної безпеки наступні моменти:

- опис аспекту — позиція організації може бути сформульована в досить загальному вигляді, а саме як набір цілей, які переслідує організація в цьому аспекті;
- сфера застосування — слід специфікувати, де, коли, як, по відношенню до кого і чому застосовується ця політика безпеки;
- ролі і обов'язки — документ повинен містити інформацію про посадовці, що відповідають за проведення політики безпеки в життя;
- санкції — політика повинна містити загальний опис заборонених дій і покарань за них;
- точки контакту — повинно бути відомо, куди слід звертатися за роз'ясненнями, допомогою і додатковою інформацією. Зазвичай «точкою контакту» служить посадовець.

Нижній рівень політики безпеки відноситься до конкретних сервісів. Вона включає два аспекти — мети і правила їх досягнення, тому її порою важко відокремити від питань реалізації. На відміну від двох верхніх рівнів, дана політика має бути детальнішою, т. е. при наслідуванні політики безпеки нижнього рівня необхідно дати відповідь, наприклад, на такі питання:

- хто має право доступу до об'єктів, підтримуваних сервісом;
- за яких умов можна читати і модифікувати дані;
- як організований видалений доступ до сервісу.

Політика безпеки нижнього рівня може виходити з міркувань цілісності, доступності і конфіденційності, але вона не повинна на них зупинятися. У загальному випадку мети повинні зв'язувати між собою об'єкти сервісу і осмислені дії з ними.

З цілей виводяться правила безпеки, що описують, хто, що і за яких умов може робити. Чим детальніше правила, чим чіткіше і формально вони викладені, тим простіше підтримувати їх виконання програмно-технічними заходами. Зазвичай найформальніше задаються права доступу до об'єктів.

3.2. Структура політики безпеки організації

Для більшості організацій політика безпеки абсолютно потрібна. Вона визначає відношення організації до забезпечення безпеки і необхідні дії організації по захисту своїх ресурсів і активів. На основі політики безпеки встановлюються необхідні засоби і процедури безпеки, а також визначаються ролі і відповідальність співробітників організації в забезпеченні безпеки.

Зазвичай політика безпеки організації включає:

- базову політику безпеки;
- спеціалізовані політики безпеки;
- процедури безпеки.

Основні положення політики безпеки організації описуються в наступних документах:

- огляд політики безпеки — розкриває мету політики безпеки, описує структуру політики безпеки, детально викладає, хто і за що відповідає, встановлює процедури і передбачувані часові рамки для внесення змін. Залежно від масштабу організації політика безпеки може містити більше або менше розділів;
- опис базової політики безпеки — визначає дозволені і заборонені дії, а також необхідні засоби управління у рамках архітектури безпеки, що реалізовується;
- керівництво по архітектурі безпеки — описує реалізацію механізмів безпеки в компонентах архітектури, використовуваних в мережі організації(Рис. 3.1).

Рис. 3.1. Структура політики безпеки організації

Головним компонентом політики безпеки організації є базова політика безпеки [9].

3.2.1. Базова політика безпеки

Базова політика безпеки встановлює, як організація обробляє інформацію, хто може отримати до неї доступ і як це можна зробити.

Низхідний підхід, що реалізовується базовою політикою безпеки, дає можливість поступово і послідовно виконувати роботу із створення системи безпеки, не намагаючись відразу виконати її цілком. Базова політика дозволяє у будь-який час ознайомитися з політикою безпеки в повному об'ємі і з'ясувати поточний стан безпеки в організації.

Структура і склад політики безпеки залежить від розміру і цілей компанії. Зазвичай базова політика безпеки організації підтримується набором спеціалізованих політик і процедур безпеки.

3.2.2. Спеціалізовані політики безпеки

Потенційно існують десятки спеціалізованих політик, які можуть застосовуватися більшістю організацій середнього і великого розміру. Деякі політики призначаються для кожної організації, інші — специфічні для певного комп'ютерного оточення.

З урахуванням особливостей застосування спеціалізовані політики безпеки можна розділити на дві групи:

- політики, що зачіпають значне число користувачів;
- політики, пов'язані з конкретними технічними областями.

До спеціалізованих політиків, що зачіпають значне число користувачів, відносяться:

- політика допустимого використання;
- політика видаленого доступу до ресурсів мережі;
- політика захисту інформації;
- політика захисту паролів та ін.

До спеціалізованих політиків, пов'язаних з конкретними технічними областями, відносяться:

- політика конфігурації міжмережевих екранів;
- політика по шифруванню і управлінню криптоключами;
- політика безпеки віртуальних захищених мереж VPN;

- політика по устаткуванню безпровідної мережі та ін.

Розглянемо детальніше деякі з ключових спеціалізованих політик.

Політика допустимого використання. Її мета — встановлення стандартних норм безпечного використання комп'ютерного устаткування і сервісів в компанії, а також відповідних заходів безпеки співробітників для захисту корпоративних ресурсів і власної інформації. Неправильне використання комп'ютерного устаткування і сервісів піддає компанію рискам, включаючи вірусні атаки, компрометацію мережевих систем і сервісів. Конкретний тип і кількість політик допустимого використання залежать від результатів аналізу вимог бізнесу, оцінки ризиків і корпоративної культури в організації.

Політика допустимого використання застосовується до співробітників, консультантів, тимчасових службовців і інших працівників компанії, включаючи співробітників сторонніх організацій. Політика допустимого використання призначена в основному для кінцевих користувачів і вказує їм, які дії дозволяються, а які заборонені. Без зафіксованої у відповідному документі політики допустимого використання, штатні співробітники управління і підтримки мережі не мають формальних підстав для застосування санкцій до свого або стороннього співробітника, який припустив грубе порушення правил безпечної роботи на комп'ютері або в мережі.

Політика допустимого використання встановлює:

- відповідальність користувачів за захист будь-якої інформації, що використовуваної і/або зберігається їх комп'ютерами;
- правомочність користувачів читати і копіювати файли, які не є їх власними, але доступні їм;
- рівень допустимого використання електронної пошти і Web- доступу.

Для освітніх і державних установ політика допустимого використання, по суті, просто обов'язкова.

Спеціального формату для політики допустимого використання не існує: має бути вказане ім'я сервісу, системи або підсистеми(наприклад політика використання комп'ютера, електронної пошти, компактних комп'ютерів і паролів) і описана в найчіткіших термінах дозволена і заборонена поведінка, а також наслідки порушення її правил і санкції, що накладаються на порушника.

Розробка політики допустимого використання виконується кваліфікованими фахівцями з відповідного сервісу, системи або підсистеми під контролем комісії(команди), якій доручена розробка політики безпеки організації.

Політика видаленого доступу. Її мета — встановлення стандартних норм безпечного видаленого з'єднання будь-якого хоста з мережею компанії. Стандартні норми покликані мінімізувати збиток компанії із-за можливого неавторизованого використання ресурсів компанії. До такого збитку відносяться: втрата інтелектуальної власності компанії, втрата конфіденційних даних, спотворення іміджу компанії, ушкодження критичних внутрішніх систем компанії і т. д.

Ця політика торкається усіх співробітників, постачальників і агентів компанії при використанні ними для видаленого з'єднання з мережею компанії комп'ютерів або робочих станцій, що є власністю компанії або знаходяться в особистій власності.

Політика видаленого доступу:

- намічає і визначає допустимі методи видаленого з'єднання з внутрішньою мережею;
- істотна у великій організації, де мережі територіально розподілені;
- повинна охоплювати по можливості усі поширені методи видаленого доступу до внутрішніх ресурсів.

Політика видаленого доступу визначає:

- які методи дозволяються для видаленого доступу;
- обмеження на дані, до яких можна отримати видалений доступ;
- хто може мати видалений доступ.

Захищений видалений доступ має бути строго контрольованим. Вживана процедура контролю повинна гарантувати, що доступ до належної інформації або сервісів отримають тільки минулі перевірку люди. Співробітник компанії не повинен передавати свій логін і пароль ніколи і нікому, включаючи членів сім'ї. Управління видаленим доступом не має бути складним і призводити до виникнення помилок.

Контроль доступу доцільно виконувати за допомогою одноразової парольної аутентифікації або за допомогою відкритих/секретних ключів(див. л. 7 і 13).

Співробітники компанії з правами видаленого доступу повинні гарантувати, що що належать їм або компанії персональний комп'ютер або робоча станція, які видалено приєднані до корпоративної мережі компанії, не будуть пов'язані в цей же час з якою-небудь іншою мережею, за винятком персональних мереж, що знаходяться під повним контролем користувача. Крім того, їх з'єднання видаленого доступу повинне мати такі ж характеристики безпеки, як звичайне локальне з'єднання з компанією.

Усі хости, які підключені до внутрішніх мереж компанії за допомогою технологій видаленого доступу, повинні використати найсучасніше антивірусне забезпечення. Ця вимога відноситься і до персональних комп'ютерів компанії.

Будь-який співробітник компанії, викритий в порушенні цієї політики, може бути підданий дисциплінарному стягненню аж до звільнення з роботи.

3.2.3. Процедури безпеки

Процедури безпеки є необхідним і важливим доповненням до політиків безпеки. Політики безпеки тільки описують, що повинно бути захищено і які основні правила захисту. Процедури безпеки визначають як захистити ресурси і які механізми виконання політики, т. е. як реалізовувати політики безпеки.

По суті процедури безпеки є покроковими інструкціями для виконання оперативних завдань. Часто процедура є тим інструментом, за допомогою якого політика перетвориться в реальну дію. Наприклад, політика паролів формулює правила конструювання паролів, правила про те, як захистити пароль і як часто його замінювати. Процедура управління паролями описує процес створення нових паролів, їх розподілу, а також процес гарантованої зміни паролів на критичних пристроях.

Процедури безпеки детально визначають дії, які треба зробити при реагуванні на конкретні події; забезпечують швидке реагування в критичній ситуації; допомагають усунути проблему єдиної точки відмови в роботі, якщо,

наприклад, під час кризи працівник несподівано покидає робоче місце або виявляється недоступний.

Багато процедур, пов'язаних з безпекою, має бути стандартними засобами у будь-якому підрозділі. В якості прикладів можна вказати процедури для резервного копіювання і позасистемного зберігання захищених копій, а також процедури для виведення користувача з активного стану і/або архівації логіна і пароля користувача, вживані відразу, як тільки цей користувач звільняється з організації.

Розглянемо декілька важливих процедур безпеки, які потрібні майже кожній організації.

Процедура реагування на події є необхідним засобом безпеки для більшості організацій. Організація особливо уразлива, коли виявляється вторгнення в її мережу або коли вона стикається із стихійним лихом.

Процедуру реагування на події іноді називають процедурою обробки подій або процедурою реагування на інциденти. Практично неможливо вказати відгуки на усі події порушень безпеки, але треба прагнути охопити основні типи порушень, які можуть статися. Наприклад: сканування портів мережі, атака типу «відмова в обслуговуванні», компрометація хоста, НСД та ін.

Ця процедура визначає:

- обов'язки членів команди реагування;
- яку інформацію реєструвати і простежувати;
- як обробляти дослідження відхилень від норми і атаки вторгнення;
- кого і коли повідомляти;
- хто може випускати у світло інформацію і яка процедура випуску інформації;
- як повинен виконуватися подальший аналіз і хто в цьому братиме участь.

У команду реагування можуть бути включені посадовці компанії, менеджер маркетингу(для зв'язку з пресою), системний і мережевий адміністратори і представник відповідних правоохоронних органів. Процедура повинна вказати, коли і в якому порядку вони викликаються.

Процедура управління конфігурацією зазвичай визначається на корпоративному рівні або рівні підрозділу. Ця процедура повинна визначити процес документування і запиту змін конфігурації на усіх рівнях ухвалення рішень. В принципі повинна існувати центральна група, яка розглядає усі запити на зміни конфігурації і приймає необхідні рішення.

Процедура управління конфігурацією визначає:

- хто має повноваження виконати зміни конфігурації апаратного і програмного забезпечення;
- як тестується і інсталюється нове апаратне і програмне забезпечення;
- як документуються зміни в апаратному і програмному забезпеченні;
- хто має бути проінформований, коли трапляються зміни в апаратному і програмному забезпеченні.

Процес управління конфігурацією важливий, оскільки документує зроблені зміни і забезпечує можливість аудиту; документує можливий простій системи; дає спосіб координувати зміни так, щоб одна зміна не завадила іншому.

Лекція 4 СТАНДАРТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Проблемою інформаційної комп'ютерної безпеки почали займатися з того моменту, коли комп'ютер став обробляти дані, цінність яких висока для користувача. З розвитком комп'ютерних мереж і зростанням попиту на електронні послуги ситуація у сфері інформаційної безпеки серйозно загострилася, а питання стандартизації підходів до її рішення стало особливо актуальним як для розробників, так і для користувачів ІТ засобів.

4.1. Роль стандартів інформаційної безпеки

Головне завдання стандартів інформаційної безпеки — створити основу для взаємодії між виробниками, споживачами і експертами по кваліфікації продуктів ІТ. Кожна з цих груп має свої інтереси і свої погляди на проблему інформаційної безпеки.

Споживачі зацікавлені в методиці, що дозволяє обґрунтовано вибрати продукт, що відповідає їх потребам і вирішальний їх проблеми, для чого їм потрібна шкала оцінки безпеки. Споживачі також потребують інструменту, за допомогою якого вони могли б формулювати свої вимоги виробникам. При цьому споживачів цікавлять виключно характеристики і властивості кінцевого продукту, а не методи і засоби їх досягнення. На жаль, багато споживачів не розуміють, що вимоги безпеки обов'язково суперечать функціональним вимогам(зручності роботи, швидкодії і т. д.), накладають обмеження на сумісність і, як правило, змушують відмовитися від широко поширених і тому незахищених прикладних програмних засобів.

Виробники потребують стандартів як засобу порівняння можливостей своїх продуктів, в застосуванні процедури сертифікації як механізму об'єктивної оцінки їх властивостей, а також в стандартизації певного набору вимог безпеки, який міг би обмежити фантазію замовника конкретного продукту і змусити його вибирати вимоги з цього набору. З точки зору виробника вимоги безпеки мають бути максимально конкретними і регламентувати необхідність застосування тих або інших засобів, механізмів, алгоритмів і т. д. Крім того, вимоги не повинні суперечити існуючим парадигмам обробки інформації, архітектурі обчислювальних систем і технологіям створення інформаційних продуктів. Проте такий підхід також не можна визнати в якості домінуючого, оскільки він не враховує потреб користувачів і намагається підігнати вимоги захисту під існуючі системи і технології.

Експерти по кваліфікації і фахівці з сертифікації розглядають стандарти як інструмент, що дозволяє їм оцінити рівень безпеки, що забезпечується продуктами ІТ, і надати споживачам можливість зробити обґрунтований вибір. Експерти по кваліфікації знаходяться в подвійному положенні: з одного боку, вони, як і виробники, зацікавлені в чітких і простих критеріях, над якими не потрібно сушити голову, як їх застосувати до конкретного продукту, а з іншого боку, вони повинні дати обґрунтовану відповідь користувачам — задовольняє продукт їх нужди або ні.

Таким чином, перед стандартами інформаційної безпеки стоїть непросте завдання — примирити три різні точки зору і створити ефективний механізм

взаємодії усіх сторін. Причому утиск потреб хоч би однієї з них приведе до неможливості взаєморозуміння і взаємодії

і, отже, не дозволить вирішити загальне завдання — створення захищеної системи обробки інформації.

Необхідність в таких стандартах була усвідомлена досить давно, і в цьому напрямі досягнутий істотний прогрес, закріплений в документах розробки 1990х рр. Першим і найбільш відомим документом була Помаранчева книга(за кольором обкладинки) «Критерії безпеки комп'ютерних систем» Міністерства оборони США. У цьому документі визначені 4 рівні безпеки — D, C, B і A. У міру переходу від рівня D до A до надійності системи пред'являються усе більш жорсткі вимоги. Рівні C і B підрозділяються на класи(C1, C2, B1, B2, B3). Щоб система в результаті процедури сертифікації могла бути віднесена до деякого класу, її захист повинен задовольняти обумовленим вимогам. До інших важливих стандартів інформаційної безпеки цього покоління відносяться: «Європейські критерії безпеки інформаційних технологій», «Федеральні критерії безпеки інформаційних технологій США», «Канадські критерії безпеки комп'ютерних систем» [30, 63].

Останнім часом в різних країнах з'явилося нове покоління стандартів, присвячених практичним питанням управління інформаційною безпекою компанії. Це передусім міжнародні стандарти управління інформаційною безпекою ISO 15408, ISO 17799 і деякі інші. Представляється доцільним проаналізувати найбільш важливі з цих документів, зіставити вимоги, що містяться в них, і критерії, а також оцінити ефективність їх практичного застосування.

4.2. Міжнародні стандарти інформаційної безпеки

Відповідно до міжнародних і національних стандартів забезпечення інформаційної безпеки у будь-якій компанії припускає наступне:

- визначення цілей забезпечення інформаційної безпеки комп'ютерних систем;
- створення ефективної системи управління інформаційною безпекою;
- розрахунок сукупності деталізованих якісних і кількісних показників для оцінки відповідності інформаційної безпеки поставленим цілям;
- застосування інструментарію забезпечення інформаційної безпеки і оцінки її поточного стану;
- використання методик управління безпекою, що дозволяють об'єктивно оцінити захищеність інформаційних активів і управляти інформаційною безпекою компанії.

Розглянемо найбільш відомі міжнародні стандарти в області захисту інформації, які можуть бути використані у вітчизняних умовах [52].

4.2.1. Стандарти ISO/IEC 17799:2002(BS 7799:2000)

Міжнародний стандарт ISO/IEC 17799:2000(BS 7799-1:2000) «Управління інформаційною безпекою — Інформаційні технології» (Information technology — Information security management) є одним з найбільш відомих стандартів в області захисту інформації. Цей стандарт був розроблений на основі першої частини Британського стандарту BS 7799-1:1995 «Практичні рекомендації по управлінню інформаційною безпекою» (Information security management — Part 1: Code of

practice for information security management) і відноситься до нового покоління стандартів інформаційної безпеки комп'ютерних ІС.

Поточна версія стандарту ISO/IEC 17799:2000(BS 7799-1:2000) розглядає наступні актуальні питання забезпечення інформаційної безпеки організацій і підприємств:

- необхідність забезпечення інформаційної безпеки;
- основні поняття і визначення інформаційної безпеки;
- політика інформаційної безпеки компанії;
- організація інформаційної безпеки на підприємстві;
- класифікація і управління корпоративними інформаційними ресурсами;
- кадровий менеджмент і інформаційна безпека;
- фізична безпека;
- адміністрування безпеки КІС;
- управління доступом;
- вимоги по безпеці до КІС в ході їх розробки, експлуатації і супроводу;
- управління бізнес процесами компанії з точки зору інформаційної безпеки;
- внутрішній аудит інформаційної безпеки компанії.

Друга частина стандарту BS 7799-2:2000 «Специфікації систем управління інформаційною безпекою» (Information security management — Part 2: Specification for information security management systems), визначає можливі функціональні специфікації корпоративних систем управління інформаційною безпекою з точки зору їх перевірки на відповідність вимогам першої частини цього стандарту. Відповідно до положень цього стандарту також регламентується процедура аудиту КІС.

Додаткові рекомендації для управління інформаційною безпекою містять керівництво Британського інституту стандартів — British Standards Institution(BSI), видані в 1995-2003 рр. у вигляді наступної серії:

- Вступ в проблему управління інформаційною безпекою (Information security managment: an introduction);
- Можливості сертифікації на вимоги стандарту BS 7799 (Preparing for BS 7799 sertification);
- Керівництво BS 7799 за оцінкою і управлінням рисками (Guide to BS 7799 risk assessment and risk management);
- Керівництво для проведення аудиту на вимоги стандарту BS 7799 Guide to BS 7799 auditing);
- Практичні рекомендації по управлінню безпекою інформаційних технологій (Code of practice for IT management).

У 2002 р. міжнародний стандарт ISO 17799 (BS 7799) був переглянутий і істотно доповнений. У новому варіанті цього стандарту велика увага приділена питанням підвищення культури захисту інформації в різних міжнародних компаніях. На думку фахівців, оновлення міжнародного стандарту ISO 17799 (BS 7799) дозволить не лише підвищити культуру захисту інформаційних активів компанії, але і скоординувати дії різних ведучих державних і комерційних структур в області захисту інформації.

4.2.2. Німецький стандарт BSI

На відміну від ISO 17799 німецьке «Керівництво по захисту інформаційних технологій для базового рівня захищеності» присвячене детальному розгляду приватних питань управління інформаційною безпекою компанії.

У німецькому стандарті BSI представлені:

- загальна методика управління інформаційною безпекою(організація менеджменту в області інформаційної безпеки, методологія використання керівництва);
- описи компонентів сучасних IT;
- описи основних компонентів організації режиму інформаційної безпеки(організаційний і технічний рівні захисту даних, планування дій в надзвичайних ситуаціях, підтримка безперервності бізнесу);
- характеристики об'єктів інформатизації(будівлі, приміщення, кабельні мережі, контрольовані зони);
- характеристики основних інформаційних активів компанії(у тому числі апаратне і програмне забезпечення, наприклад робочі станції і сервери під управлінням ОС сімейства DOS, Windows і UNIX);
- характеристики комп'ютерних мереж на основі різних мережевих технологій, наприклад мережі Novell NetWare, мережі UNIX і Windows).
- характеристика активного і пасивного телекомунікаційного устаткування провідних постачальників, наприклад Cisco Systems;
- детальні каталоги загроз безпеки і заходів контролю(більше 600 найменувань в кожному каталозі).

Питання захисту приведених інформаційних активів компанії розглядаються за певним сценарієм: загальний опис інформаційного активу компанії — можливі загрози і уразливості безпеки — можливі засоби контролю і захисту.

4.2.3. Міжнародний стандарт ISO 15408 «Загальних критеріїв безпеки інформаційних технологій»

Одним з головних результатів стандартизації у сфері систематизації вимог і характеристик захищених інформаційних комплексів стала система міжнародних і національних стандартів безпеки інформації, яка налічує більше сотні різних документів. Важливе місце в цій системі стандартів займає стандарт ISO 15408, відомий як «Common Criteria».

У 1990 р. Міжнародна організація по стандартизації(ISO) приступила до розробки міжнародного стандарту за критеріями оцінки безпеки IT для загального використання. У розробці брали участь: Національний інститут стандартів і технології і Агентство національної безпеки(США), Установа безпеки комунікацій(Канада), Агентство інформаційної безпеки(Німеччина), Агентство національної безпеки комунікацій(Голландія), органи виконання Програми безпеки і сертифікації IT(Англія), Центр забезпечення безпеки систем(Франція), які спиралися на свій солідний заділ.

За десятиліття розробки кращими фахівцями світу документ неодноразово редагувався. Перші дві версії були опубліковані відповідно в січні і травні 1998 р. Версія 2.1 цього стандарту затверджена 8 червня 1999 р. Міжнародною організацією по стандартизації(ISO) в якості міжнародного стандарту

інформаційної безпеки ISO/IEC 15408 під назвою «Загальні критерії оцінки безпеки інформаційних технологій», або «Common Criteria».

«Загальні критерії» (ЗКР) узагальнили зміст і досвід використання Помаранчевої книги, розвинули європейські і канадські критерії і утілили в реальні структури концепцію типових профілів захисту федеральних критеріїв США.

У ЗКР проведена класифікація широкого набору вимог безпеки ІТ, визначені структури їх групування і принципи використання. Головні достоїнства ЗКР — повнота вимог безпеки і їх систематизація, гнучкість в застосуванні і відкритість для подальшого розвитку.

Провідні світові виробники устаткування ІТ відразу стали поставляти замовникам засоби, що повністю відповідають вимогам ЗКР.

ЗКР розроблялися для задоволення запитів трьох груп фахівців, що в рівній мірі є користувачами цього документу: виробників і споживачів продуктів ІТ, а також експертів за оцінкою рівня їх безпеки. ЗКР забезпечують нормативну підтримку процесу вибору ІТ продукт, до якого пред'являються вимоги функціонування в умовах дії певних загроз, служать керівним матеріалом для розробників таких систем, а також регламентують технологію їх створення і процедуру оцінки забезпечуваного рівня безпеки.

ЗКР розглядають інформаційну безпеку, по-перше, як сукупність конфіденційності і цілісності інформації, оброблюваною ІТ продуктом, а також доступності ресурсів ВС і, по друге, ставлять перед засобами захисту завдання протидії загрозам, актуальним для середовища експлуатації цього продукту і реалізації політики безпеки, прийнятої в цьому середовищі експлуатації. Тому в концепцію ЗКР входять усі аспекти процесу проектування, виробництва і експлуатації ІТ продуктів, призначених для роботи в умовах дії певних загроз безпеки.

Споживачі ІТ продуктів заклопотані наявністю загроз безпеки, що призводять до певних рисок для оброблюваної інформації. Для протидії цим загрозам ІТ продукти повинні включати до свого складу засоби захисту, протидіючі цим загрозам і спрямовані на усунення вразливостей, проте помилки в засобах захисту у свою чергу можуть призводити до появи нових вразливостей. Сертифікація засобів захисту дозволяє підтвердити їх адекватність загрозам і рискам.

ЗКР регламентують усі стадії розробки, кваліфікаційного аналізу і експлуатації ІТ продуктів. ЗКР пропонують концепцію процесу розробки і кваліфікаційного аналізу ІТ продуктів, що вимагає від споживачів і виробників великої роботи по складанню і оформленню об'ємних і детальних нормативних документів.

Вимоги ЗКР є практично усеосяжною енциклопедією інформаційної безпеки, тому їх можна використати в якості довідника по безпеці ІТ.

Стандарт ISO 15408 підняв стандартизацію ІТ на міждержавний рівень. Виникла реальна перспектива створення єдиного безпечного інформаційного простору, в якому сертифікація безпеки систем обробки інформації здійснюватиметься на глобальному рівні, що надають можливості для інтеграції національних ІС, що у свою чергу відкриє нові сфери застосування ІТ.

4.2.4. Стандарти для безпровідних мереж

Стандарт IEEE 802.11. У 1990 р. Комітет IEEE 802 сформував робочу групу 802.11 для розробки стандарту для безпровідних локальних мереж. Роботи із створення стандарту були завершені через 7 років. У 1997 р. була ратифікована перша специфікація безпровідного стандарту IEEE 802.11, що забезпечує передачу даних з гарантованою швидкістю 1 Мб/с (в деяких випадках до 2 Мб/с) в смузі частот 2,4 ГГц. Ця смуга частот доступна для неліцензійного використання у більшості країн світу.

Стандарт IEEE 802.11 є базовим стандартом і визначає протоколи, необхідні для організації безпровідних локальних мереж WLAN (Wireless Local Area Network). Основні з них — протокол управління доступом до середовища MAC (Medium Accsess Control — нижній підрівень канального рівня) і протокол PHY передачі сигналів у фізичному середовищі. В якості фізичного середовища допускається використання радіохвиль і інфрачервоного випромінювання.

У основу стандарту IEEE 802.11 покладена стільникова архітектура, причому мережа може складатися як з однієї, так і декількох осередків. Кожна з них управляється базовою станцією, що називається точкою доступу AP (Access Point), яка разом з тими, що знаходяться в межах радіусу її дії робочими станціями користувачів утворює базову зону обслуговування BSS (Basic Service Set). Точки доступу багатостільникової мережі взаємодіють між собою через розподільну систему DS (Distribution System), що є еквівалентом магістрального сегменту кабельних JTC. Уся інфраструктура, що включає точки доступу і розподільну систему утворює розширену зону обслуговування ESS (Extended Service Set). Стандартом передбачений також одностільниковий варіант безпровідної мережі, який може бути реалізований і без точки доступу, при цьому частина її функцій виконуються безпосередньо робочими станціями.

Для забезпечення переходу мобільних робочих станцій із зони дії однієї точки доступу до іншої у багато стільникових системах передбачені спеціальні процедури сканування (активного і пасивного прослуховування ефіру) і приєднання (Association), проте строгих специфікацій по реалізації роумінгу стандарт IEEE 802.11 не передбачає.

Для захисту WLAN стандартом IEEE 802.11 передбачений алгоритм WEP (Wired Equivalent Privacy). Він включає засоби протидії НСД до мережі, а також шифрування для запобігання перехопленню інформації.

Проте закладена в першу специфікацію стандарту IEEE 802.11 швидкість передачі даних у безпровідній мережі перестала задовольняти потребам користувачів: алгоритм WEP мав ряд істотних недоліків — відсутність управління ключем, використання загального статичного ключа, малі розрядності ключа і вектору ініціалізації, складності використання алгоритму RC4.

Щоб зробити технологію Wireless LAN недорогою, популярною і задовольняючою жорстким вимогам бізнес додатків, розробники створили сімейство нових специфікацій стандарту IEEE 802.11 — a, b, ..., i. Стандарти цього сімейства, по суті, є безпровідними розширеннями протоколу Ethernet, що забезпечує хорошу взаємодію з дротяними мережами Ethernet.

Стандарт IEEE 802.11b був ратифікований IEEE у вересні 1999 р. як розвиток базового стандарту 802.11; у ньому використовується смуга частот 2,4 ГГц,

швидкість передачі досягає 11 Мб/с (подібно до Ethernet). Завдяки орієнтації на освоєний діапазон 2,4 ГГц стандарт 802.11b завоював велику популярність у виробників устаткування. В якості базової радіотехнології в ньому використовується метод розподіленого спектру з прямою послідовністю DSSS (Direct Sequence Spread Spectrum), який відрізняється високою стійкістю до спотворення даних перешкодами, у тому числі умисними. Цей стандарт отримав широке поширення, і безпровідні LAN стали привабливим рішенням з технічної і фінансової точки зору.

Стандарт IEEE 802.11a призначений для роботи в частотному діапазоні 5 ГГц. Швидкість передачі даних до 54 Мбіт/с, т. е. приблизно у 5 разів швидше за мережі 802.11b. Асоціація WECA називає цей стандарт WiFi5. Це найбільш широкосмуговий стандарт з сімейства стандартів 802.11. Визначені три обов'язкові швидкості — 6, 12 і 24 Мбіт/с і п'ять необов'язкових — 9, 18, 36, 48 і 54 Мбіт/с. В якості методу модуляції сигналу прийнято ортогональне частотне мультиплексування OFDM (Orthogonal Frequency Division Multiplexing). Його відмінність від методу DSSS полягає в тому, що OFDM припускає паралельну передачу корисного сигналу одночасно по декількох частотах діапазону, тоді як технології розширення спектру DSSS передають сигнали послідовно. В результаті підвищується пропускна спроможність каналу і якість сигналу. До недоліків стандарту 802.11a відноситься велика споживана потужність радіопередавачів для частот 5 ГГц, а також менший радіус дії(близько 100 м).

Для простоти запам'ятовування в якості загального імені для стандартів 802.11b і 802.11a, а також усіх подальших, таких, що відносяться до безпровідних локальних мереж(WLAN), Асоціацією безпровідної сумісності з Ethernet WECA (Wireless Ethernet Compatibility Aliance) був введений термін WiFi (Wireless Fidelity). Якщо пристрій помічений цим знаком, воно протестоване на сумісність з іншими пристроями 802.11.

Стандарт IEEE 802.11g є розвитком 802.11b і назад поєднаємо з 802.11b; призначений для забезпечення швидкостей передачі даних до 54 Мбіт/с. У числі переваг 802.1 lg потрібно відмітити низьку споживану потужність, великі відстані (до 300 м) і високу проникаючу здатність сигналу.

Стандарт IEEE 802.11i — стандарт забезпечення безпеки у безпровідних мережах; ратифікований IEEE в 2004 р. Цей стандарт вирішив існуючі проблеми в області аутентифікації і протоколу шифрування, забезпечивши значно більш високий рівень безпеки. Стандарт 802.11 і може застосовуватися в мережах WiFi, незалежно від використовуваного стандарту — 802.11a, b або g.

Існують два дуже схожих стандарту — WPA і 802.11i. WPA був розроблений в WiFi Alliance як рішення, яке можна застосувати негайно, не чекаючи завершення тривалої процедури ратифікації 802.11i в IEEE. Обидва стандарти використовують механізм 802.1x для забезпечення надійної аутентифікації, обоє використовують сильні алгоритми шифрування і призначені для заміни протоколу WEP.

Їх основна відмінність полягає у використанні різних механізмів шифрування. У WPA застосовується протокол TKIP (Temporal Key Integrity Protocol), який, також як і WEP, використовує шифр RC4, але значно безпечнішим способом. Забезпечення конфіденційності даних в стандарті IEEE 802.1 li засноване на використанні алгоритму шифрування AES (Advanced Encryption Standard). Захисний протокол, що використовує його, дістав назву CCMP (CounterMode CBC

MAC Protocol). Алгоритм AES має високу криптостійкістю. Довжина ключа AES дорівнює 128, 192 або 256 біт, що забезпечує найбільш надійне шифрування з доступних зараз.

Стандарт 802.11i припускає наявність трьох учасників процесу аутентифікації:

1. сервер аутентифікації AS (Authentication Server),
2. точка доступу AP (Access Point)
3. робоча станція STA (Station).

В процесі шифрування даних беруть участь тільки AP і STA(AS не використовується). Стандарт передбачає двосторонню аутентифікацію (на відміну від WEP, де аутентифікує тільки робоча станція, але не точка доступу). При цьому місцями ухвалення рішення про дозвіл доступу є сервер аутентифікації AS і робоча станція STA, а місцями виконання цього рішення — точка доступу AP і STA.

Для роботи за стандартом 802.11i створюється ієрархія ключів, що містить:

- головний ключ МК (Master Key)
- парний головний ключ РМК (Pairwise Master Key),
- парний тимчасовий ключ РТК (Pairwise Transient Key),
- групові тимчасові ключі GTK (Group Transient Key),
- службові для захисту широкомовного мережевого трафіку.

МК — це симетричний ключ, що реалізовує рішення STA і AS про взаємну аутентифікацію. Для кожної сесії створюється новий МК.

РМК — оновлюваний симетричний ключ, володіння яким означає дозвіл(авторизацію) на доступ до середовища передачі даних впродовж цієї сесії. РМК створюється на основі МК. Для кожної пари STA і AP в кожній сесії створюється новий РМК.

РТК — це колекція операційних ключів, які використовуються для прив'язки РМК до даних STA і AP, поширення GTK і шифрування даних.

Процес аутентифікації і доставки ключів визначається стандартом 802.1x. Він надає можливість використати у безпровідних мережах такі традиційні сервери аутентифікації, як RADIUS (Remote Authentication DialIn User Server). Стандарт 802.11i не визначає тип сервера аутентифікації, але використання RADIUS для цієї мети є стандартним рішенням.

Транспортом для повідомлень 802.1x служить протокол EAP (Extensible Authentication Protocol). EAP дозволяє легко додавати

нові методи аутентифікації. Точці доступу не вимагається знати про використовуваний метод аутентифікації, тому зміна методу ніяк не зачіпає точку доступу. Найбільш популярні методи EAP — це LEAP, PEAP, TTLS і FAST. Кожен з методів має свої сильні і слабкі сторони, умови застосування, по-різному підтримується виробниками устаткування і ПЗ.

Виділяють п'ять фаз роботи 802.11i.

Перша фаза — виявлення. У цій фазі робоча станція STA знаходить точку доступу AP, з якою може встановити зв'язок і отримує від неї використовувані в цій мережі параметри безпеки. Таким чином STA дізнається ідентифікатор мережі SSID і методи аутентифікації, доступні в цій мережі. Потім STA вибирає метод аутентифікації, і між STA і AP встановлюється з'єднання. Після цього STA і AP готові до початку другої фази 802.1x.

Друга фаза — аутентифікація. У цій фазі виконується взаємна аутентифікація STA і сервера AS, створюються МК і РМК. У цій фазі STA і AP блокують увесь трафік, окрім трафіку 802.1x.

Третя фаза — AS переміщає ключ РМК на AP. Тепер STA і AP володіють дійсними ключами РМК.

Четверта фаза — управління ключами 802.1x. У цій фазі відбувається генерація, прив'язка і верифікація ключа РТК.

П'ята фаза — шифрування і передача даних. Для шифрування використовується відповідна частина РТК.

Стандартом 802.11i передбачений режим PSK (PreShared Key), який дозволяє обійтися без сервера аутентифікації AS. При використанні цього режиму на STA і на AP вручну вводиться PreShared Key, який використовується як РМК. Далі генерація РТК відбувається описаним вище порядком. Режим PSK може використовуватися в невеликих мережах, де недоцільно встановлювати AS.

4.2.5. Стандарти інформаційної безпеки в Інтернеті

За оцінкою Комітету ООН з попередження злочинності і боротьби з нею, комп'ютерна злочинність вийшла на рівень однієї з міжнародних проблем. Тому надзвичайно важливо домагатися ефективного рішення проблем забезпечення комерційної інформації в глобальній мережі Інтернет і суміжних Інтранет мережах, які по своїй технічній суті не мають принципових відмінностей і розрізняються в основному масштабами і відкритістю.

Розглянемо особливості стандартизації процесу забезпечення безпеки комерційної інформації в мережах з протоколом передачі даних IP/TCP і з акцентом на захист телекомунікацій [90].

Забезпечення безпеки IT особливе актуально для відкритих систем комерційного застосування, оброблювальних інформацію обмеженого доступу, що не містить державну таємницю. Під відкритими системами розуміють сукупності всілякого обчислювального і телекомунікаційного устаткування різного виробництва, спільне функціонування якого забезпечується відповідністю вимогам міжнародних стандартів.

Термін «відкриті системи» має на увазі також, що якщо обчислювальна система відповідає стандартам, то вона буде відкрита для взаємозв'язку з будь-якою іншою системою, яка відповідає тим же стандартам. Це, зокрема, відноситься і до механізмів криптографічного захисту інформації або до захисту від НСД до інформації.

Важлива заслуга Інтернету полягає в тому, що він змусив по-новому поглянути на такі технології.

По-перше, Інтернет заохочує застосування відкритих стандартів, доступних для впровадження усім, хто виявить до них цікавість.

По-друге, він є найбільшою і ймовірно, єдиною мережею у світі, до якої підключається така кількість різних комп'ютерів.

І нарешті, Інтернет стає загальноприйнятим засобом представлення швидкозмінюваної нової продукції і нових технологій на світовому ринку.

У Інтернеті вже давно існує ряд комітетів, в основному з організацій, які обережно проводять пропоновані технології через процес стандартизації. Ці

комітети, що становлять основну частину Робочої групи інженерів Інтернету IETF (Internet Engineering Task Force) провели стандартизацію декількох важливих протоколів, прискорюючи їх впровадження в Інтернеті. Безпосередніми результатами зусиль IETF є такі протоколи, як сімейство TCP/IP для передачі даних, SMTP (Simple Mail Transport Protocol) і POP (Post Office Protocol) для електронної пошти, а також SNMP (Simple Network Management Protocol) для управління мережею.

У Інтернеті популярні протоколи безпечної передачі даних, а саме SSL, SET, IPSec. Перераховані протоколи з'явилися в Інтернеті порівняно недавно як необхідність захисту цінної інформації і відразу стали стандартами де-факто.

Протокол SSL (Secure Socket Layer) — популярний мережевий протокол з шифруванням даних для безпечної передачі по мережі. Він дозволяє встановлювати захищене з'єднання, робити контроль цілісності даних і вирішувати різні супутні завдання. Протокол SSL забезпечує захист даних між сервісними протоколами (такими як HTTP, FTP та ін.) і транспортними протоколами (TCP/IP) за допомогою сучасної криптографії. Протокол SSL детально розглянутий в лекції 11.

Протокол SET (Security Electronics Transaction) — перспективний стандарт безпечних електронних транзакцій в мережі Інтернет, призначений для організації електронної торгівлі через мережу Інтернет. Протокол SET заснований на використанні цифрових сертифікатів із стандарту X. 509.

Протокол виконання захищених транзакцій SET є стандартом, розробленим компаніями MasterCard і Visa при значній участі IBM, GlobeSet і інших партнерів. Він дозволяє покупцям придбавати товари через Інтернет, використовуючи захищений механізм виконання платежів.

SET є відкритим стандартним багатостороннім протоколом для проведення безпечних платежів з використанням пластикових карток в Інтернеті. SET забезпечує кросаутентифікацію рахунку утримувача карти, продавця і банку продавця для перевірки готовності оплати, а також цілісність і секретність повідомлення, шифрування цінних і уразливих даних. Тому SET правильніше можна назвати стандартною технологією або системою протоколів виконання безпечних платежів з використанням пластикових карт через Інтернет. SET дозволяє споживачам і продавцям підтверджувати достовірність усіх учасників угоди, що відбувається в Інтернеті, за допомогою криптографії, у тому числі застосовуючи цифрові сертифікати.

Як згадувалося раніше, базовими завданнями захисту інформації є забезпечення її доступності, конфіденційності, цілісності і юридичної значущості. SET, у відмінності від інших протоколів, дозволяє вирішувати вказані завдання захисту інформації в цілому.

Зокрема, він забезпечує наступні спеціальні вимоги захисту операцій електронної комерції:

- секретність даних оплати і конфіденційність інформації замовлення, переданої разом з даними про оплату;
- збереження цілісності цих платежів. Цілісність інформації платежів забезпечується за допомогою цифрового підпису;
- спеціальну криптографію з відкритим ключем для проведення аутентифікації;

- аутентифікацію утримувача по кредитній картці. Вона забезпечується застосуванням цифрового підпису і сертифікатів утримувача карт;
- аутентифікацію продавця і його можливості приймати платежі за пластиковими картками із застосуванням цифрового підпису і сертифікатів продавця;
- аутентифікацію того, що банк продавця є діючою організацією, яка може приймати платежі за пластиковими картками через зв'язок з картковою системою. Аутентифікація банку продавця забезпечується використанням цифрового підпису і сертифікатів банку продавця;
- готовність оплати транзакцій в результаті аутентифікації сертифікату з відкритим ключем для усіх сторін;
- безпека передачі даних за допомогою переважного використання криптографії.

Основна перевага SET в порівнянні з іншими існуючими системами забезпечення інформаційної безпеки полягає у використанні цифрових сертифікатів(стандарт X509, версія 3), які асоціюють утримувача карти, продавця і банк продавця з банківськими установами платіжних систем Visa і Mastercard. Крім того, SET дозволяє зберегти існуючі стосунки між банком, утримувачами карт і продавцями і інтегрується з існуючими системами.

Протокол IPSec. Специфікація IPSec входить в стандарт IP v.6 і є додатковою по відношенню до поточної версії протоколів TCP/IP. Вона розроблена Робочою групою IP Security IETF. Нині IPSec включає 3 алгоритмонезалежних базових специфікації, що представляють відповідні RFC стандарти. Протокол IPSec забезпечує стандартний спосіб шифрування трафіку на мережевому (третьому) рівні IP і захищає інформацію на основі наскрізного шифрування: незалежно від працюючого застосування при цьому шифрується кожен пакет даних, що проходить по каналу. Це дозволяє організаціям створювати в Інтернеті віртуальні приватні мережі. Протокол IPSec детально розглянутий в л. 12.

Інфраструктура управління відкритими ключами PKI (Public Key Infrastructure) призначена для захищеного управління криптографічними ключами електронного документообігу, заснованого на застосуванні криптографії з відкритими ключами. Ця інфраструктура має на увазі використання цифрових сертифікатів, що задовольняють рекомендаціям міжнародного стандарту X. 509 і розгорнутій мережі центрів сертифікації, видачу, що забезпечують, і супровід цифрових сертифікатів для усіх учасників електронного обміну документами. Інфраструктура PKI детально розглядається в л. 13.

4.3. Вітчизняні стандарти безпеки інформаційних технологій

Історично склалося так, що проблеми безпеки IT вивчалися і своєчасно вирішувалися в основному у сфері охорони державної таємниці. Аналогічні завдання комерційного сектора економіки довгий час не знаходили відповідних рішень.

Інформація, що міститься в системах або продуктах IT, є критичним ресурсом, що дозволяє організаціям успішно вирішувати свої завдання. Крім того, приватні особи мають право чекати, що їх персональна інформація, будучи

розміщеною в продуктах або системах ІТ, залишиться приватною, доступною їм в міру необхідності і не зможе бути піддана несанкціонованій модифікації.

Проблема захисту інформації в комерційній АС має свої особливості, які необхідно враховувати, оскільки вони роблять серйозний вплив на інформаційну безпеку (ІБ). Перерахуємо основні з них.

Пріоритет економічних чинників. Для комерційної АС важливо понизити або виключити фінансові втрати і забезпечити отримання прибутку власником і користувачами цього інструментарію в умовах реальних ризиків. Важливою умовою при цьому, зокрема, являється мінімізація типових банківських ризиків (наприклад втрат за рахунок помилкових напрямів платежів, фальсифікації платіжних документів і т. п.).

Відкритість проектування, що передбачає створення підсистеми захисту інформації із засобів, широко доступних на ринку і працюючих у відкритих системах.

Юридична значущість комерційної інформації, яку можна визначити як властивість безпечної інформації, що дозволяє забезпечити юридичну силу електронним документам або інформаційним процесам відповідно до законодавства.

Стандарти в структурі ІБ виступають як сполучна ланка між технічною і концептуальною стороною питання.

Введення в 1999 р. Міжнародного стандарту ISO 15408 в області забезпечення ІБ мало велике значення як для розробників комп'ютерних ІС, так і для їх користувачів. Стандарт ISO 15408-2002 став свого роду гарантією якості і надійності сертифікованих по ньому програмних продуктів. Цей стандарт дозволив споживачам краще орієнтуватися при виборі ПЗ і придбавати продукти, що відповідають їх вимогам безпеки, і, як наслідок цього, підвищив конкурентоспроможність ІТ компаній, що сертифікують свою продукцію відповідно до ISO 15408.

Головні достоїнства 15408:

- повнота вимог до ІБ;
- гнучкість в застосуванні;
- відкритість для подальшого розвитку з урахуванням новітніх досягнень науки і техніки.

Лекція 5 ПРИНЦИПИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Безпека даних означає їх конфіденційність, цілісність і достовірність. Критерії безпеки даних можуть бути визначені таким чином.

Конфіденційність даних припускає їх доступність тільки для тих осіб, які мають на це відповідні повноваження. Під забезпеченням конфіденційності інформації розуміється створення таких умов, при яких зрозуміти зміст передаваних даних може тільки законний одержувач, якому ця інформація призначена.

Цілісність інформації припускає її незмінність в процесі передачі від Відправника до одержувача. Під забезпеченням цілісності інформації розуміється досягнення ідентичності приймаються даних, що відправляються і.

Достовірність інформації припускає відповідність цієї інформації її явному опису і змісту, зокрема, відповідність дійсним характеристикам вказаних: Відправника, часу відправлення і змісту. Забезпечення достовірності інформації, що реалізовується на основі аутентифікації, полягає в достовірному встановленні Відправника, а також захисті інформації від зміни при її передачі від Відправника до одержувача.

Своєчасно виявлене порушення достовірності і цілісності отриманого повідомлення дозволяє запобігти негативним наслідкам, пов'язаним з подальшим використовуваним такого спотвореного повідомлення.

5.1. Основні поняття криптографічного захисту інформації

Криптографія є методологічною основою сучасних систем забезпечення безпеки інформації в комп'ютерних системах і мережах. Історично криптографія(у перекладі з грецького цей термін означає «тайнопис») зародилася як спосіб прихованого передання повідомлень. Криптографія є сукупністю методів перетворення даних, спрямованих на те, щоб захистити ці дані, зробивши їх даремними для незаконних користувачів. Такі перетворення забезпечують рішення трьох головних проблем захисту даних: забезпечення конфіденційності, цілісності і достовірності передаваних або даних, що зберігаються.

Для забезпечення безпеки даних необхідно підтримувати три основні функції:

- захист конфіденційності передаваних або таких, що зберігаються в пам'яті даних;
- підтвердження цілісності і достовірності даних;
- аутентифікацію абонентів при вході в систему і при встановленні з'єднання;

Для реалізації вказаних функцій використовуються криптографічні технології шифрування, цифрового підпису і аутентифікації.

Конфіденційність забезпечується за допомогою алгоритмів і методів симетричного і асиметричного шифрування, а також шляхом взаємної аутентифікації абонентів на основі багаторазових і одноразових паролів, цифрових сертифікатів, смарт карт і т. п.

Цілісність і достовірність передаваних даних зазвичай досягається за допомогою різних варіантів технології електронного підпису, заснованих на односторонніх функціях і асиметричних методах шифрування.

Аутентифікація дозволяє встановлювати з'єднання тільки між легальними користувачами і запобігає доступу до засобів мережі небажаних осіб. Абонентам, що довели свою легальність(автентичність), надаються дозволені види мережевого обслуговування.

Забезпечення конфіденційності, цілісності і достовірності передаваних і даних, що зберігаються, здійснюється передусім правильним використанням криптографічних способів і засобів захисту інформації. Основою більшості криптографічних засобів захисту інформації є шифрування даних.

Під шифром розуміють сукупність процедур і правил криптографічних перетворень, використовуваних для зашифровування і розшифровки інформації по ключу шифрування. Під зашифровуванням інформації розуміється процес перетворення відкритої інформації(початковий текст) в зашифрований текст(шифртекст). Процес відновлення початкового тексту по криптограмі з використанням ключа шифрування називають розшифровкою(дешифруванням).

Узагальнена схема криптосистеми шифрування показана на Рис. 5.1. Початковий текст передаваного повідомлення(чи інформації, що зберігається) M зашифровується за допомогою криптографічного перетворення E_{k_1} з отриманням в результаті шифр тексту C:

$$C = E_{k_1}(M),$$

де k_1 — параметр функції E, що називається ключем шифрування.

Шифртекст C, що називається також криптограмою, містить початкову інформацію M в повному об'ємі, проте послідовність знаків в нім зовні представляється випадковою і не дозволяє відновити початкову інформацію без знання ключа шифрування kt.

Ключ шифрування є тим елементом, за допомогою якого можна варіювати результат криптографічного перетворення. Цей елемент може належати конкретному користувачеві або групі користувачів і являтися для них унікальним. Зашифрована з використанням конкретного ключа інформація може бути розшифрована тільки його власником(чи власниками).

Рис. 5.1. Узагальнена схема криптосистеми шифрування.

Зворотне перетворення інформації виглядає таким чином:

$$M' = D_{k_2}(C).$$

Функція D є зворотною до функції E і робить розшифровку шифртекста. Вона також має додатковий параметр у вигляді ключа к2. Ключ розшифровки к2 повинен однозначно відповідати ключу к1 в цьому випадку отримане в результаті розшифровки повідомлення M' буде еквівалентне M. За відсутності вірного ключа к2 отримати початкове повідомлення M' = M за допомогою функції D неможливо.

Перетворення шифрування може бути симетричним або асиметричним відносно перетворення розшифровки. Відповідно розрізняють два класи криптосистем:

- симетричні криптосистеми(з єдиним ключем);
- асиметричні криптосистеми(з двома ключами).

5.2. Симетричні криптосистеми шифрування

Історично першими з'явилися симетричні криптографічні системи. У симетричній криптосистемі шифрування використовується один і той же ключ для зашифровування і розшифровки інформації. Це означає, що будь-хто, хто має доступ до ключа шифрування, може розшифрувати повідомлення.

Відповідно з метою запобігання несанкціонованому розкриттю зашифрованої інформації усі ключі шифрування в симетричних криптосистемах повинні триматися в секреті. Саме тому симетричні криптосистеми називають криптосистемами з секретним ключем — ключ шифрування має бути доступний тільки тим, кому призначено повідомлення. Симетричні криптосистеми називають ще одноключовими криптографічними системами, або криптосистемами із закритим ключем. Схема симетричної криптосистеми шифрування показана на Рис. 5.2.

Рис. 5.2. Схема симетричної криптосистеми шифрування

Ці криптосистеми характеризуються найбільш високою швидкістю шифрування, і з їх допомогою забезпечуються як конфіденційність і достовірність, так і цілісність передаваної інформації [31]. Конфіденційність передачі інформації за допомогою симетричної криптосистеми залежить від надійності шифру і забезпечення конфіденційності ключа шифрування.

Зазвичай ключ шифрування є файлом або масивом даних і зберігається на персональному ключовому носії, наприклад дискеті або смарткарті; обов'язкове вжиття заходів, що забезпечують недоступність персонального ключового носія комулибо, окрім його власника.

Достовірність забезпечується за рахунок того, що без попередньої розшифровки практично неможливо здійснити смислову модифікацію і підробку

криптографічний закритого повідомлення. Фальшиве повідомлення не може бути правильно зашифроване без знання секретного ключа.

Цілісність даних забезпечується приєднанням до передаваних даних спеціального коду (імітовставки), по секретному ключу. Імітовставка є різновидом контрольної суми, т. е. деякою еталонною характеристикою повідомлення, по якій здійснюється перевірка цілісності останнього. Алгоритм формування імітовставки повинен забезпечувати її залежність за деяким складним криптографічним законом від кожного біта повідомлення. Перевірка цілісності повідомлення виконується одержувачем повідомлення шляхом вироблення по секретному ключу імітовставки, що відповідає отриманому повідомленню, і її порівняння з отриманим значенням імітовставки. При збігу робиться висновок про те, що інформація не була модифікована на шляху від Відправника до одержувача.

Симетричне шифрування ідеально підходить для шифрування інформації «для себе», наприклад, з метою запобігання НСД до неї у відсутність власника. Це може бути як архівне шифрування вибраних файлів, так і прозоре(автоматичне) шифрування цілих логічних або фізичних дисків.

Маючи високу швидкість шифрування, одноключові криптосистеми дозволяють вирішувати багато важливих завдань захисту інформації. Проте автономне використання симетричних криптосистем в комп'ютерних мережах породжує проблему розподілу ключів шифрування між користувачами.

Перед початком обміну зашифрованими даними необхідно обмінятися секретними ключами з усіма адресатами. Передача секретного ключа симетричної криптосистеми не може бути здійснена по загальнодоступних каналах зв'язку, секретний ключ потрібно передавати відправникові і одержувачеві по захищеному каналу. Для забезпечення ефективного захисту циркулюючих в мережі повідомлень потрібне величезне число ключів(один ключ на кожну пару користувачів), що часто міняються. При передачі ключів користувачам необхідно забезпечити конфіденційність, достовірність і цілісність ключів шифрування, що вимагає великих додаткових витрат. Ці витрати пов'язані з необхідністю передачі секретних ключів по закритих каналах зв'язку або розподілом таких ключів за допомогою спеціальної служби доставки, наприклад за допомогою кур'єрів.

Проблема розподілу секретних ключів при великому числі користувачів є дуже трудомістким і складним завданням. У мережі на N користувачів необхідно розподілити N/2 секретних ключів, т. е. число розподілюваних секретних ключів росте за квадратичним законом зі збільшенням числа абонентів мережі.

У розд. 5.6 розглядаються методи, що забезпечують захищений розподіл ключів абонентам мережі.

5.3. Асиметричні криптосистеми шифрування

Асиметричні криптографічні системи були розроблені в 1970х рр. Принципова відмінність асиметричної криптосистеми від криптосистеми симетричного шифрування полягає в тому, що для шифрування інформації і її подальшої розшифровки використовуються різні ключі:

- відкритий ключ До використовується для шифрування інформації, обчислюється з секретного ключа до;

• секретний ключ до використовується для розшифровки інформації, зашифрованої за допомогою парного йому відкритого ключа К.

Ці ключі розрізняються таким чином, що за допомогою обчислень не можна вивести секретний ключ з відкритого ключа К. Тому відкритий ключ До може вільно передаватися по каналах зв'язку.

Асиметричні системи називають також двохключовими криптографічними системами, або криптосистемами з відкритим ключем.

Узагальнена схема асиметричної криптосистеми шифрування з відкритим ключем показана на Рис. 5.3.

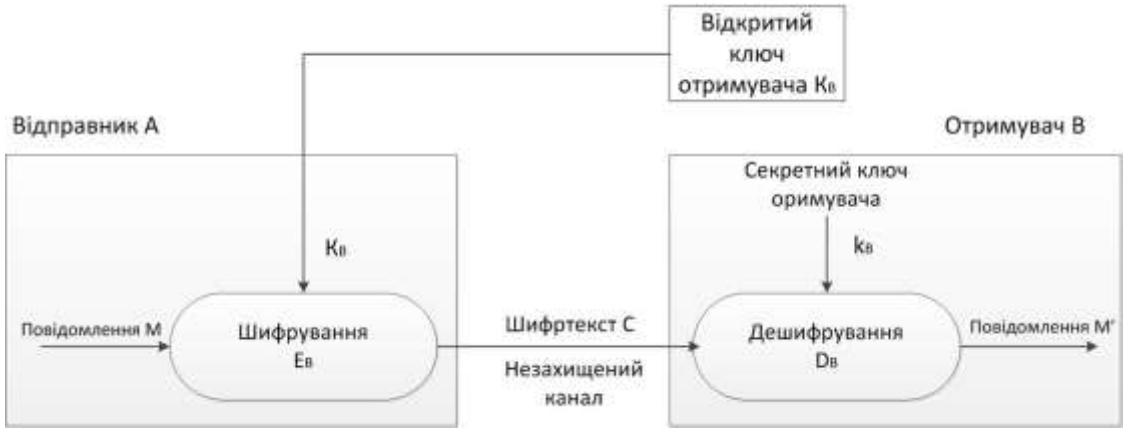

Рис. 5.3. Узагальнена схема асиметричної криптосистеми шифрування

Для криптографічного закриття і подальшої розшифровки передаваної інформації використовується відкритий і секретний ключі одержувача В повідомлення.

Як ключ зашифровування повинен використовуватися відкритий ключ одержувача, а в якості ключа розшифровки — його секретний ключ.

Секретний і відкритий ключі генеруються попарно. Секретний ключ повинен залишатися у його власника і бути надійно захищений від НСД(аналогічно ключу шифрування в симетричних алгоритмах). Копія відкритого ключа повинна знаходитися у кожного абонента криптографічної мережі, з яким обмінюється інформацією власник секретного ключа.

Процес передачі зашифрованої інформації в асиметричній криптосистемі здійснюється таким чином.

Підготовчий етап:

• абонент В генерує пару ключів: секретний ключ кв і відкритий ключ Кв

• відкритий ключ Кв посилається абонентові Л і іншим абонентам(чи робиться доступним, наприклад на ресурсі, що розділяється).

Використання — обмін інформацією між абонентами А і В:

• абонент А зашифровує повідомлення за допомогою відкритого ключа Кв абонента В і відправляє шифртекст абонентові В;

• абонент В розшифровує повідомлення за допомогою свого секретного ключа кв. Ніхто інший(у тому числі абонент А) не може розшифрувати це повідомлення, оскільки не має секретного ключа абонента В. Захист інформації в асиметричній криптосистемі заснована на секретності ключа кв одержувача повідомлення.

Характерні особливості асиметричних криптосистем:

• відкритий ключ Кв і криптограма З можуть бути відправлені по незахищених каналах, т. е. супротивникові відомі Кв і З;

• алгоритми шифрування і розшифровки:

$$E_B : M \to C;$$

$$D_B : C \to M$$

є відкритими.

У. Диффи і М. Хеллман сформулювали вимоги, виконання яких забезпечує безпеку асиметричної криптосистеми [28].

1. Обчислення пари ключів(Кв, кв) одержувачем В має бути простим.

2. Відправник А, знаючи відкритий ключ Кв і повідомлення М, може легко вичислити криптограму

$$C = E_{K_B}(M).$$

3. Одержувач В, використовуючи секретний ключ Кв і криптограму С, може легко відновити початкове повідомлення

$$M = D_{k_B}(C).$$

4. Супротивник, знаючи відкритий ключ Кв, при спробі вичислити секретний ключ Кв натрапляє на непереборну обчислювальну проблему.

5. Супротивник, знаючи пару(Кв, С), при спробі вичислити початкове повідомлення М натрапляє на непереборну обчислювальну проблему.

Концепція асиметричних криптографічних систем з відкритим ключем заснована на застосуванні однонапрямлених функцій. Однонапрямленою функцією називається функція F(X), що має дві властивості:

• існує алгоритм обчислення значень функції

$$y= F(X);$$

• не існує ефективного алгоритму звернення(інвертування) функції F(т. е. не існує рішення рівняння F = Y відносно X).

Як приклад однонапрямленій функції можна вказати цілочисельне множення. Пряме завдання — обчислення твору двох дуже великих цілих чисел Р і Q, т. е. знаходження значення N=P Q — відносно нескладне завдання для комп'ютера.

Зворотне завдання — факторизація, або розкладання на множники великого цілого числа, т. е. знаходження дільників Р і Q великого цілого числа N = P Q, — являється практично нерозв'язною при досить великих значеннях N.

Інший характерний приклад однонапрямленої функції — це модульна експонента з фіксованими основою і модулем [62].

Як і у разі симетричних криптографічних систем, за допомогою асиметричних криптосистем забезпечується не лише конфіденційність, але також достовірність і цілісність передаваної інформації. Достовірність і цілісність будь-якого повідомлення забезпечується формуванням цифрового підпису цього повідомлення і відправкою в зашифрованому виді повідомлення разом з цифровим підписом. Перевірка відповідності підпису отриманому повідомленню після його попередньої розшифровки є перевіркою цілісності і достовірності прийнятого повідомлення. Процедури формування і перевірки електронного цифрового підпису розглянуті в розд. 5.5.

Переваги асиметричних криптографічних систем перед симетричними криптосистемами:

- у асиметричних криптосистемах розв'язана складна проблема розподілу ключів між користувачами, оскільки кожен користувач може згенерувати свою пару ключів сам, а відкриті ключі користувачів можуть вільно публікуватися і поширюватися по мережевих комунікаціях;
- зникає квадратична залежність числа ключів від числа користувачів; у асиметричній криптосистемі число використовуваних ключів пов'язане з числом абонентів лінійною залежністю(у системі з N користувачів використовуються 2N ключів), а не квадратичною, як в симетричних системах;
- асиметричні криптосистеми дозволяють реалізувати протоколи взаємодії сторін, які не довіряють один одному, оскільки при використанні асиметричних криптосистем закритий ключ має бути відомий тільки його власникові.

Недоліки асиметричних криптосистем:

- на сьогодні немає математичного доказу безповоротності використовуваних в асиметричних алгоритмах функцій;
- асиметричне шифрування істотно повільніше за симетричне, оскільки при шифруванні і розшифровці використовуються дуже ресурсоємні операції. З цієї ж причини реалізувати апаратний шифратор з асиметричним алгоритмом істотно складніше, ніж реалізувати апаратно симетричний алгоритм;
- необхідність захисту відкритих ключів від підміни.

5.4. Комбінована криптосистема шифрування

Аналіз розглянутих вище особливостей симетричних і асиметричних криптографічних систем показує, що при спільному використанні вони ефективно доповнюють один одного, компенсуючи недоліки.

Дійсно, головним достоїнством асиметричних криптосистем з відкритим ключем є їх потенційно висока безпека: немає необхідності ні передавати, ні повідомляти комусь значення секретних ключів, ні переконуватися в їх достовірності. Проте їх швидкодія звичайна в сотні(і більше) разів менше швидкодії симетричних криптосистем з секретним ключем.

У свою чергу, швидкодіючі симетричні криптосистеми страждають істотним недоліком: обновлюваний секретний ключ симетричної криптосистеми повинен регулярно передаватися партнерам по інформаційному обміну і під час цих передач виникає небезпека розкриття секретного ключа.

Спільне використання цих криптосистем дозволяє ефективно реалізовувати таку базову функцію захисту, як криптографічне закриття передаваної інформації з метою забезпечення її конфіденційності. Комбіноване застосування симетричного і асиметричного шифрування усуває основні недоліки, властиві обом методам, і дозволяє поєднувати переваги високої секретності, що надаються асиметричними криптосистемами з відкритим ключем, з перевагами високої швидкості роботи, властивими симетричним криптосистемам з секретним ключем.

Метод комбінованого використання симетричного і асиметричного шифрування полягає в наступному.

Симетричну криптосистему застосовують для шифрування початкового відкритого тексту, а асиметричну криптосистему з відкритим ключем застосовують тільки для шифрування секретного ключа симетричної криптосистеми. В результаті асиметрична криптосистема з відкритим ключем не замінює, а лише доповнює симетричну криптосистему з секретним ключем, дозволяючи підвищити в цілому захищеність передаваної інформації. Такий підхід іноді називають схемою електронного «цифрового конверта».

Нехай користувач А хоче використати комбінований метод шифрування для захищеної передачі повідомлення М користувача В.

Тоді послідовність дій користувачів А і У буде наступною.

Дії користувача А:

1. Він створює(наприклад, генерує випадковим чином) сеансовий секретний ключ Ks, який буде використаний в алгоритмі симетричного шифрування для шифрування конкретного повідомлення або ланцюжка повідомлень.
2. Зашифровує симетричним алгоритмом повідомлення М на сеансовому секретному ключі Ks.
3. Зашифровує асиметричним алгоритмом секретний сеансовий ключ Ks на відкритому ключі Кв користувача В(одержувача повідомлення).
4. Передає по відкритому каналу зв'язку на адресу користувача В зашифроване повідомлення М разом із зашифрованим сеансовим КЛЮЧЕМ Kg.

Дії користувача А ілюструються схемою шифрування повідомлення комбінованим методом(Рис. 5.4).

Рис. 5.4. Схема шифрування повідомлення комбінованим методом

Дії користувача В(при отриманні електронного «цифрового конверта» — зашифрованого повідомлення М і зашифрованого сеансового ключа Ks):

5. Розшифровує асиметричним алгоритмом сеансовий ключ Ks за допомогою свого секретного ключа кв.
6. Розшифровує симетричним алгоритмом прийняте повідомлення М за допомогою отриманого сеансового ключа Ks.

Дії користувача В ілюструються схемою розшифровки повідомлення комбінованим методом(Рис. 5.5).

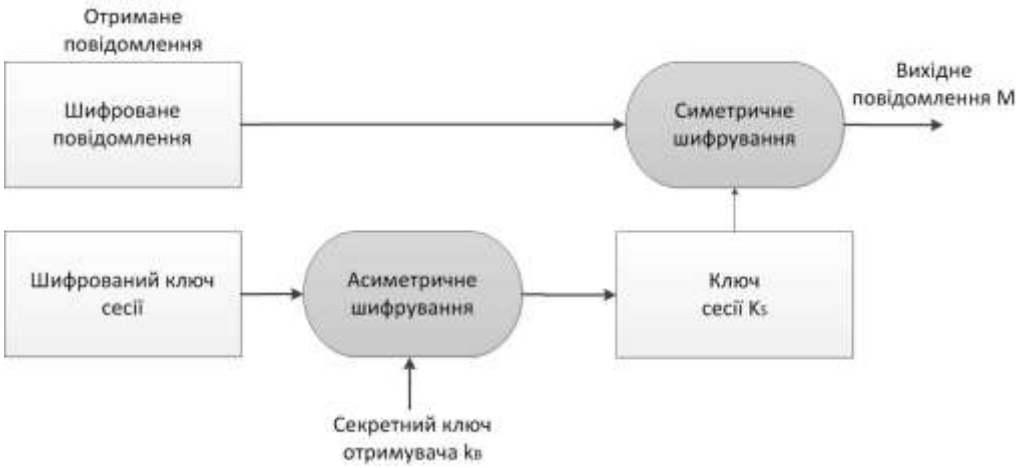

Рис. 5.5. Схема розшифровки повідомлення комбінованим методом

Отриманий електронний «цифровий конверт» може розкрити тільки законний одержувач — користувач В. Тільки користувач В, той, що володіє особистим секретним ключем кв зможе правильно розшифрувати секретний сеансовий ключ Ks і потім за допомогою цього ключа розшифрувати і прочитати отримане повідомлення М.

При методі «цифрового конверта» недоліки симетричного і асиметричного криптоалгоритмов компенсуються таким чином:

- проблема поширення ключів симетричного криптоалгоритма усувається тим, що сеансовий ключ Ks, на якому шифруються власне повідомлення, передається по відкритих каналах зв'язку в зашифрованому виді; для за шифровывания ключа Ks використовується асиметричний криптоалгоритм;
- проблеми повільної швидкості асиметричного шифрування в даному випадку практично не виникає, оскільки асиметричним криптоалгоритмом шифрується тільки короткий ключ Ks, а усі дані шифруються швидким симетричним криптоалгоритмом.

В результаті отримують швидке шифрування у поєднанні із зручним розподілом ключів.

Коли вимагається реалізувати протоколи взаємодії що не довіряють один одному сторін, використовується наступний спосіб взаємодії. Для кожного повідомлення на основі випадкових параметрів генерується окремий секретний ключ симетричного шифрування, який і зашифровується асиметричною системою для передачі разом з повідомленням, зашифрованим цим ключем. В цьому випадку розголошування ключа симетричного шифрування не матиме сенсу, оскільки для за шифрування наступного повідомлення буде використаний інший випадковий секретний ключ.

При комбінованому методі шифрування застосовуються криптографічні ключі як симетричних, так і асиметричних криптосистем. Очевидно, вибір довжин ключів для криптосистеми кожного типу слід здійснювати так, щоб зловмисникові було однаково важко атакувати будь-який механізм захисту комбінованої криптосистеми.

5.5. Електронний цифровий підпис і функція хешування

Електронний цифровий підпис використовується для аутентифікації текстів, що передаються по телекомунікаційних каналах. При такому обміні істотно знижуються витрати на обробку і зберігання документів, прискорюється їх пошук. Але виникає проблема аутентифікації автора електронного документу і самого документу, т. е. встановлення достовірності автора і відсутності змін в отриманому електронному документі.

Метою аутентифікації електронних документів є їх захист від можливих видів зловмисних дій, до яких відносяться:

- активне перехоплення — порушник, що підключився до мережі, перехоплює документи(файли) і змінює їх;
- маскарад — абонент З посилає документ абонентові У від імені абонента А;
- ренегатство — абонент А заявляє, що не посилав повідомлення абонента В, хоча насправді послав;
- підміна — абонент В змінює або формує новий документ і заявляє, що отримав його від абонента А;
- повтор — абонент З повторює раніше переданий документ, який абонент А посилав абонентові В.

Ці види зловмисних дій можуть завдати істотного збитку банківським і комерційним структурам, державним підприємствам і організаціям, приватним особам, що застосовують у своїй діяльності комп'ютерні ИТ.

Проблему перевірки цілісності повідомлення і достовірності автора повідомлення дозволяє ефективно розв'язати методологія електронного цифрового підпису.

5.5.1. Основні процедури цифрового підпису

Функціонально цифровий підпис аналогічний звичайному рукописному підпису і має її основні достоїнства:

- засвідчує, що підписаний текст виходить від особи, що поставила підпис;
- не дає самому цьому обличчю можливості відмовитися від зобов'язань, пов'язаних з підписаним текстом;
- гарантує цілісність підписаного тексту.

Електронний цифровий підпис(ЕЦП) є відносно невеликою кількістю додаткової цифрової інформації, що передається разом з підписуваним текстом.

ЕЦП заснована на оборотності асиметричних шифрів, а також на взаємозв'язаній утримуваного повідомлення, самого підпису і пари ключів. Зміна хоч би одного з цих елементів зробить неможливим підтвердження достовірності цифрового підпису. ЕЦП реалізується за допомогою асиметричних алгоритмів шифрування і Хешфункций.

Технологія застосування системи ЕЦП припускає наявність мережі абонентів, що посилають один одному підписані електронні документи. Для кожного абонента генерується пара ключів: секретний і відкритий. Секретний ключ зберігається абонентом в таємниці і використовується ним для формування ЕЦП.

Відкритий ключ відомий усім іншим користувачам і призначений для перевірки ЕЦП одержувачем підписаного електронного документу.

Система ЕЦП включає дві основні процедури:

- формування цифрового підпису;
- перевірки цифрового підпису.

У процедурі формування підпису використовується секретний ключ Відправника повідомлення, в процедурі перевірки підпису — відкритий ключ Відправника.

Процедура формування цифрового підпису. На підготовчому етапі цієї процедури абонент А — Відправник повідомлення — генерує пару ключів: секретний ключ кА і відкритий ключ КА. Відкритий ключ КА обчислюється з парного йому секретного ключа кА. Відкритий ключ КА розсилається іншим абонентам мережі(чи робиться доступним, наприклад на ресурсі, що розділяється) для використання при перевірці підпису. Для формування цифрового підпису Відправник А передусім

обчислює значення хешфункції h(M) підписуваного тексту М (Рис. 5.6).

Рис. 5.6. Схема формування електронного цифрового підпису

Хешфункція служить для стискування початкового підписуваного тексту М в дайджест т — відносно коротке число, що складається з фіксованого невеликого числа бітів і характеризує увесь текст М в цілому(див. розд. 5.5.2). Далі Відправник А шифрує дайджест т своїм секретним ключем кА. Отримувана при цьому пара чисел є цифровим підписом для цього тексту М. Сполучення разом з цифровим підписом вирушає на адресу одержувача.

Процедура перевірки цифрового підпису. Абоненти мережі можуть перевірити цифровий підпис отриманого повідомлення М за допомогою відкритого ключа КА Відправника цього повідомлення(Рис. 5.7).

При перевірці ЕЦП абонент В — одержувач повідомлення М — розшифровує прийнятий дайджест т відкритим ключем КА Відправника А. Крім того, одержувач сам обчислює за допомогою хешфункції h(M) дайджест т' прийнятого повідомлення М і порівнює його з розшифрованим. Якщо т і т' співпадають, то цифровий підпис є справжнім. Інакше або підпис підроблений, або змінений зміст повідомлення.

Рис. 5.7. Схема перевірки електронного цифрового підпису

Принциповим моментом в системі ЕЦП є неможливість підробки ЕЦП користувача без знання його секретного ключа підписки. Тому необхідно захистити секретний ключ підписки від НСД. Секретний ключ ЕЦП аналогічно ключу симетричного шифрування рекомендується зберігати на персональному ключовому носії в захищеному виді.

Електронний цифровий підпис є унікальним числом, залежним від підписуваного документу і секретного ключа абонента. В якості підписуваного документу може бути використаний будь-який файл. Підписаний файл створюється з непідписаного шляхом додавання в нього одній або більше електронних підписів.

Структура ЕЦП, що поміщається в підписуваний файл(чи в окремий файл електронного підпису), зазвичай містить додаткову інформацію, що однозначно ідентифікує автора підписаного документу. Ця інформація додається до документу до обчислення ЕЦП, що забезпечує і її цілісність. Кожен підпис містить наступну інформацію:

- дату підпису;
- термін закінчення дії ключа цього підпису;
- інформацію про особу, що підписала файл (ПІБ, посада, коротке найменування фірми);
- ідентифікатор того, що підписав(ім'я відкритого ключа);
- власне цифровий підпис.

Важливо відмітити, що з точки зору кінцевого користувача процес формування і перевірки цифрового підпису відрізняється від процесу криптографічного закриття передаваних даних наступними особливостями.

При формуванні цифрового підпису використовуються закритий ключ Відправника, тоді як при зашифровуванні використовується відкритий ключ одержувача. При перевірці цифрового підпису використовується відкритий ключ Відправника, а при розшифровці — закритий ключ одержувача.

Перевірити сформований підпис може будь-яка особа, оскільки ключ перевірки підпису є відкритим. При позитивному результаті перевірки підпису робиться укладення про достовірність і цілісність отриманого повідомлення, т. е. про те, що це повідомлення дійсно відправлено тим або іншим Відправником і не було модифіковано при передачі по мережі.

Проте, якщо користувача цікавить, чи не являється отримане повідомлення повторенням раніше відправленого або чи не було воно затримано на шляху

дотримання, то він повинен перевірити дату і час його відправки, а за наявності — порядковий номер.

Аналогічно асиметричному шифруванню, необхідно забезпечити неможливість підміни відкритого ключа, використовуваного для перевірки ЕЦП. Відкриті ключі ЕЦП можна захистити від підміни за допомогою відповідних цифрових сертифікатів(див. гл. 13).

Сьогодні існує декілька стандартів ЕЦП, наприклад ГОСТ 34.102001.

5.5.2. Функція хешування

Як видно з схеми на Рис. 5.7, в якості початкового значення для обчислення ЕЦП береться не сам електронний документ, а його Хешзначення, або дайджест.

Хешзначення h(M) — це дайджест повідомлення M, т. е. стисле двійкове представлення основного повідомлення M довільної довжини. Хешзначення h(M) формується функцією хешування. Функція хешування(Хешфункція) є перетворенням, на вхід якого подається повідомлення змінної довжини M, а виходом є рядок фіксованої довжини I{M). Інакше кажучи, Хешфункція h( ) приймає як аргумент повідомлення(документ) M довільної довжини і повертає Хешзначення(Хеш) H=h(M) фіксованої довжини(Рис. 5.8).

Рис. 5.8. Схема формування Хеша H = h(M)

Функція хешування дозволяє стиснути підписуваний документ до 128 і більше біт(зокрема до 128 або 256 біт), тоді як M може бути розміром в мегабайт або більше. Слід зазначити, що значення хешфункції h(M) залежить складним чином від документу M і не дозволяє відновити сам документ M.

Функція хешування повинна мати наступні властивості.

1. Хешфункція може бути застосована до аргументу будь-якого розміру.
2. Вихідне значення хешфункції має фіксований розмір.
3. Хешфункцию h(x) досить просто вичислити для будь-якого x. Швидкість обчислення хешфункції має бути такою, щоб швидкість вироблення і перевірки ЕЦП при використанні хешфункції була значно більше, чим при використанні самого повідомлення.
4. Хешфункція має бути чутлива до всіляких змін в тексті M, таким як вставки, викиди, перестановки і т. п.
5. Хешфункція має бути однонапрямленою, т. е. мати властивість безповоротності, інші слова, завдання підбору документу M', який мав би необхідне значення Хеш функції, має бути обчислювально нерозв'язна.
6. Вірогідність того, що значення Хешфункций двох різних документів(незалежно від їх довжин) співпадуть, має бути нікчемно мала; т. е. для будь-кого фіксованого x з обчислювальної точки зору неможливо знайти $x' \neq x$, таке, що $h(x') = h(x)$..

Теоретично можливо, що два різні повідомлення можуть бути стислі (так звана колізія, або «зіткнення»). Тому для забезпечення стійкості функції хешування необхідно уникати зіткнень. Повністю зіткнень уникнути не можна, оскільки в загальному випадку кількість можливих повідомлень перевищує кількість можливих вихідних значень функції хешування. Проте вірогідність зіткнення має бути низькою.

Властивість 5 еквівалентно тому, що /г( ) є односторонньою функцією. Властивість 6 гарантує, що не може бути знайдене інше повідомлення, що дає ту ж свертку. Це запобігає фальсифікації повідомлення.

Таким чином, функція хешування може використовуватися для виявлення змін повідомлення, т. е. може служити для формування криптографічної контрольної суми(що також називається кодом виявлення змін або кодом аутентифікації повідомлення). У цій якості Хешфункція використовується для контролю цілісності повідомлення при формуванні і перевірці ЕЦП.

Хешфункції широко використовуються також для аутентифікації користувачів. У ряді технологій інформаційної безпеки застосовується своєрідний прийом шифрування — шифрування за допомогою односторонньої хешфункції. Своєрідність цього шифрування полягає в тому, що воно по суті є одностороннім, т. е. не супроводжується зворотною процедурою — розшифровкою на приймальній стороні. Обидві сторони(Відправник і одержувач) використовують одну і ту ж процедуру одностороннього шифрування на основі хешфункції [62, 82].

Відомі алгоритми хешування:

- вітчизняний стандарт ГОСТ Р34.ll — 94 [12]. Обчислює Хеш розміром 32 байти;
- MD(Message Digest) — ряд алгоритмів хешування, найбільш поширених у світі. Наприклад, алгоритм MD5 [62, 72] застосовується в останніх версіях Microsoft Windows для перетворення пароля користувача в 16байтное число;
- SHA1(Secure Hash Algorithm) — це алгоритм обчислення дайджеста повідомлень, що виробляє 160битовый Хеш код вхідних даних, широко поширений у світі, використовується у багатьох мережевих протоколах захисту інформації.

Хеш функції широко використовуються також для аутентифікації користувачів.

5.6. Управління криптоключами

Будь-яка криптографічна система заснована на використанні криптографічних ключів. Під ключовою інформацією розуміють сукупність усіх ключів, що діють в інформаційній мережі або системі. Якщо не забезпечено досить надійне управління ключовою інформацією, то, оволодівши нею, зловмисник дістає необмежений доступ до усієї інформації в мережі або системі. Управління ключами включає реалізацію таких функцій, як генерація, зберігання і розподіл ключів. Розподіл ключів — найвідповідальніший процес в управлінні ключами.

При використанні симетричної криптосистеми дві вступаючі в інформаційний обмін сторони повинні спочатку погоджувати секретний сесійний ключ, т. е. ключ для шифрування усіх повідомлень, що передаються в процесі обміну. Цей ключ має бути невідомий усім іншим і повинен періодично

оновлюватися одночасно у Відправника і одержувача. Процес узгодження сесійного ключа називають також обміном або розподілом ключів.

Асиметрична криптосистема припускає використання двох ключів — відкритого і закритого(секретного). Відкритий ключ можна розголошувати, а закритий — слід зберігати в таємниці. При обміні повідомленнями необхідно пересилати тільки відкритий ключ, забезпечивши достовірність відкритого ключа, що пересилається.

До розподілу ключів пред'являються наступні вимоги:

- оперативність і точність розподілу;
- конфіденційність і цілісність розподілюваних ключів.

Для розподілу ключів між користувачами комп'ютерної мережі застосовуються два основні способи [9]:

1) використання одного або декількох центрів розподілу ключів;
2) прямий обмін ключами між користувачами мережі.

Обидва підходи спричиняють за собою деякі проблеми. У першому випадку центру розподілу ключів відомо, кому і які ключі розподілені, і це дозволяє читати усі повідомлення, що передаються по мережі. Можливі зловживання можуть істотно порушити безпеку мережі. У другому — необхідно надійно упевнитися в достовірності суб'єктів мережі.

Завдання розподілу ключів зводиться до побудови такого протоколу розподілу ключів, який забезпечує:

- взаємне підтвердження достовірності учасників сеансу;
- підтвердження достовірності сеансу;
- використання мінімального числа повідомлень при обміні ключами.

Характерним прикладом реалізації першого підходу є система аутентифікації і розподілу ключів Kerberos; вона розглянута в гл. 13.

Зупинимося детальніше на другому підході.

При використанні для захищеного інформаційного обміну криптосистеми з симетричним секретним ключем два користувачі, що бажають обмінятися криптографічний захищеною інформацією, повинні мати загальний секретним ключем. Ці користувачі повинні обмінятися загальним ключем по каналу зв'язку безпечним чином. Якщо користувачі міняють ключ досить часто, то доставка ключа перетворюється на серйозну проблему.

Для вирішення цієї проблеми можливо:

1) використання асиметричної криптосистеми з відкритим ключем для захисту секретного ключа симетричної криптосистеми;
2) використання системи відкритого розподілу ключів Диффи — Хеллмана.

Реалізація першого способу здійснюється у рамках комбінованої криптосистеми з симетричними і асиметричними ключами. При такому підході симетрична криптосистема застосовується для шифрування і передачі початкового відкритого тексту, а асиметрична криптосистема з відкритим ключем застосовується для шифрування, передачі і подальшої розшифровки тільки секретного ключа симетричної криптосистеми.

Другий спосіб заснований на застосуванні алгоритму відкритого розподілу ключів Диффи — Хеллмана, що дозволяє користувачам обмінюватися ключами по незахищених каналах зв'язку.

Метод розподілу ключів Диффи — Хеллмана

У. Диффи і М. Хеллман винайшли метод відкритого розподілу ключів в 1976 р. Цей метод дозволяє користувачам обмінюватися ключами по незахищених каналах зв'язку. Його безпека обумовлена трудністю обчислення дискретних логарифмів в кінцевому полі, на відміну від легкості рішення прямої задачі дискретного піднесення до степеня в тому ж кінцевому полі.

Суть методу Діффі-Хеллмана полягає в наступному(Рис. 5.9).

Користувачі А і В, що беруть участь в обміні інформації, генерують незалежно один від одного свої випадкові секретні ключі кА і кВ (ключі кА і кВ — випадкові великі цілі числа, які зберігаються користувачами А і В в секреті).

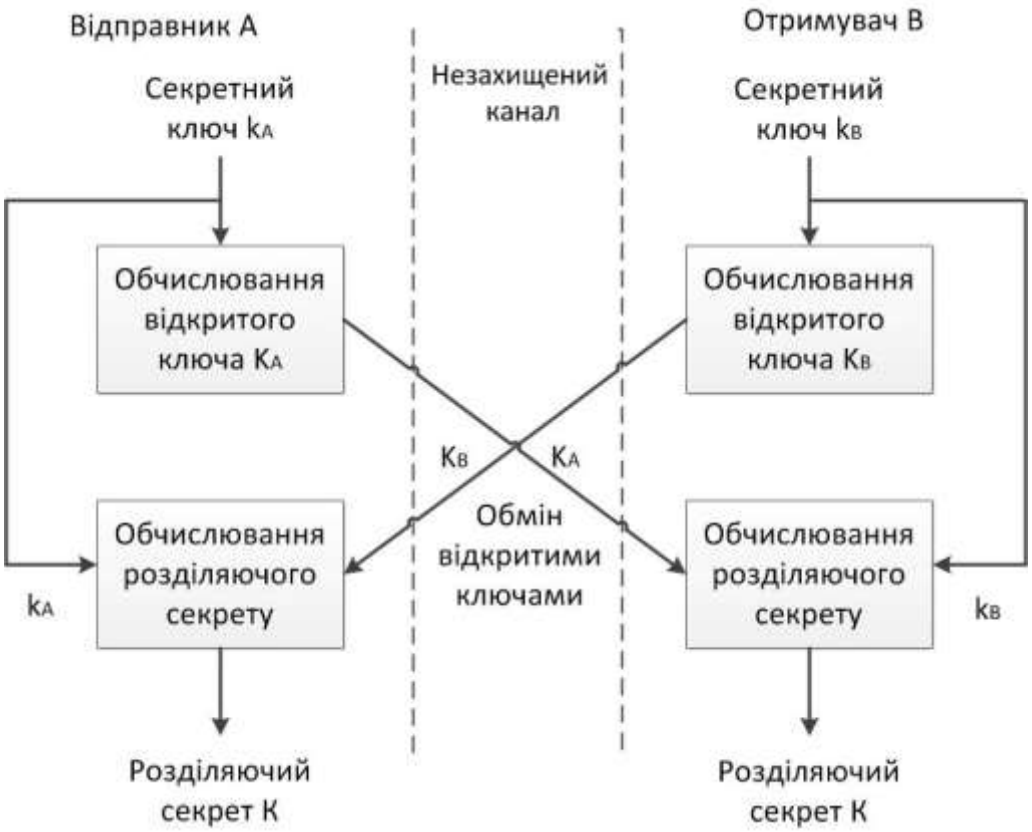

Рис. 5.9 Схема відкритого розподілу ключів Диффи — Хеллмана

Потім користувач А обчислює на підставі свого секретного ключа кА відкритий ключ одночасно користувач В обчислює на підставі свого секретного ключа кВ відкритий ключ.

$$K_A = g^{k_A} \pmod N,$$
$$K_B = g^{k_B} \pmod N,$$

де N і g — великі цілі прості числа. Арифметичні дії виконуються з приведенням по модулю N [62]. Числа N і g можуть не зберігатися в секреті. Як правило, ці значення є загальними для усіх користувачів мережі або системи.

Потім користувачі А і В обмінюються своїми відкритими ключами кА і кВ по незахищеному каналу і використовують їх для обчислення загального сесійного ключа До(секрету, що розділяється):

користувач А: $K = (K_B)^{k_A} \pmod N = (g^{k_B})^{k_A} \pmod N;$

користувач В: $K' = (K_A)^{k_B} \pmod N = (g^{k_A})^{k_B} \pmod N;$

при цьому К = К', оскільки $(g^{k_B})^{k_A} = (g^{k_A})^{k_B} (\mathrm{mod}\ N)$.

Таким чином, результатом цих дій виявляється загальний сесійний ключ, який є функцією обох секретних ключів кА і кв.

Зловмисник, що перехопив значення відкритих ключів КА і Кв, не може вичислити сесійний ключ, тому що він не має відповідних значень секретних ключів кА і кв.

Завдяки використанню однонапрямленої функції, операція обчислення відкритого ключа необратима, т. е. неможливо за значенням відкритого ключа абонента вичислити його секретний ключ.

Унікальність методу Діффі-Хеллмана полягає в тому, що пара абонентів має можливість отримати відоме тільки їм секретне число, передаючи по відкритій мережі відкриті ключі. Після цього абоненти можуть приступити до захисту передаваної інформації вже відомим перевіреним способом — застосовуючи симетричне шифрування з використанням отриманого секрету, що розділяється.

Схема Діффі-Хеллмана дає можливість шифрувати дані при кожному сеансі зв'язки на нових ключах. Це дозволяє не зберігати секрети на дискетах або інших носіях. Не слід забувати, що будь-яке зберігання секретів підвищує вірогідність попадання їх в руки конкурентів або супротивника.

На основі схеми Діффі-Хеллмана функціонує протокол управління криптоключами IKE(Internet Key Exchange), вживаними при побудові захищених віртуальних мереж VPN на мережевому рівні.

Лекція 6 КРИПТОГРАФІЧНІ АЛГОРИТМИ

Більшість засобів захисту інформації базуються на використанні криптографічних шифрів і процедур шифрування/розшифрування. Відповідно до стандарту шифрування ГОСТ 28147-89 під шифром розуміють сукупність оборотних перетворень безлічі відкритих даних на безліч зашифрованих даних, що задаються ключем і алгоритмом криптографічного перетворення [10]. Існує безліч різних криптографічних алгоритмів. Призначення цих алгоритмів — захист інформації. Захищати ж інформацію доводиться від різних загроз і різними способами. Щоб забезпечити надійний і адекватний захист за допомогою криптоалгоритма(КА), треба розуміти, які бувають КА і який тип алгоритму краще пристосований для вирішення конкретного завдання.

6.1. Класифікація криптографічних алгоритмів

Відомі декілька класифікацій криптографічних алгоритмів [50]. Одна з них підрозділяє КА залежно від числа ключів, вживаних в конкретному алгоритмі:

- безключеві КА — не використовують в обчисленнях ніяких ключів;
- одноключеві КА — працюють з одним ключевим параметром(секретним ключем);
- двохключеві КА — на різних стадіях роботи в них застосовуються два ключеві параметри: секретний і відкритий ключі.

Існують детальніші класифікації, одна з яких Приведена на Рис. 6.1.

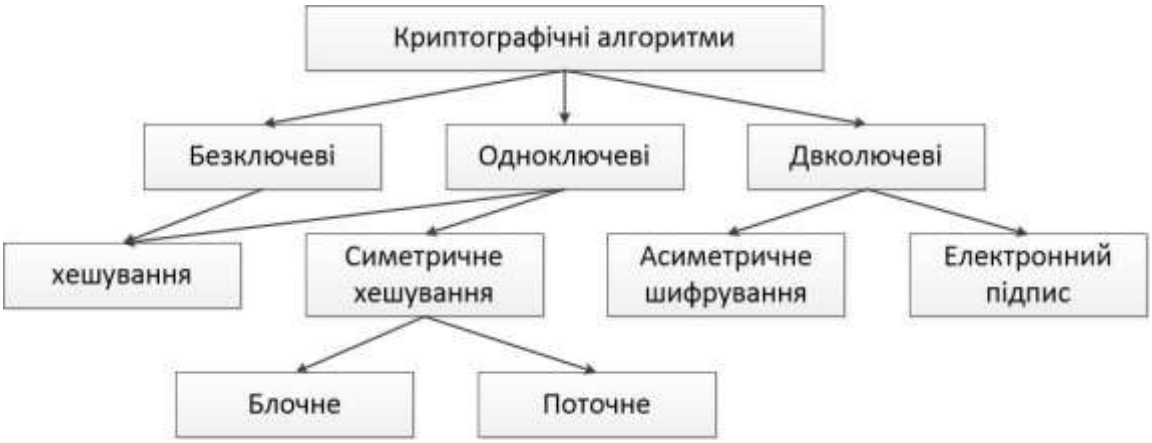

Рис. 6.1. Класифікація криптоалгоритмів захисту інформації

Охарактеризуємо коротко основні типи КА.

Хешування — це метод криптозахисту, що є контрольним перетворенням інформації: з даних необмеженого розміру шляхом виконання криптографічних перетворень обчислюється хеш-значення фіксованої довжини, що однозначно відповідає початковим даним.

Симетричне шифрування використовує один і той же ключ як для зашифровування, так і для розшифрування інформації.

Симетричне шифрування поділяється на два види: блокове і потокове, хоча слід зазначити, що в деяких класифікаціях вони не розділяються і вважається, що потокове шифрування — це шифрування блоків одиничної довжини.

Блокове шифрування характеризується тим, що інформація заздалегідь розбивається на блоки фіксованої довжини(наприклад, 64 або 128 біт). При цьому в різних КА або навіть в різних режимах роботи одного і того ж алгоритму блоки можуть шифруватися як незалежно один від одного, так і «із зчепленням», тобто коли результат шифрування поточного блоку даних залежить від значення попереднього блоку або від результату шифрування попереднього блоку.

Потокове шифрування застосовується, передусім, тоді, коли інформацію неможливо розбити на блоки — скажімо, є деякий потік даних, кожен символ яких вимагається зашифрувати і відправити, не чекаючи інших даних, достатніх для формування блоку. Алгоритми потокового шифрування шифрують дані побітний або посимвольний.

Асиметричне шифрування характеризується застосуванням двох типів ключів: відкритого — для зашифровування інформації і секретного — для її розшифровки. Секретний і відкритий ключі пов'язані між собою досить складним співвідношенням.

Електронний цифровий підпис(ЕЦП) використовується для надійного підтвердження цілісності і авторства даних.

6.2. Симетричні алгоритми шифрування

6.2.1. Основні поняття

У симетричних криптоалгоритмах для зашифровування і розшифровки повідомлення використовується один і той же блок інформації(ключ). Хоча алгоритм дії на передавані дані може бути відомий стороннім особам, але він залежить від секретного ключа, який повинні мати тільки посилач і одержувач. Симетричні криптоалгоритми виконують перетворення невеликого блоку даних(1 біт або 32-128 біт) залежно від секретного ключа таким чином, що прочитати початкове повідомлення можна тільки знаючи цей секретний ключ.

Симетричні криптосистеми дозволяють на основі симетричних криптоалгоритмів кодувати і декодувати файли довільної довжини.

Характерна особливість симетричних блокових криптоалгоритмів — перетворення блоку вхідної інформації фіксованої довжини і отримання результуючого блоку того ж об'єму, але недоступного для прочитання стороннім особам, що не володіють ключем. Схему роботи симетричного блокового шифру можна описати функціями

$$C = E_K(M) \text{ и } M = D_K(C),$$

де М — початковий(відкритий) блок даних, С — зашифрований блок даних.

Ключ К є параметром симетричного блокового криптоалгоритму і є блоком двійкової інформації фіксованого розміру. Початковий М і зашифрований С блоки даних також мають фіксовану розрядність, рівну між собою, але необов'язково рівну довжині ключа К.

Блокові шифри є тією основою, на якій реалізовані практично усі симетричні криптосистеми. Практично усі алгоритми використовують для перетворень певний набір оборотних математичних перетворень.

Методика створення ланцюжків із зашифрованих блоковими алгоритмами байтів дозволяє шифрувати ними пакети інформації необмеженої довжини.

Відсутність статистичної кореляції між бітами вихідного потоку блокового шифру використовується для обчислення контрольних сум пакетів даних і в хешуванні паролів. На сьогодні розроблені досить багато стійких блокових шифрів.

Криптоалгоритм вважається ідеально стійким, якщо для прочитання зашифрованого блоку даних потрібний перебір усіх можливих ключів до тих пір, поки розшифроване повідомлення не виявиться осмисленим. У загальному випадку стійкість блокового шифру залежить тільки від довжини ключа і зростає експоненціально з її зростанням. Ідеально стійкі криптоалгоритми повинні задовольняти ще одній важливій вимозі. Ключ, яким зроблено це перетворення, при відомих початковому і зашифрованому значеннях блоку можна дізнатися тільки шляхом повного перебору його значень.

6.2.2. Блокові алгоритми шифрування даних

Алгоритм шифрування даних DES (Data Encryption Standard) був опублікований в 1977 р. і залишається доки поширеним блоковим симетричним алгоритмом, використовуваним в системах захисту комерційної інформації.

Алгоритм DES побудований відповідно до методології мережі Фейстеля і складається з послідовності перестановок і підстановок, що чергується. Алгоритм DES здійснює шифрування 64бітових блоків даних за допомогою 64 бітового ключа, в якому значущими є 56 біт (інші 8 — перевірочні біти для контролю на парність).

Процес шифрування полягає в початковій перестановці бітів 64бітового блоку, 16 циклах(раундах) шифрування і, нарешті, в кінцевій перестановці бітів(Рис. 6.2).

Рис. 6.2. Узагальнена схема шифрування в алгоритмі DES

Розшифровка в DES є операцією, зворотною шифруванню, і виконується шляхом повторення операцій шифрування в зворотній послідовності.

Основні достоїнства алгоритму DES:

- використовується тільки один ключ завдовжки 56 біт;
- відносна простота алгоритму забезпечує високу швидкість обробки;
- зашифрувавши повідомлення за допомогою одного пакету програм, для розшифровки можна використати будь-який інший пакет програм, що відповідає алгоритму DES;
- крипостійкість алгоритму цілком достатня для забезпечення інформаційної безпеки більшості комерційних застосувань.

Сучасна мікропроцесорна техніка дозволяє за досить прийнятний час зламувати симетричні блокові шифри з довжиною ключа 40 біт. Для такого злому використовується метод повного перебору — тотального випробування усіх можливих значень ключа(метод «грубої сили»). До недавнього часу DES вважався відносно безпечним алгоритмом шифрування.

Існує багато способів комбінування блокових алгоритмів для отримання нових стійкіших алгоритмів. Одним з таких способів є багатократне шифрування — використання блокового алгоритму кілька разів з різними ключами для шифрування одного і того ж блоку відкритого тексту. При триразовому шифруванні можна застосувати три різні ключі.

Алгоритм 3DES (Triple DES — потрійний DES) використовується в ситуаціях, коли надійність алгоритму DES вважається недостатньою.

Сьогодні все ширше використовуються два сучасні криптостійких алгоритми шифрування: вітчизняний стандарт шифрування ГОСТ 28147-89 і новий криптостандарт США — AES (Advanced Encryption Standard).

Стандарт шифрування ГОСТ 28147-89 призначений для апаратної і програмної реалізації, задовольняє криптографічним вимогам і не накладає обмежень на міру секретності інформації, що захищається. Алгоритм шифрування даних, визначуваний ГОСТ 28147-89, є 64бітовий блоковим алгоритмом з 256 бітовим ключем.

Дані, що підлягають шифруванню, розбивають на 64 розрядні блоки. Ці блоки розбиваються на два субблоки N1, і N2 по 32 біт (Рис. 6.3). Субблок N1, обробляється певним чином, після чого його значення складається зі значенням субблоку N2(складання виконується по модулю 2, тобто застосовується логічна операція XOR — що «виключає або»), а потім субблоки міняються місцями. Це перетворення виконується певне число разів(«раундів») — 16 або 32, залежно від режиму роботи алгоритму.

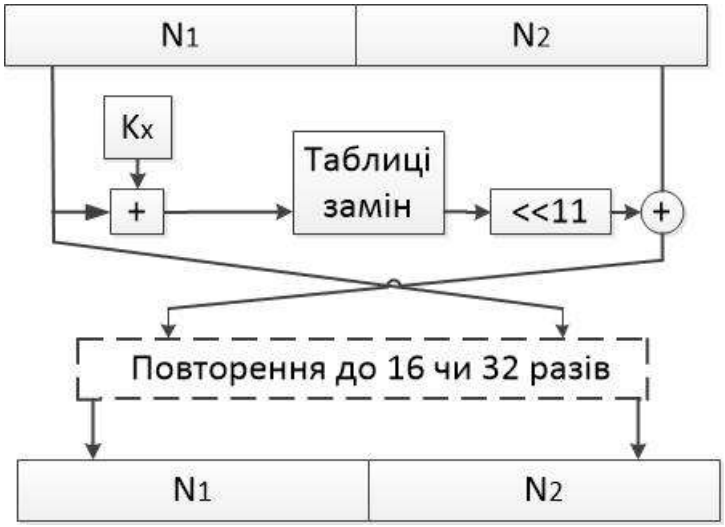

Рис. 6.3. Схема алгоритму ГОСТ 28147-89

У кожному раунді виконуються дві операції.

Перша операція — накладення ключа. Вміст субблоку N1 складається по модулю 2^{32} з 32 бітовою частиною ключа Кх. Повний ключ шифрування представляється у вигляді конкатенації 32 бітових підключів: К0, К1, …К7. В процесі шифрування використовується один з цих підключів — залежно від номера раунду і режиму роботи алгоритму.

Друга операція — таблична заміна. Після накладення ключа субблок N1, розбивається на 8 частин по 4 біт, значення кожної з яких замінюється відповідно до таблиці заміни для цієї частини субблоку. Потім виконується побітове циклічне зрушення субблоку вліво на 11 біт.

Табличні заміни. Блок підстановки S-box (Substitution box) часто використовуються в сучасних алгоритмах шифрування, тому варто пояснити, як організовується подібна операція.

Блок підстановки S-box складається з восьми вузлів заміни(S блоків заміни) S_1, S_2, ..., S_8 з пам'яттю по 64 біт кожен. S 32 бітовий вектор, що поступає на блок підстановки розбивають на 8 4-бітових векторів, що послідовно йдуть, кожен з яких перетвориться в 4-бітовий вектор відповідним вузлом заміни. Кожен вузол заміни можна представити у вигляді таблиці перестановки 16 4-бітових двійкових чисел в діапазоні 0000... 1111. Вхідний вектор вказує адресу рядка в таблиці, а число в цьому рядку є вихідним вектором. Потім 4-бітові вихідні вектори послідовно об'єднують в 32бітовий вектор. Вузли заміни(таблиці перестановки) є ключовими елементами, які є спільними для мережі ЕОМ і рідко змінюються. Ці вузли заміни повинні зберігатися в секреті.

Алгоритм, визначуваний ГОСТ 28147-89, передбачає чотири режими роботи: простої заміни, гамування, гамування із зворотним зв'язком і генерації імітоприставок. У них використовується одне і те ж описане вище шифруюче перетворення, але, оскільки призначення режимів різне, здійснюється це перетворення в кожному з них по-різному.

У режимі простої заміни для зашифровування кожного 64-бітового блоку інформації виконуються 32 описаних

вище за раунд. При цьому 32-бітові підключі використовуються в наступній послідовності:

$K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_0, K_1$ і т. д. у раундах з 1-го по 24-й;

$K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0$ — в раундах з 25-го по 32-й.

Розшифровка в цьому режимі проводиться так само, але з дещо іншою послідовністю застосування підключів:

$K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7$ — в раундах з 1-го по 8-й;

$K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0, K_7, K_6$ і т. д. — в раундах з 9-го по 32-й.

Усі блоки шифруються незалежно один від одного, тобто результат шифрування кожного блоку залежить тільки від його вмісту (відповідного блоку початкового тексту). За наявності декількох однакових блоків початкового(відкритого) тексту блоки шифротексту, що відповідають їм, теж будуть однакові, що дає додаткову корисну інформацію для того, що намагається розкрити шифр криптоаналітика. Тому цей режим застосовується в основному для шифрування самих ключів шифрування(дуже часто реалізуються багатоключеві схеми, в яких по ряду міркувань ключі шифруються один на одному). Для шифрування власне інформації призначені два інші режими роботи — гамування і гамування із зворотним зв'язком.

У режимі гамування кожен блок відкритого тексту побітно складається по модулю 2 з блоком гамми шифру розміром 64 біт. Гамма шифру — це спеціальна послідовність, яка виходить в результаті певних операцій з регістрами N_1 і N_2 (Рис. 6.9):

1. У регістри N_1, і N_2 записується їх початкове заповнення — 64-бітова величина, яка називається синхропосилкою.
2. Виконується зашифровування вмісту регістрів N1 і N2(В даному випадку — синхропосилки) в режимі простої заміни.
3. Вміст регістра N, складається по модулю(2^{32}- 1) з константою $C_1 = 2^{24} + 2^{16} + 2^8 + 2^4$, а результат складання записується в регістр N1.
4. Вміст регістра N2 складається по модулю 232 з константою $C2 = 2^{24} + 2^{16} + 2^8 + 1$, а результат складання записується в регістр N2.
5. Вміст регістрів N_1 і N_2 подається на вихід в якості 64бітового блоку гамми шифру(в даному випадку N_1 і N_2 утворюють перший блок гамми).

Якщо потрібний наступний блок гамми (тобто необхідно продовжити зашифровування або розшифровку), виконується повернення до операції 2.

Для розшифровки гамма виробляється аналогічним чином, а потім до біт зашифрованого тексту і гамми знову застосовується операція XOR. Оскільки ця операція оборотна, у разі правильно виробленої гамми виходить початковий текст (таблиця. 6.1).

Таблиця 6.1. Зашифровування і розшифровка в режимі гамування

	Операція	Результат
Початковий текст		100100
Гамма	XOR	111000
Шифротекст	=	011100
Гамма	XOR	111000
Вихідний текст	=	100100

Для вироблення потрібної для розшифровки гамми шифру у користувача, що розшифровує криптограму, має бути той же ключ і те ж значення синхропосилки, які застосовувалися при зашифровуванні інформації. Інакше отримати початковий текст із зашифрованого не вдасться.

У більшості реалізацій алгоритму ГОСТ 28147-89 синхропосилка не секретна, проте є системи, де синхропосилка такий же секретний елемент, як і ключ шифрування. Для таких систем ефективна довжина ключа алгоритму(256 біт) збільшується ще на 64 біт секретної синхропосилки, яку також можна розглядати як ключовий елемент.

У режимі гамування із зворотним зв'язком для заповнення регістрів N_1 і N_2, починаючи з 2-го блоку, використовується не попередній блок гамми, а результат зашифрування попереднього блоку відкритого тексту(Рис. 6.4). Перший же блок в цьому режимі генерується повністю аналогічно попередньому.

Розглядаючи режим генерації імітоприставок, слід визначити поняття предмета генерації. Імітоприставка — це криптографічна контрольна сума, що обчислюється з використанням ключа шифрування і призначена для перевірки цілісності повідомлень. При генерації імітоприставки виконуються наступні операції: перший 64-бітовий блок масиву інформації, для якого обчислюється імітоприставка, записується в регістри N_1, N_2 і зашифровується в скороченому режимі простої заміни (виконуються перші 16 раундів з 32). Отриманий результат підсумовується по модулю 2 з наступним блоком інформації зі збереженням результату в N_1 і N_2.

Рис. 6.4. Вироблення гамми шифру в режимі гамування із зворотним зв'язком

Цикл повторюється до останнього блоку інформації. Отримане в результаті цих перетворень 64-бітовий вміст регістрів N_1 і N_2 або його частина і називається імітоприставкою. Розмір імітоприставки вибирається, виходячи з необхідної достовірності повідомлень: при довжині імітоприставки г біт вірогідність, що зміна повідомлення залишиться непоміченою, дорівнюватиме 2^{-r}.

Найчастіше використовується 32-бітова імітоприставка, тобто половина вмісту регістрів. Цього вистачає, оскільки, як будь-яка контрольна сума, імітоприставка призначена передусім для захисту від випадкових спотворень інформації. Для захисту ж від умисної модифікації даних застосовуються інші криптографічні методи — в першу чергу електронний цифровий підпис.

При обміні інформацією імітоприставка служить свого роду додатковим коштом контролю. Вона обчислюється для відкритого тексту при зашифровуванні інформації і посилається разом з шифртекстом. Після розшифровки обчислюється

нове значення імітоприставки, яке порівнюється з присланою. Якщо значення не співпадають, означає шифр текст був спотворений при передачі або при розшифровці використовувалися невірні ключі. Особливо корисна імітоприставка для перевірки правильності розшифровки ключової інформації при використанні багатоключових схем.

Алгоритм ГОСТ 28147-89 є дуже стійким алгоритмом — нині для його розкриття не запропоновано ефективніших методів, ніж згаданий вище метод «грубої сили». Його висока стійкість досягається в першу чергу за рахунок великої довжини ключа — 256 біт. При використанні секретної синхропосилки ефективна довжина ключа збільшується до 320 біт, а засекречування таблиці замін додає додаткові біти. Крім того, криптостійкість залежить від кількості раундів перетворень, яких по ГОСТ 28147-89 повинно бути 32(повний ефект розсіювання вхідних даних досягається вже після 8 раундів).

Стандарт шифрування AES. У 1997 р. Американський інститут стандартизації NIST(National Institute of Standards & Technology) оголосив конкурс на новий стандарт симетричного криптоалгоритму AES(Advanced Encryption Standard). До його розробки були підключені найбільші центри криптології всього світу. Переможець цього змагання фактично ставав світовим криптостандартом на найближчі 10-20 років.

До криптоалгоритмам — кандидатів на новий стандарт AES — були пред'явлені наступні вимоги:

- алгоритм має бути симетричним;
- алгоритм має бути блоковим шифром;
- алгоритм повинен мати довжину блоку 128 біт і підтримувати три довжини ключа: 128, 192 і 256 біт.

Додатково розробникам криптоалгоритмів рекомендувалося:

- використати операції, що легко реалізовуються як апаратно(у мікрочіпах), так і програмно(на персональних комп'ютерах і серверах);
- орієнтуватися на 32-розрядні процесори;
- не ускладнювати без необхідності структуру шифру, для того, щоб усі зацікавлені сторони були в змозі самостійно провести незалежний криптоаналіз алгоритму і переконатися, що в ньому не закладені недокументовані можливості.

Підсумки конкурсу були підведені в жовтні 2000 р. — переможцем був оголошений алгоритм Rijndael, розроблений двома криптографами з Бельгії, Вінсентом Риджменом (Vincent Rijmen) і Джоан Даймен (Joan Daemen). Алгоритм Rijndael став новим стандартом шифрування даних AES [91, 92].

Алгоритм AES не схожий на більшість відомих алгоритмів симетричного шифрування, структура яких носить назву «Мережа Фейстеля» і аналогічна російському ГОСТ 28147-89. На відміну від вітчизняного стандарту шифрування, алгоритм AES представляє кожен блок оброблюваних даних у вигляді двомірного байтового масиву розміром 4 x 4, 4 x 6 або 4 x 8 залежно від встановленої довжини блоку (допускається використання декількох фіксованих розмірів шифрованого блоку інформації). Далі на відповідних етапах робляться перетворення або над незалежними стовпцями, або над незалежними рядками, або взагалі над окремими байтами.

Алгоритм AES складається з певної кількості раундів(від 10 до 14 — це залежить від розміру блоку і довжини ключа) і виконує чотири перетворення:

BS (ByteSub) — таблична заміна кожного байта масиву(Рис. 6.5);

SR (ShiftRow) — зрушення рядків масиву(Рис. 6.6). При цій операції перший рядок залишається без змін, а інші циклічно побайтно зрушуються вліво на фіксоване число байт, залежне від розміру масиву. Наприклад, для масиву розміром 4x4 рядки 2, 3 і 4 зрушуються відповідно на 1, 2 і 3 байти;

MC (MixColumn) — операція над незалежними стовпцями масиву(Рис. 6.7), коли кожен стовпець за певним правилом множиться на фіксовану матрицю з(x);

AK (AddRoundKey) — додавання ключа. Кожен біт масиву складається по модулю 2 з відповідним бітом ключа раунду, який у свою чергу певним чином обчислюється з ключа шифрування(Рис. 6.8).

Рис. 6.5. Перетворення BS(ByteSub) використовує таблицю замін(підстановок) для обробки кожного байта масиву State

Рис. 6.6. Перетворення SR(ShiftRow) циклічно зрушує три останніх рядки в масиві State

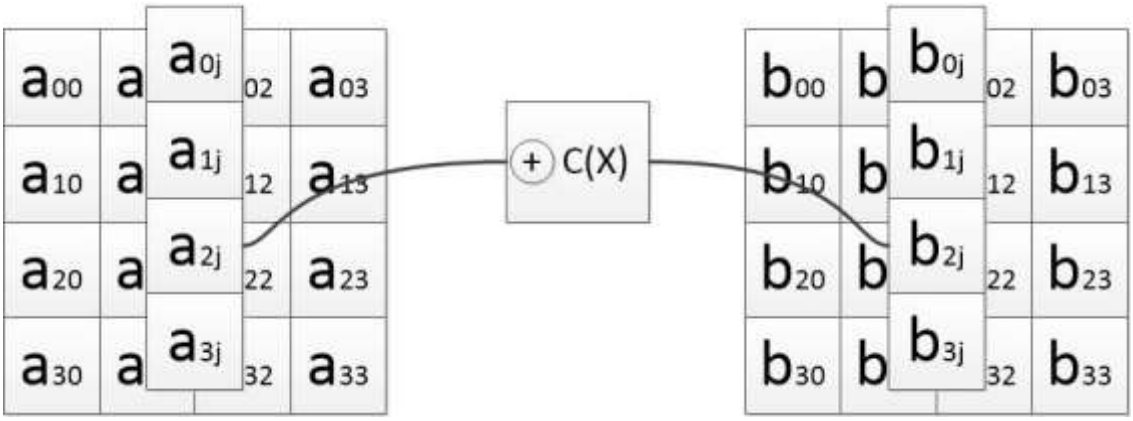

Рис. 6.7. Перетворення MC(MixCoIumn) по черзі обробляє стовпці масиву State

Рис. 6.8. Перетворення АК(AddRoundKey) робить складання XOR кожного стовпця масиву State із словом з ключевого набору

Ці перетворення впливають на масив State, який адресується за допомогою покажчика 'state'. Перетворення AddRoundKey використовує додатковий покажчик для адресації ключа раунду Round Key.

Перетворення BS (ByteSub) є нелінійною байтовою підстановкою, яка впливає незалежно на кожен байт масиву State, використовуючи таблицю замін(підстановок).

У кожному раунді(з деякими виключеннями) над шифрованими даними по черзі виконуються перераховані перетворення(Рис. 6.9). Виключення торкаються першого і останнього раундів: перед першим раундом додатково виконується операція АК, а в останньому раунді відсутній MC.

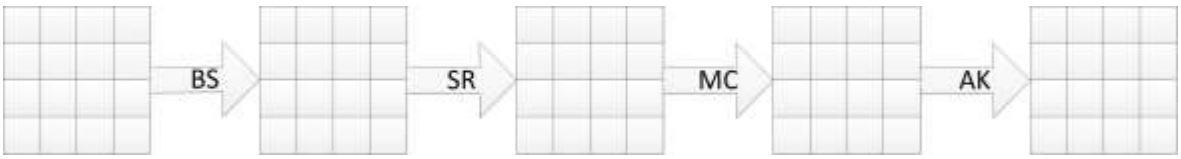

Рис. 6.9. Раунд алгоритму AES

В результаті послідовність операцій при шифруванні виглядає так:

АК, {BS, SR, MC, АК} (повторюється R-1 раз) BS, SR, АК.

Кількість раундів шифрування R в алгоритмі AES змінна(10, 12 або 14 раундів) і залежить від розмірів блоку і ключа шифрування(для ключа також передбачені декілька фіксованих розмірів).

Розшифровка виконується за допомогою наступних зворотних операцій. Виконується звернення таблиці і таблична заміна на інверсній таблиці(відносно вживаною при зашифровуванні). Зворотна операція до SR — це циклічне зрушення рядків управо, а не вліво. Зворотна операція для MC — множення за тими ж правилами на іншу матрицю d(x), що задовольняє умові $c(x) \cdot d(x) = 1$. Додавання ключа АК є зворотним самому собі, оскільки в нім використовується тільки операція XOR. Ці зворотні операції застосовуються при розшифровці в послідовності, обернені до тих, що використовувалася при шифруванні.

Усі перетворення в шифрі AES мають строге математичне обгрунтування. Сама структура і послідовність операцій дозволяють виконувати цей алгоритм ефективно як на 8битних так і на 32битних процесорах. У структурі алгоритму закладена можливість паралельного виконання деяких операцій, що може підняти швидкість шифрування на багатопроцесорних станціях в 4 рази.

Алгоритм AES став новим стандартом шифрування даних завдяки ряду переваг перед іншими алгоритмами. Передусім він забезпечує високу швидкість шифрування на усіх платформах: як при програмній, так і при апаратній реалізації. Крім того, вимоги до ресурсів для його роботи мінімальні, що важливо при його використанні в пристроях, що мають обмежені обчислювальні можливості.

Недоліком алгоритму AES можна вважати лише його нетрадиційну схему. Річ у тому, що властивості алгоритмів, заснованих на «мережі Фейстеля», добре досліджені, а AES, на відміну від них, може містити приховані уразливості, які можуть виявитися тільки після деякого часу з моменту початку його широкого поширення.

Для шифрування даних застосовуються і інші симетричні блокові криптоалгоритми.

Основні режими роботи блокового симетричного алгоритму

Більшість блокових симетричних криптоалгоритмів безпосередньо перетворять 64-бітовий вхідний відкритий текст в 64бітовий вихідний шифрований текст, проте дані рідко обмежуються 64 розрядами.

Щоб скористатися блоковим симетричним алгоритмом для вирішення різноманітних криптографічних завдань, розроблені чотири робочі режими:

- електронна кодова книга ECB (Electronic Code Book);
- зчеплення блоків шифру CBC (Cipher Block Chaining);
- зворотний зв'язок по шифротексту CFB (Cipher Feed Back);
- зворотний зв'язок по виходу OFB (Output Feed Back).

Ці робочі режими спочатку були розроблені для блокового алгоритму DES, але у будь-якому з цих режимів можуть працювати і інші блокові криптоалгоритми.

6.3. Асиметричні криптоалгоритми

Всього за 30 років асиметрична криптографія перетворилася на один з основних напрямів криптології і використовується в IT так само часто, як і симетричні криптосистеми.

6.3.1. Алгоритм шифрування RSA

Криптоалгоритм RSA запропонували в 1978 р. три автори: Р. Райвест (Rivest), А. Шамір (Shamir) і А. Адлеман (Adleman). Алгоритм дістав свою назву по перших буквах прізвищ його авторів. Він став першим алгоритмом з відкритим ключем, який може працювати як в режимі шифрування даних, так і в режимі електронного цифрового підпису [62].

Надійність алгоритму RSA ґрунтується на складності факторизації великих чисел і складності обчислення дискретних логарифмів в кінцевому полі.

У алгоритмі RSA відкритий ключ Кв, секретний ключ кв, повідомлення М і криптограма С належать множині цілих чисел

$$Z_N = \{0,\ 1,\ 2,\ ...,\ N-1\},$$

де N — модуль:

$$N = PQ$$

а P і Q — випадкові великі прості числа. Для забезпечення максимальної безпеки вибирають P і Q рівної довжини і зберігають в таємниці.

Безліч Z_N з операціями додавання і множення по модулю N утворює арифметику по модулю N.

Відкритий ключ Кв вибирають випадковим чином так, щоб виконувалися умови:

$$1 < K_B \le \varphi(N),\ \text{НОД}\ (K_B,\ \varphi(N)) = 1$$

$$\varphi(N) = (P-1)(Q-1),$$

де $\varphi(N)$ — функція Ейлера.

Функція Ейлера $\varphi(N)$ вказує кількість позитивних цілих чисел в інтервалі від 1 до N, які взаємно прості з N.

Друге з вказаних вище умов означає, що відкритий ключ Кв і функція Ейлера $\varphi(N)$ мають бути взаємно простими.

Далі, використовуючи розширений алгоритм Евкліда, обчислюють секретний ключ кв, такий, що

$$k_B \cdot K_B \equiv 1\ (\text{mod}\ \varphi(N))$$

чи

$$k_B = K_B^{-1} (\text{mod}\ (P-1)(Q-1)).$$

Це можна здійснити, оскільки одержувач В знає пару простих чисел (P, Q) і може легко знайти $\varphi(N)$. Помітимо, що кв і N мають бути взаємно простими.

Відкритий ключ Кв використовують для шифрування даних, а секретний ключ кв — для розшифровки.

Процедура шифрування визначає криптограму С через пару (Кв, М) відповідно до наступної формули:

З = ЕКв = Мк'(mod N).

В якості алгоритму швидкого обчислення значення С використовують ряд послідовних зведень в квадрат цілого М і множень на М з приведенням по модулю N.

Розшифровка криптограми С виконують, використовуючи пару(кв, С) по наступній формулі:

$$C = E_{K_в}(M) = M^{K_в} (\text{mod}\ N).$$

Криптоалгоритм RSA усебічно досліджений і визнаний стійким при достатній довжині ключів. Нині довжина ключа — 1024 біта — вважається прийнятним варіантом. Деякі автори стверджують, що із зростанням потужності процесорів криптоалгоритм RSA втратить стійкість до атаки повного перебору. Проте збільшення потужності процесорів дозволить застосувати довші ключі, що підвищує стійкість RSA.

У асиметричній криптосистемі RSA кількість використовуваних ключів пов'язана з кількістю абонентів лінійною залежністю(у системі з N користувачів використовуються 2N ключів), а не квадратичною, як в симетричних системах.

Слід зазначити, що швидкодія RSA істотно нижча швидкодії DES, а програмна і апаратна реалізація криптоалгоритму RSA набагато складніша, ніж DES. Тому криптосистема RSA, як правило, використовується при передачі невеликого об'єму повідомлень.

6.3.2. Алгоритми цифрового підпису

Стандарт цифрового підпису ГОСТ Р 34.10-94 — перший вітчизняний стандарт цифрового підпису — вступив в дію з початку 1995 р. В ньому використовуються наступні параметри:

p — велике просте число завдовжки 509-512 біт або 1020-1024 біт;

q — простий співмножник числа(p-1), що має довжину 254-256 біт;

a — будь-яке число, менше (p-1), причому таке, що $a^q \bmod p = 1$;

x — деяке число, менше q

$y = a^x \bmod p$.

Крім того, цей алгоритм використовує однонапрямлену хешфункцію $H(x)$. ГОСТ Р 34.11-94 визначає хешфункцію, засновану на використанні стандартного симетричного алгоритму ГОСТ 28147-89.

Перші три параметри — p, q і a — є відкритими і можуть бути загальними для усіх користувачів мережі. Число x — секретний ключ, число y — відкритий ключ.

Щоб підписати деяке повідомлення m, а потім перевірити підпис, виконуються наступні кроки.

1. Користувач A генерує випадкове число до, причому $k < q$.
2. Користувач A обчислює значення:

$$r = (a^k \bmod p) \bmod q;$$

$$s = (x \cdot r + k(H(m))) \bmod q.$$

Якщо $H(m) \bmod q = 0$, то значення $H(m) \bmod q$ набувають рівним одиниці. Якщо $r = 0$, то вибирають інше значення до і починають знову.

Цифровий підпис є двома числами:

$$r \bmod 2^{256} \quad \text{и} \quad s \bmod 2^{256}.$$

Користувач A відправляє ці числа користувачеві B.

3. Користувач B перевіряє отриманий підпис, обчислюючи:

$$v = H(m)^{q-2} \bmod q;$$

$$z_1 = (s \cdot v) \bmod q;$$

$$z_2 = ((q - r) \cdot v) \bmod q;$$

$$u = ((a^{z_1} \cdot y^{z_2}) \bmod p) \bmod q$$

Якщо $u = r$, то підпис вважається вірним.

Відмінність між цим алгоритмом і алгоритмом DSA полягає в тому, що в DSA

$$s = (k^{-1}(x \cdot r + (H(m)))) \bmod q$$

що призводить до іншого рівняння верифікації.

Слід також відмітити, що у вітчизняному стандарті ЕЦП параметр q має довжину 256 біт. Західних криптографів цілком влаштовує q довжиною приблизно 160 біт. Відмінність в значеннях параметра q є прагненням розробників вітчизняного стандарту до отримання безпечнішого підпису.

Новий вітчизняний стандарт цифрового підпису ГОСТ Р 34.10-2001 був прийнятий в 2001 р. Його принципова відмінність від попереднього ГОСТ Р 34.10-

94 полягає в тому, що усі обчислення при генерації і перевірці ЕЦП в новому алгоритмі робляться в групі точок еліптичної кривої, визначеної над кінцевим полем F_p,. Приналежність точки (пари чисел x і y) до цієї групи визначається наступним співвідношенням:

$$y^2 \equiv x^3 + ax + b \bmod p$$

де модуль системи p є простим числом, великим 3, а коефіцієнти a і b є константами, що задовольняють наступним співвідношенням:

$$a < p,\ b < p;$$

$$4a^3 + 27b^2 \neq 0 \bmod p.$$

Подальші математичні подробиці можна знайти в [17, 62]. Слід зазначити, що принципи обчислень по цьому алгоритму аналогічні використаним в ГОСТ Р 34.10-94. Спочатку генерується випадкове число x, з його допомогою обчислюється r-частина ЕЦП, потім обчислюється s частина ЕЦП з r-частини, значення x, значення секретного ключа і хешзначення підписуваних даних.

При перевірці ж підпису аналогічним чином перевіряється відповідність певним співвідношенням r, s, відкритого ключа і хешзначення інформації, підпис якої перевіряється. Підпис вважається невірним, якщо співвідношення не дотримуються.

У перспективі криптосистеми на основі еліптичних кривих, ймовірно, витіснять існуючі алгоритми ЕЦП, асиметричного шифрування і вироблення ключів парного зв'язку(ключ для шифрування інформації між двома конкретними користувачами обчислюється з секретного ключа відправника інформації і відкритого ключа одержувача). Алгоритми на базі еліптичних кривих дозволяють помітно скоротити час обчислень без втрат криптостійкості або відповідно збільшити рівень зашиті при тих же тимчасових витратах.

Вітчизняний стандарт хешування ГОСТ Р 34.11-94

Вітчизняним стандартом генерування хешфункції є алгоритм ГОСТ Р 34.11-94. Коротко цей алгоритм хешування можна описати таким чином (Рис. 6.10) [12].

Рис. 6.10. Хешування по алгоритму ГОСТ Р 34.11-94

Крок 1. Ініціалізація регістра хешзначення. Якщо довжина повідомлення не перевищує 256 біт — перехід до кроку 3, якщо перевищує - перехід до кроку 2.

Крок 2. Ітеративне обчислення хешзначення блоків хешуємих даних по 256 біт з використанням того, що зберігається в регістрі хешзначення попереднього блоку. Обчислення включає наступні дії:

- генерацію ключів шифрування на основі блоку хешируемих даних;
- зашифровування того, що зберігається в регістрі хешзначення у вигляді чотирьох блоків по 64 біта по алгоритму ГОСТ 28147-89 в режимі простої заміни;
- перемішування результату.

Обчислення робиться до тих пір, поки довжина необроблених вхідних даних не стане менше або рівною 256 біт. В цьому випадку — перехід до кроку 3.

Крок 3. Доповнення бітовими нулями необробленої частини повідомлення до 256 біт. Обчислення хеш-значення аналогічно кроку 2. В результаті в регістрі опиняється шукане хеш-значення.

Лекція 7 ТЕХНОЛОГІЇ АУТЕНТИФІКАЦІЇ

Застосування відкритих каналів передачі даних створює потенційні можливості для дій зловмисників (порушників). Тому одним з важливих завдань забезпечення інформаційної безпеки при взаємодії користувачів є використання методів і засобів, що дозволяють одній (перевіряючій) стороні переконатися в достовірності іншої (що перевіряється) сторони. Зазвичай для вирішення цієї проблеми застосовуються спеціальні прийоми, що дають можливість перевірити достовірність сторони, що перевіряється.

7.1. Аутентифікація, авторизація і адміністрування дій користувачів

З кожним зареєстрованим в комп'ютерній системі суб'єктом (користувачем або процесом, що діє від імені користувача) пов'язана деяка інформація, що однозначно ідентифікує його. Це може бути число або рядок символів, що іменують цей суб'єкт. Цю інформацію називають ідентифікатором суб'єкта. Якщо користувач має ідентифікатор, зареєстрований в мережі, він вважається легальним (законним) користувачем; інші користувачі відносяться до нелегальних користувачів. Перш ніж отримати доступ до ресурсів комп'ютерної системи, користувач повинен пройти процес первинної взаємодії з комп'ютерною системою, який включає ідентифікацію і аутентифікацію.

Ідентифікація (Identification) — процедура розпізнавання користувача по його ідентифікатору (імені). Ця функція виконується, коли користувач робить спробу увійти до мережі. Користувач повідомляє систему по її запиту свій ідентифікатор, і система перевіряє у своїй базі даних його наявність.

Аутентифікація (Authentication) — процедура перевірки достовірності заявленого користувача, процесу або пристрою. Ця перевірка дозволяє достовірно переконатися, що користувач (процес або пристрій) є саме тим, ким себе оголошує. При проведенні аутентифікації перевіряюча сторона переконується в достовірності сторони, що перевіряється, сторона, що при цьому перевіряється, теж активно бере участь в процесі обміну інформацією. Зазвичай користувач підтверджує свою ідентифікацію, вводячи в систему унікальну, не відому іншим користувачам інформацію про себе (наприклад, пароль або сертифікат).

Ідентифікація і аутентифікація є взаємозв'язаними процесами розпізнавання і перевірки достовірності суб'єктів (користувачів). Саме від них залежить подальше рішення системи: чи можна дозволити доступ до ресурсів системи конкретному користувачеві або процесу. Після ідентифікації і аутентифікації суб'єкта виконується його авторизація.

Авторизація (Authorization) — процедура надання суб'єктові певних повноважень і ресурсів в цій системі. Іншими словами, авторизація встановлює сферу його дії і доступні йому ресурси. Якщо система не може надійно відрізнити авторизовану особу від неавторизованої, то конфіденційність і цілісність інформації в цій системі можуть бути порушені. Організації необхідно чітко визначити свої вимоги до безпеки, щоб приймати рішення про відповідні межі авторизації.

З процедурами аутентифікації і авторизації тісно пов'язана процедура адміністрування дій користувача.

Адміністрування (Accounting) — реєстрація дій користувача в мережі, включаючи його спроби доступу до ресурсів. Хоча ця облікова інформація може бути використана для виписування рахунку, з позицій безпеки вона особливо важлива для виявлення, аналізу інцидентів безпеки в мережі і відповідного реагування на них. Записи в системному журналі, аудиторські перевірки і ПЗ accounting — усе це може бути використано для забезпечення підзвітності користувачів, якщо щось станеться при вході в мережу з їх ідентифікатором.

Необхідний рівень аутентифікації визначається вимогами безпеки, які встановлені в організації. Загальнодоступні Webсервери можуть дозволити анонімний або гостьовий доступ до інформації. Фінансові транзакції можуть зажадати строгої аутентифікації. Прикладом слабкої форми аутентифікації може служити використання IPадреса для визначення користувача. Підміна (spoofing) IPадреса може легко зруйнувати механізм аутентифікації. Надійна аутентифікація є тим ключовим чинником, який гарантує, що тільки авторизовані користувачі отримають доступ до контрольованої інформації.

При захисті каналів передачі даних повинна виконуватися взаємна аутентифікація суб'єктів, тобто взаємне підтвердження достовірності суб'єктів, що зв'язуються між собою по лініях зв'язку. Процедура підтвердження достовірності виконується зазвичай на початку сеансу встановлення з'єднання абонентів. Термін «з'єднання» вказує на логічний зв'язок (потенційно двосторонній) між двома суб'єктами мережі. Мета цієї процедури — забезпечити упевненість, що з'єднання встановлене із законним суб'єктом і уся інформація дійде до місця призначення.

Для підтвердження своєї достовірності суб'єкт може пред'являти системі різні сутності. Залежно від сутностей, що пред'являються суб'єктом, процеси аутентифікації можуть бути розділені на основі:

- знання чогось Прикладами можуть служити пароль, персональний ідентифікаційний код PIN (Personal Identification Number), а також секретні і відкриті ключі, знання яких демонструється в протоколах типу запит-відповідь;
- володіння чимось. Звичайно це магнітні карти, смарт карти, сертифікати і облаштування touch memory
- якихось невід'ємних характеристик. Ця категорія включає методи, що базуються на перевірці біометричних характеристик користувача (голосу, райдужної оболонки і сітківки ока, відбитків пальців, геометрії долоні та ін.). У цій категорії не використовуються криптографічні методи і засоби. Аутентифікація на основі біометричних характеристик застосовується для контролю доступу в приміщення або до будь-якої техніки [9, 54].

Пароль — це те, що знає користувач і інший учасник взаємодії. Для взаємної аутентифікації учасників взаємодії може бути організований обмін паролями між ними.

Персональний ідентифікаційний номер PIN (Personal Identification Number) є випробуваним способом аутентифікації утримувача пластикової карти і смарткарти. Секретне значення PIN-кода має бути відоме тільки утримувачеві карти.

Динамічний (одноразовий) пароль — це пароль, який після одноразового застосування ніколи більше не використовується. На практиці зазвичай використовується значення, що регулярно міняється, яке базується на постійному паролі або ключовій фразі.

Система запит-відповідь. Одна із сторін ініціює аутентифікацію за допомогою посилки іншій стороні унікального і непередбачуваного значення «запит», а інша сторона посилає відповідь, вичислену за допомогою «запиту» і секрету. Оскільки обидві сторони володіють одним секретом, то перша сторона може перевірити правильність відповіді другої сторони.

Сертифікати і цифрові підписи. Якщо для аутентифікації використовуються сертифікати, то потрібно застосування цифрових підписів на цих сертифікатах. Сертифікати видаються відповідальною особою в організації користувача, сервером сертифікатів або зовнішньою довіреною організацією. У рамках Інтернету з'явилися комерційні інфраструктури управління відкритими ключами PKI (Public Key Infrastructure) для поширення сертифікатів відкритих ключів. Користувачі можуть отримати сертифікати різних рівнів.

Процеси аутентифікації можна також класифікувати по рівню забезпечуваної безпеки [9, 54]. Відповідно до цього процеси аутентифікації розділяються на наступні типи:

- аутентифікація, що використовує паролі і PINкоди;
- строга аутентифікація на основі використання криптографічних методів і засобів;
- біометрична аутентифікація користувачів.

З точки зору безпеки кожен з перерахованих типів сприяє рішенню своїх специфічних завдань, тому процеси і протоколи аутентифікації активно використовуються на практиці.

Основні атаки на протоколи аутентифікації:

- маскарад (impersonation). Користувач видає себе за іншого з метою отримання повноважень і можливості дій від імені іншого користувача;
- підміна сторони аутентифікаційного обміну (interleaving attack). Зловмисник в ході цієї атаки бере участь в процесі аутентифікаційного обміну між двома сторонами з метою модифікації трафіку, що проходить через нього;
- повторна передача (replay attack) полягає в повторній передачі аутентифікаційних даних будь-ким користувачем;
- примусова затримка (forced delay). Зловмисник перехоплює деяку інформацію і передає її через деякий час;
- атака з вибіркою тексту (chosentext attack). Зловмисник перехоплює аутентифікаційний трафік і намагається отримати інформацію про довготривалі криптографічні ключі.

Для запобігання таким атакам при побудові протоколів аутентифікації застосовуються:

- використання механізмів типу «запит-відповідь», «відмітка часу», випадкових чисел, ідентифікаторів, цифрових підписів;
- прив'язка результату аутентифікації до подальших дій користувачів у рамках системи. Прикладом подібного підходу може служити здійснення в процесі аутентифікації обміну секретними сеансовими ключами, які використовуються при подальшій взаємодії користувачів;
- періодичне виконання процедур аутентифікації у рамках вже встановленого сеансу зв'язку і т. п.

Механізм «запит-відповідь» полягає в наступній. Якщо користувач А хоче бути упевненим, що повідомлення, що отримуються їм від користувача В, не є

неправдивими, він включає в відправлене для В повідомлення непередбачуваний елемент — запит X (наприклад, деяке випадкове число). При відповіді користувач В повинен виконати над цим елементом деяку операцію (наприклад, вичислити деяку функцію f (X)). Це неможливо здійснити заздалегідь, оскільки користувачеві В невідомо, яке випадкове число X прийде в запиті. Отримавши відповідь з результатом дій В, користувач А може бути упевнений, що В - справжній. Недолік цього методу — можливість встановлення закономірності між запитом і відповіддю.

Механізм «відмітка часу» має на увазі реєстрацію часу для кожного повідомлення. В цьому випадку кожен користувач мережі визначає, наскільки повідомлення, що «застаріло» прийшло, і вирішує не приймати його, оскільки воно може бути неправдивим.

У обох випадках для захисту механізму контролю слід застосовувати шифрування, щоб бути упевненим, що відповідь послана не зловмисником.

При використанні відміток часу виникає проблема допустимого тимчасового інтервалу затримки для підтвердження достовірності сеансу: сполучення з «тимчасовим штемпелем» в принципі не може бути передане миттєво. Крім того, комп'ютерний годинник одержувача і відправника не може бути абсолютно синхронізований.

При порівнянні і виборі протоколів аутентифікації необхідно враховувати наступні характеристики:

- наявність взаємної аутентифікації. Ця властивість відображає необхідність обопільної аутентифікації між сторонами аутентифікаційного обміну;
- обчислювальну ефективність. Це кількість операцій, необхідних для виконання протоколу;
- комунікаційну ефективність. Це властивість відображає кількість повідомлень і їх довжину, необхідну для здійснення аутентифікації;
- наявність третьої сторони. Прикладом третьої сторони може служити довірений сервер розподілу симетричних ключів або сервер, що реалізовує дерево сертифікатів для розподілу відкритих ключів;
- гарантії безпеки. Прикладом може служити застосування шифрування і цифрового підпису [9, 54].

7.2. Методи аутентифікації, що використовують паролі і PINкоди

Однією з поширених схем аутентифікації є проста аутентифікація, яка заснована на застосуванні традиційних багаторазових паролів з одночасним узгодженням засобів його використання і обробки. Аутентифікація

на основі багаторазових паролів — простий і наочний приклад використання інформації, що розділяється. Поки у більшості захищених віртуальних мереж VPN (Virtual Private Network) доступ клієнта до сервера дозволяється по паролю. Проте все частіше застосовуються ефективніші засоби аутентифікації, наприклад програмні і апаратні системи аутентифікації на основі одноразових паролів, смарткарт, PINко дов і цифрових сертифікатів.

7.2.1. Аутентифікація на основі багаторазових паролів

Базовий принцип «єдиного входу» припускає достатність одноразового проходження користувачем процедури аутентифікації для доступу до усіх мережевих ресурсів. Тому в сучасних операційних системах передбачається централізована служба аутентифікації, яка виконується одним з серверів мережі і використовує для своєї роботи базу даних (БД). У цій БД зберігаються облікові дані про користувачів мережі, що включають ідентифікатори і паролі користувачів, а також іншу інформацію [45].

Процедуру простої аутентифікації користувача в мережі можна представити таким чином. Користувач при спробі логічного входу в мережу набирає свої ідентифікатор і пароль. Ці дані поступають для обробки на сервер аутентифікації. У БД, що зберігається на сервері аутентифікації, по ідентифікатору користувача знаходиться відповідний запис. З неї витягається пароль і порівнюється з тим паролем, який ввів користувач. Якщо вони співпали, то аутентифікація пройшла успішно — користувач отримує легальний статус і отримує ті права і ресурси мережі, які визначені для його статусу системою авторизації.

У схемі простої аутентифікації (Рис. 7.1) передача пароля і ідентифікатора користувача може робитися наступними способами [9]:

- у незашифрованому виді; наприклад, згідно з протоколом парольної аутентифікації PAP (Password Authentication Protocol) паролі передаються по лінії зв'язку у відкритій незахищеній формі;

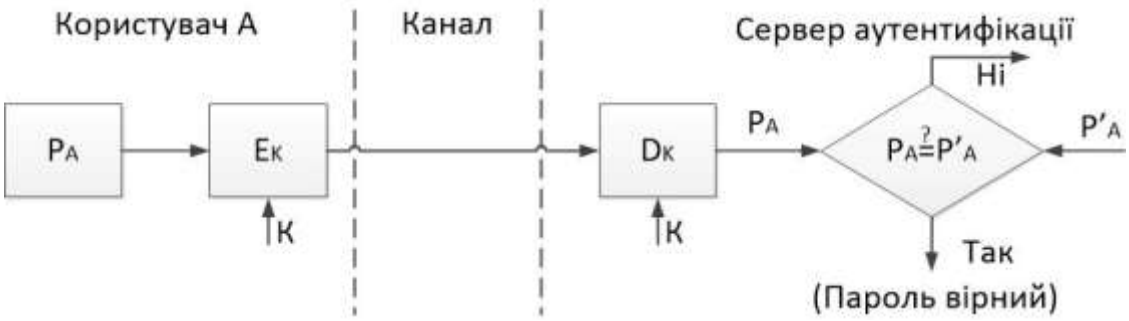

Рис. 7.1. Проста аутентифікація з використанням пароля

- у захищеному виді; усі передавані дані (ідентифікатор і пароль користувача, випадкове число і мітки часу) захищені за допомогою шифрування або однонапрямленої функції.

Очевидно, що варіант аутентифікації з передачею пароля користувача в незашифрованому виді не гарантує навіть мінімального рівня безпеці, оскільки схильний до численних атак і легко компрометується. Щоб захистити пароль, його треба зашифрувати перед пересилкою по незахищеному каналу. Для цього в схему включені засоби шифрування і розшифровки DK, керовані секретним ключем К., що розділяється, Перевірка достовірності користувача заснована на порівнянні присланого користувачем пароля РА і початкового значення Р'л, що зберігається на сервері аутентифікації. Якщо значення РА і Р'А співпадають, то пароль Р вважається справжнім, а користувач А — законним.

Схеми організації простої аутентифікації відрізняються не лише методами передачі паролів, але і видами їх зберігання і перевірки. Найбільш поширеним способом являється зберігання паролів користувачів у відкритому виді в системних

файлах, причому на ці файли встановлюються атрибути захисту від читання і запису (наприклад, за допомогою опису відповідних привілеїв в списках контролю доступу ОС). Система зіставляє введений користувачем пароль із записом, що зберігається у файлі паролів. При цьому способі не використовуються криптографічні механізми, такі як шифрування або однонапрямлені функції. Очевидним недоліком цього способу є можливість отримання зловмисником в системі привілеїв адміністратора, включаючи права доступу до системних файлів, і зокрема, до файлу паролів.

Для забезпечення надійного захисту ОС пароль кожного користувача має бути відомий тільки цьому користувачеві і нікому іншому, у тому числі і адміністраторам системи. На перший погляд те, що адміністратор знає пароль деякого користувача, не відображається негативно на безпеці системи, оскільки адміністратор, увійшовши до системи від імені звичайного користувача, отримує права менші ніж ті, які він отримає, зайшовши в систему від свого імені. Проте, входячи в систему від імені іншого користувача, адміністратор дістає можливість обходити систему аудиту, а також здійснювати дії, компрометуючі цього користувача, що неприпустимо в захищеній системі. Таким чином, паролі користувачів не повинні зберігатися в ОС у відкритому виді.

З точки зору безпеки переважним є метод передачі і зберігання паролів з використанням односторонніх функцій. Зазвичай для шифрування паролів в списку користувачів використовують одну з відомих криптографічний стійких хешфункцій. У списку користувачів зберігається не сам пароль, а образ пароля, що є результатом застосування до пароля хешфункції.

Однонаправленість хешфункції не дозволяє відновити пароль по образу пароля, але дозволяє, вичисливши хеш функцію, отримати образ введеного користувачем пароля і таким чином перевірити правильність введеного пароля. У простому випадку як хешфункції використовується результат шифрування деякої константи на паролі.

Наприклад, одностороння функція h ( ) може бути визначена таким чином:

$$h = E_p (ID)$$

де P — пароль користувача; ID — ідентифікатор користувача; E_P — процедура шифрування, що виконується з використанням пароля P в якості ключа.

Такі функції зручні, якщо довжина пароля і ключа однакові. В цьому випадку перевірка достовірності користувача A за допомогою пароля P_A складається з пересилки серверу аутентифікації відображення $h(P_A)$ і порівняння його із заздалегідь вичисленим і таким, що зберігається у БД сервера аутентифікації еквівалентом h (Рис. 7.2). Якщо відображення $h(P_A)$ і $h'(P_A)$ рівні, то вважається, що користувач успішно пройшов аутентифікацію.

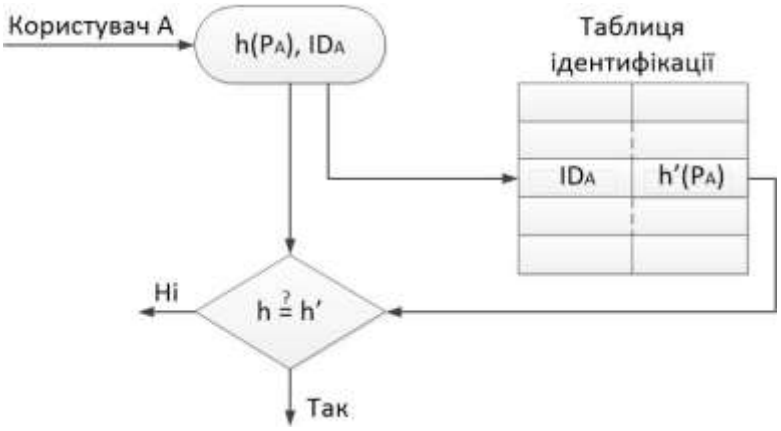

Рис. 7.2. Використання односторонньої функції для перевірки пароля

На практиці паролі складаються лише з декількох символів, щоб дати можливість користувачам запам'ятати їх. Короткі паролі уразливі до атаки повного перебору усіх варіантів. Для того, щоб запобігти такій атаці, функції I (P) можна визначити інакше, наприклад у виді:

$$h(P) = E_{P \oplus K}(ID)$$

де K і ID — відповідно ключ і ідентифікатор відправника.

Розрізняють дві форми представлення об'єктів, аутентифікуючих користувача:

- зовнішній аутентифікуючий об'єкт, що не належить системі;
- внутрішній об'єкт, що належить системі, в який переноситься інформація із зовнішнього об'єкту.

Зовнішні об'єкти можуть бути представлені на різних носіях інформації: пластикових картах, смарткартах, гнучких магнітних дисках і т. п. Природно, що зовнішня і внутрішня форми представлення аутентифікуючого об'єкту мають бути семантично тотожні.

Системи простої аутентифікації на основі багаторазових паролів мають знижену стійкість, оскільки вибір аутентифікуючий інформації походить з відносно невеликого числа слів. Термін дії багаторазового пароля має бути визначений в політиці безпеки організації. Паролі повинні регулярно змінюватися, бути важкими для вгадування і не бути присутнім в словнику.

У гл. 13 розглядаються: протокол аутентифікації по багаторазовому паролю PAP (Password Authentication Protocol), протокол аутентифікації на основі процедури запит-відгук CHAP (ChallengeHandshake Authentication Protocol), а також протоколи централізованого контролю доступу до мережі видалених користувачів TACACS (Terminal Access Controller Access Control System), TACACS+ і RADIUS (Remote Authentication DialIn User Service).

7.2.2. Аутентифікація на основі одноразових паролів

Схеми аутентифікації, засновані на традиційних багаторазових паролях, не мають достатньої безпеки. Такі паролі можна перехопити, розгадати, підглянути або просто вкрасти. Надійнішими є процедури аутентифікації на основі одноразових паролів.

Суть схеми одноразових паролів — використання різних паролів при кожному новому запиті на надання доступу. Одноразовий динамічний пароль

дійсний тільки для одного входу в систему, і потім його дія витікає. Навіть якщо його перехопили, він буде даремний. Динамічний механізм завдання пароля — один з кращих способів захисту процесу аутентифікації від загроз ззовні. Зазвичай системи аутентифікації з одноразовими паролями використовуються для перевірки видалених користувачів.

Генерація одноразових паролів може здійснюватися апаратним або програмним способом. Деякі апаратні засоби доступу на основі одноразових паролів реалізуються у вигляді мініатюрних пристроїв зі вбудованим мікропроцесором, зовні схожих на платіжні пластикові картки. Такі карти, що зазвичай називаються ключами, можуть мати клавіатуру і невелике дисплейне вікно.

Як приклад розглянемо технологію аутентифікації SecurlD на основі одноразових паролів з використанням апаратних ключів і механізму тимчасової синхронізації. Ця технологія розроблена компанією Security Dynamics і реалізована в комунікаційних серверах ряду компаній, зокрема в серверах компанії Cisco Systems та ін.

Схема аутентифікації з використанням тимчасової синхронізації базується на алгоритмі генерації випадкових чисел через певний інтервал часу. Цей інтервал установлюється і може бути змінений адміністратором мережі. Схема аутентифікації використовує два параметри:

- секретний ключ, що є унікальне 64 бітове число, що призначається кожному користувачеві і що зберігається у БД аутентифікаційного сервера і в апаратному ключі користувача;
- значення поточного часу.

Коли видалений користувач робить спробу логічного входу в мережу, йому пропонується ввести його персональний ідентифікаційний номер PIN, що складається з чотирьох десяткових цифр, і шість цифр випадкового числа, що відображається у цей момент на дисплеї апаратного ключа. Використовуючи введений користувачем PINкод, сервер витягає з БД секретний ключ користувача і виконує алгоритм генерації випадкового числа, використовуючи як параметри витягнутий секретний ключ і значення поточного часу. Потім сервер перевіряє, чи співпадають згенероване число і число, введене користувачем. Якщо ці числа співпадають, то сервер дозволяє користувачеві здійснити логічний вхід в систему.

При використанні цієї схеми аутентифікації потрібно жорстку тимчасову синхронізацію апаратного ключа і сервера. З схемою аутентифікації, заснованої на тимчасовій синхронізації, пов'язана ще одна проблема. Генероване апаратним ключем випадкове число є достовірним паролем впродовж невеликого кінцевого проміжку часу. Тому можлива короткочасна ситуація, коли можна перехопити PIN-код і випадкове число, щоб використати їх для доступу в мережу. Це — вразливе місце схеми.

Одним з найбільш поширених протоколів аутентифікації на основі одноразових паролів є стандартизований в Інтернеті протокол S/Key (RFC 1760). Цей протокол реалізований у багатьох системах, що вимагають перевірки достовірності видалених користувачів, зокрема в системі TACACS+ компанії Cisco. Протокол S/Key детально розглядається в л. 13.

7.2.3. Аутентифікація на основі PINкоду

Найбільш поширеним методом аутентифікації утримувача пластикової карти і смарткарти є введення секретного числа, яке зазвичай називають PINкодом (Personal Identification Number — персональний ідентифікаційний код) або іноді CHV (CardHolder Verification). Захист PINкода карти є критичним для безпеки усієї системи. Карти можуть бути втрачені, вкрадені або підроблені. У таких випадках єдиним контрзаходом проти несанкціонованого доступу залишається секретне значення PINкода. Ось чому відкрита форма PIN має бути відома тільки законному утримувачеві карти. Очевидно, значення PIN треба тримати в секреті впродовж усього терміну дії карти.

Довжина PIN-кода має бути досить великою, щоб мінімізувати вірогідність визначення правильного PIN-кода методом проб і помилок. З іншого боку, довжина PIN-кода має бути досить короткою, щоб дати можливість утримувачам карт запам'ятати його значення. Згідно рекомендації стандарту ISO 95641, PIN-код повинен містити від 4 до 12 буквено-цифрових символів. Проте у більшості випадків введення нецифрових символів технічно неможливе, оскільки доступна тільки цифрова клавіатура. Тому зазвичай PIN-код є чотирирозрядним числом, кожна цифра якого може набувати значення від 0 до 9.

PIN-код вводиться за допомогою клавіатури терміналу або комп'ютера і потім вирушає на смарткарту. Смарткарта порівнює отримане значення PINкода з еталонним значенням, що зберігається в карті, і відправляє результат порівняння на термінал. Введення PIN-кода відноситься до заходів безпеки, особливо для фінансових транзакцій, і, отже, вимоги до клавіатури часто визначаються в прикладній області. PIN-клавіатури мають усі ознаки модуля безпеки і шифрують PIN-код відразу при його введенні. Це забезпечує надійний захист від проникнення в клавіатуру для перехоплення PIN-кода під час введення.

При ідентифікації клієнта за значенням PIN-кода і пред'явленій карті використовуються два основні способи перевірки PIN-кода: неалгоритмічний і алгоритмічний [29].

Неалгоритмічний спосіб перевірки PIN-кода не вимагає застосування спеціальних алгоритмів. Перевірка PIN-кода здійснюється шляхом безпосереднього порівняння введеного клієнтом PIN-кода зі значеннями, що зберігаються у БД. Зазвичай БД зі значеннями PIN-кодів клієнтів шифрується методом прозорого шифрування, щоб підвищити її захищеність, не ускладнюючи процесу порівняння.

Алгоритмічний спосіб перевірки PIN-кода полягає в тому, що введений клієнтом PIN-код перетворять по певному алгоритму з використанням секретного ключа і потім порівнюють зі значенням PIN-кода, що зберігається в певній формі на карті. Достоїнства цього методу перевірки:

- відсутність копії PIN-кода на головному комп'ютері виключає його розкриття обслуговуючим персоналом;
- відсутність передачі PIN-кода між банкоматом і головним комп'ютером банку виключає його перехоплення зловмисником або нав'язування результатів порівняння;
- спрощення роботи із створення програмного забезпечення системи, оскільки вже немає необхідності дій в реальному масштабі часу.

7.3. Строга аутентифікація

7.3.1. Основні поняття

Ідея строгої аутентифікації, що реалізовується в криптографічних протоколах, полягає в наступному. Сторона, що перевіряється (що доводить), доводить свою достовірність перевіряючій стороні, демонструючи знання деякого секрету [54, 62]. Наприклад, цей секрет може бути заздалегідь розподілений безпечним способом між сторонами аутентифікаційного обміну. Доказ знання секрету здійснюється за допомогою послідовності запитів і відповідей з використанням криптографічних методів і засобів.

Істотним є факт, що сторона, що доводить, демонструє тільки знання секрету, але сам секрет в ході аутентифікаційного обміну не розкривається. Це забезпечується за допомогою відповідей сторони, що доводить, на різні запити перевіряючої сторони. При цьому результуючий запит залежить тільки від призначеного для користувача секрету і початкового запиту, який зазвичай представляє довільно вибране на початку протоколу велике число.

У більшості випадків строга аутентифікація полягає в тому, що кожен користувач аутентифікується за ознакою володіння своїм секретним ключем. Інакше кажучи, користувач має можливість визначити, чи володіє його партнер по зв'язку належним секретним ключем і чи може він використати цей ключ для підтвердження того, що він дійсно є справжнім партнером по інформаційному обміну.

Відповідно до рекомендацій стандарту X. 509 розрізняють процедури строгої аутентифікації наступних типів:

- одностороння аутентифікація;
- двостороння аутентифікація;
- трибічна аутентифікація.

Одностороння аутентифікація передбачає обмін інформацією тільки в одному напрямі.

Двостороння аутентифікація в порівнянні з односторонньою містить додаткову відповідь перевіряючої сторони стороні доказуючій, який повинен переконати її, що зв'язок встановлюється саме з тією стороною, якою були призначені аутентифікаційні дані;

Трибічна аутентифікація містить додаткову передачу даних від сторони доказуючої, стороні перевіряючій. Цей підхід дозволяє відмовитися від використання міток часу при проведенні аутентифікації.

Слід зазначити, що ця класифікація досить умовна. На практиці набір використовуваних прийомів і засобів залежить безпосередньо від конкретних умов реалізації процесу аутентифікації. Необхідно враховувати, що проведення строгої аутентифікації вимагає обов'язкового узгодження сторонами використовуваних криптографічних алгоритмів і додаткових параметрів .

Перш ніж перейти до розгляду конкретних варіантів протоколів строгої аутентифікації, слід зупинитися на призначенні і можливостях так званих одноразових параметрів, використовуваних в протоколах аутентифікації. Одноразові параметри іноді називають також nonces — це величина, використовувана для однієї і тієї ж мети не більше одного разу. Серед

використовуваних на сьогодні одноразових параметрів слід виділити: випадкові числа, мітки часу і номера послідовностей.

Одноразові параметри дозволяють уникнути повтору передачі, підміни сторони аутентифікаційного обміну і атаки з вибором відкритого тексту. З їх допомогою можна забезпечити унікальність, однозначність і тимчасові гарантії передаючих повідомлень. Різні типи одноразових параметрів можуть вживатися як окремо, так і доповнювати один одного.

Слід зазначити, що одноразові параметри широко використовуються і в інших варіантах криптографічних протоколів (наприклад, в протоколах розподілу ключової інформації).

Залежно від використовуваних криптографічних алгоритмів протоколи строгої аутентифікації діляться на протоколи, засновані:

- на симетричних алгоритмах шифрування;
- однонапрямлених ключових хешфункціях;
- асиметричних алгоритмах шифрування;
- алгоритмах електронного цифрового підпису.

7.3.2. Строга аутентифікація, заснована на симетричних алгоритмах

Для роботи протоколів аутентифікації, побудованих на основі симетричних алгоритмів, необхідно, щоб перевіряючий і такий, що доводить із самого початку мали один і той же секретний ключ. Для закритих систем з невеликою кількістю користувачів кожна пара користувачів може заздалегідь розділити його між собою. У великих розподілених системах, що застосовують технологію симетричного шифрування, часто використовуються протоколи аутентифікації за участю довіреного сервера, з яким кожна сторона розділяє знання ключа. Такий сервер розподіляє сеансові ключі для кожної пари користувачів всякий раз, коли один з них просить аутентифікацію іншого. Уявна простота цього підходу є оманливою, насправді розробка протоколів аутентифікації цього типу є складною і з точки зору безпеки не очевидної.

Протоколи аутентифікації з симетричними алгоритмами шифрування

Нижче наводяться три приклади протоколів аутентифікації, специфікованих в ISO/IEC 97982. Ці протоколи припускають попередній розподіл секретних ключів, що розділяються [54, 62].

Розглянемо наступні варіанти аутентифікації:

- одностороння аутентифікація з використанням міток часу;
- одностороння аутентифікація з використанням випадкових чисел;
- двостороння аутентифікація.

У кожному з цих випадків користувач доводить свою достовірність, демонструючи знання секретного ключа, оскільки робить розшифровку запитів за допомогою цього секретного ключа.

При використанні в процесі аутентифікації симетричного шифрування необхідно також реалізувати механізми забезпечення цілісності передаваних даних на основі загальноприйнятих способів.

Введемо наступні позначення:

r_A — випадкове число, згенероване учасником А;

r_B — випадкове число, згенероване учасником В;

t_A — мітка часу, згенерована учасником А;

E_K Симетричне шифрування на ключі К (ключ К має бути заздалегідь розподілений між А і В).

1. Одностороння аутентифікація, заснована на мітках часу:

$$A \rightarrow B\colon E_K(t_A, B). \quad (1)$$

Після отримання і розшифровки цього повідомлення учасник В переконується в тому, що мітка часу t_A дійсна і ідентифікатор В, вказаний в повідомленні, співпадає з його власним. Запобігання повторній передачі цього повідомлення ґрунтується на тому, що без знання ключа неможливо змінити мітку часу t_A і ідентифікатор В.

2. Одностороння аутентифікація, заснована на використанні випадкових чисел:

$$A \leftarrow B\colon r_B; \quad (1)$$

$$A \rightarrow B\colon E_K(r_B, B). \quad (2)$$

Учасник В відправляє учасникові А випадкове число r_B. Учасник А шифрує повідомлення, що складається з отриманого числа r_B і ідентифікатора В, і відправляє зашифроване повідомлення учасника В. Учасник В розшифровує отримане повідомлення і порівнює випадкове число, що міститься в повідомленні з тим, яке він послав учасникові А. Додатково він перевіряє ім'я, вказане в повідомленні.

3. Двостороння аутентифікація, що використовує випадкові значення:

$$A \leftarrow B\colon r_B \quad (1)$$

$$A \rightarrow B\colon E_K(r_A, r_B, B); \quad (2)$$

$$A \leftarrow B\colon E_K(r_A, r_B); \quad (3)$$

При отриманні повідомлення (2) учасник У виконує ті ж перевірки, що і в попередньому протоколі, і додатково розшифровує випадкове число r_A для включення його в повідомлення (3) для учасника А. Повідомлення (3), отримане учасником А, дозволяє йому переконатися на основі перевірки значень r_A і r_B, що він має справу саме з учасником В.

Широко відомими представниками протоколів, що забезпечують аутентифікацію користувачів із залученням в процесі аутентифікації третьої сторони, являються протокол розподілу секретних ключів Нідхема і Шредера і протокол Kerberos.

Протоколи, засновані на використанні однонапрямлених ключових хешфункцій

Протоколи, представлені вище, можуть бути модифіковані шляхом заміни симетричного шифрування на шифрування за допомогою односторонньої ключовий хешфункції [45, 62]. Це буває необхідно, якщо алгоритми блокового шифрування недоступні або не відповідають вимогам (наприклад, у разі експортних обмежень), що пред'являються.

Своєрідність шифрування за допомогою односторонньої хеш функції полягає в тому, що воно по суті є одностороннім, т. е. не супроводжується зворотним перетворенням — розшифровкою на приймальній стороні. Обидві сторони

(відправник і одержувач) використовують одну і ту ж процедуру одностороннього шифрування [45].

Одностороння хешфункція $h_K(\cdot)$ з параметром ключом к, застосовується до шифрованих М, дає в результаті хешзначение m (дайджест), що складається з фіксованого невеликого числа байт (Рис. 7.3). Дайджест $m = h_K(M)$ передається одержувачеві разом з початковим повідомленням М. Одержувач повідомлення, знаючи, яка одностороння хешфункція була застосована для отримання дайджеста, наново обчислює її, використовуючи розшифроване повідомлення М. Якщо значення отриманого дайджеста m і вичисленого дайджеста m' співпадають, означає вміст повідомлення М не було піддано ніяким змінам.

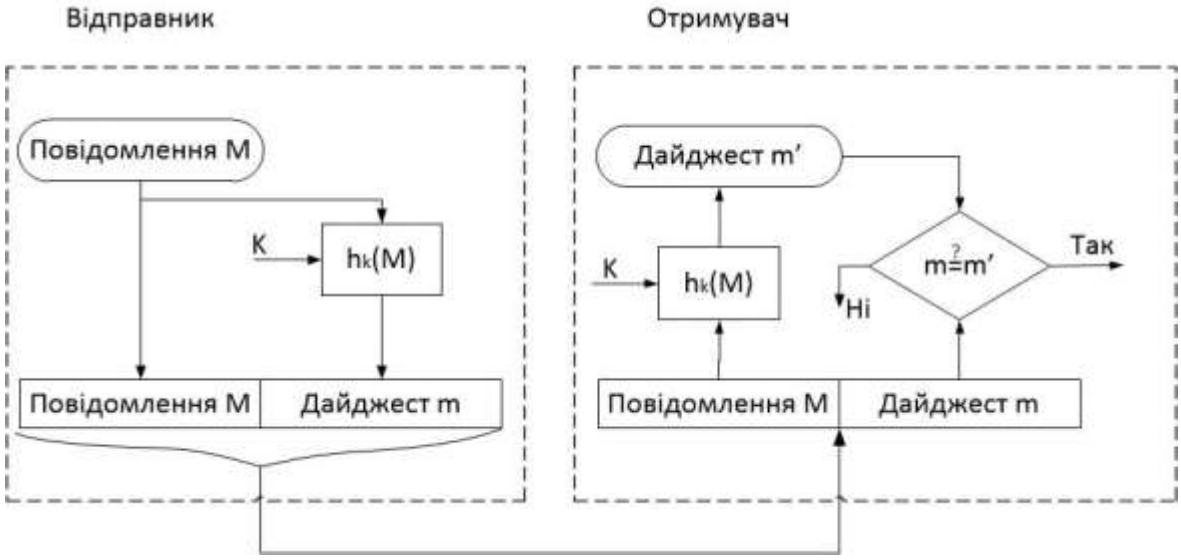

Рис. 7.3. Застосування для аутентифікації односторонньої хешфункції з параметром ключем

Знання дайджеста не дає можливості відновити початкове повідомлення, але дозволяє перевірити цілісність даних. Дайджест можна розглядати як свого роду контрольну суму для початкового повідомлення. Проте між дайджестом і звичайною контрольною сумою є і істотна відмінність. Контрольну суму використовують як засіб перевірки цілісності передаваних повідомлень по ненадійних лініях зв'язку. Цей засіб перевірки не розрахований на боротьбу із зловмисниками, яким в такій ситуації ніщо не заважає підмінити повідомлення, додавши до нього нове значення контрольної суми. Одержувач у такому разі не помітить ніякої підміни.

На відміну від звичайної контрольної суми при обчисленні дайджеста застосовуються секретні ключі. У разі, якщо для отримання дайджеста використовується одностороння хешфункція з параметром ключем До, який відомий тільки відправнику і одержувачеві, будь-яка модифікація початкового повідомлення буде негайно виявлена.

На Рис. 7.4 показаний інший варіант використання односторонньої хеш-функції для перевірки цілісності даних. В цьому випадку одностороння хеш-функція $h(\cdot)$ не має параметра-ключа, але застосовується не просто до повідомлення М, а до повідомлення, доповненого секретним ключем К, тобто

відправник обчислює дайджест $m = h(M, K)$. Одержувач, витягаючи початкове повідомлення М, також доповнює його тим же відомим йому секретним ключем К, після чого застосовує до отриманих даних односторонню хешфункцию $h(\cdot)$. Результат обчислень — дайджест m' — порівнюється з отриманим по мережі дайджестом m.

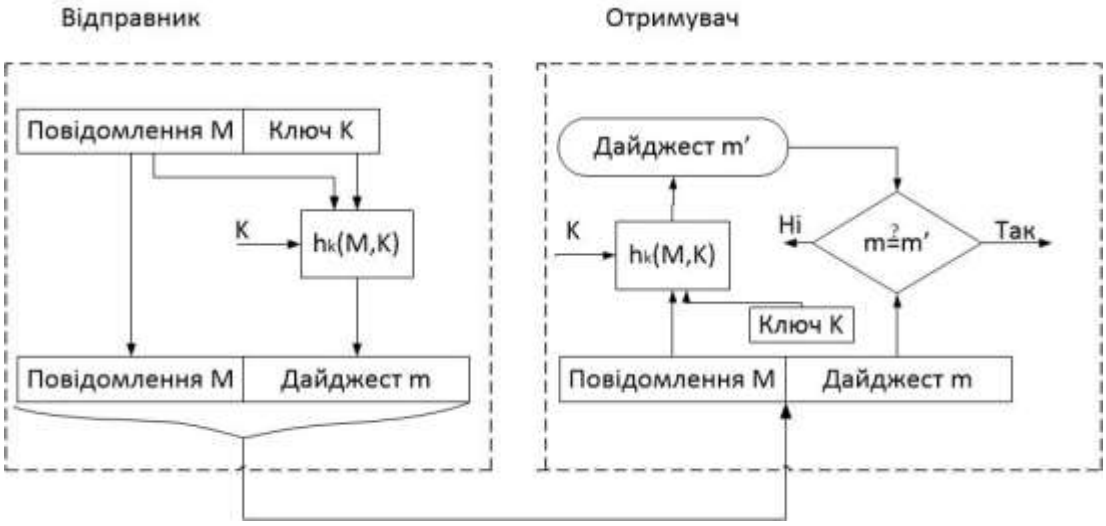

Рис. 7.4. Застосування односторонньої хешфункції до повідомлення доповненого секретним ключем К

При використанні односторонніх функцій шифрування в розглянуті вище протоколи необхідно внести наступні зміни:

- функція симетричного шифрування E_K замінюється функцією h_K
- перевіряючий замість встановлення факту збігу полів в розшифрованих сполученнях з передбачуваними значеннями обчислює значення однонапрямленої функції і порівнює його з отриманим від іншого учасника обміну інформацією;
- для забезпечення незалежного обчислення значення однонапрямленої функції одержувачем повідомлення в протоколі 1 мітка часу t_A повинна передаватися додатково у відкритому виді, а в повідомленні (2) протоколи 3 випадкове число r_A повинне передаватися додатково у відкритому виді.

Модифікований варіант протоколу 3 з урахуванням сформульованих змін має наступну структуру:

$$A \leftarrow B: r_B; \qquad (1)$$

$$A \rightarrow B: r_A, h_K(r_A, r_B, B); \qquad (2)$$

$$A \leftarrow B: h_K(r_A, r_B, A). \qquad (3)$$

Помітимо, що в повідомлення (3) протоколу включено поле А. Результуючий протокол забезпечує взаємну аутентифікацію і відомий як протокол SKID 3 [54, 62].

7.3.3. Строга аутентифікація, заснована на асиметричних алгоритмах

У протоколах строгої аутентифікації можуть бути використані асиметричні алгоритми з відкритими ключами. Той, що в цьому випадку доводить може продемонструвати знання секретного ключа одним з наступних способів:

- розшифрувати запит, зашифрований на відкритому ключі;
- поставити свій цифровий підпис на запиті [54, 62].

Пара ключів, необхідна для аутентифікації, не повинна використовуватися для інших цілей (наприклад, для шифрування) з міркувань безпеки. Важливо відмітити, що вибрана система з відкритим ключем має бути стійкою до атак з вибіркою шифрованого тексту навіть у тому випадку, якщо порушник намагається отримати критичну інформацію, видаючи себе за перевіряючого і діючи від його імені.

Аутентифікація з використанням асиметричних алгоритмів шифрування

Як приклад протоколу, побудованого на використанні асиметричного алгоритму шифрування, можна привести наступний протокол аутентифікації:

$$A \leftarrow B\colon\ h(r),\ B,\ P_A(r,\ B); \qquad (1)$$

$$A \rightarrow B\colon\ r. \qquad (2)$$

Учасник У вибирає випадковим чином r і обчислює значення $x = h(r)$ (значення х демонструє знання r без розкриття самого значення r), далі він обчислює значення $e = P_A(r,\ B)$. Під P_A мається на увазі алгоритм асиметричного шифрування (наприклад, RSA), а під $h(\cdot)$ — хешфункція. Учасник В відправляє повідомлення (1) учасника А. Учасник А розшифровує $e = P_A(r,\ B)$ і отримує значення r_1, і B_1, а також обчислює $x_1 = h(r_1)$. Після цього робиться ряд порівнянь, що доводять, що $x = x_1$, і що отриманий ідентифікатор 5, дійсно вказує на учасника В. У разі успішного проведення порівняння учасник А посилає r. Отримавши його, учасник В перевіряє, чи то це значення, яке він відправив в повідомленні (1).

В якості іншого прикладу приведемо модифікований протокол Нідхема і Шредера, заснований на асиметричному шифруванні (досить детально він описаний в розділі, присвяченому розподілу ключової інформації, оскільки основний варіант протоколу використовується для аутентифікаційного обміну ключової інформації).

Розглядаючи варіант протоколу Нідхема і Шредера, використовуваний тільки для аутентифікації, матимемо на увазі під Рв алгоритм шифрування відкритим ключем учасника В. Протокол має наступну структуру:

$$A \rightarrow B\colon\ P_B(r_1,\ A); \qquad (1)$$

$$A \leftarrow B\colon\ P_A(r_2,\ r_1); \qquad (2)$$

$$A \leftarrow B\colon\ r_2. \qquad (3)$$

Аутентифікація, заснована на використанні цифрового підпису

У рекомендаціях стандарту Х.509 специфікована схема аутентифікації, заснована на використанні цифрового підпису, міток часу і випадкових чисел.

Для опису цієї схеми аутентифікації введемо наступні позначення:

t_A, r_A и r_B — тимчасова мітка і випадкові числа відповідно;

SA — підпис, згенерований учасником А;

SB — підпис, згенерований учасником В;

certA — сертифікат відкритого ключа учасника А;

certB — сертифікат відкритого ключа учасника В.

Якщо учасники мають автентичні відкриті ключі, отримані один від одного, то можна не користуватися сертифікатами, інакше вони служать для підтвердження достовірності відкритих ключів.

В якості прикладів приведемо наступні протоколи аутентифікації.

1. Одностороння аутентифікація із застосуванням міток часу:

$$A \to B\text{: } \mathrm{cert}_A,\ t_A,\ B,\ S_A(t_A,\ B). \quad (1)$$

Після прийняття цього повідомлення учасник В перевіряє правильність мітки часу t_A, отриманий ідентифікатор В і, використовуючи відкритий ключ з сертифікату certA коректність цифрового підпису $S_A(t_A,\ B)$.

2. Одностороння аутентифікація з використанням випадкових чисел:

$$A \leftarrow B\text{: } r_B; \quad (1)$$

$$A \to B\text{: } \mathrm{cert}_A,\ r_A,\ B,\ S_A(r_A,\ r_B,\ B). \quad (2)$$

Учасник В, отримавши повідомлення від учасника А, переконується, що саме він є адресатом повідомлення; використовуючи відкритий ключ учасника А, узятий з сертифікату certA перевіряє коректність підпису $S_A(r_A,\ r_B,\ B)$ під числом r_A, отриманим у відкритому виді, числом r_B, яке було відіслане в повідомленні (1), і його ідентифікатором В. Підписане випадкове число r_A використовується для запобігання атакам з вибіркою відкритого тексту.

3. Двостороння аутентифікація з використанням випадкових чисел:

$$A \leftarrow B\text{: } r_B; \quad (1)$$

$$A \to B\text{: } \mathrm{cert}_A,\ r_A,\ B,\ S_A(r_A,\ r_B,\ B); \quad (2)$$

$$A \leftarrow B\text{: } \mathrm{cert}_B,\ A,\ S_B(r_A,\ r_B,\ A). \quad (3)$$

У цьому протоколі обробка повідомлень (1) і (2) виконується так само, як і в попередньому протоколі, а повідомлення (3) обробляється аналогічно повідомленню (2).

7.4. Біометрична аутентифікація користувача

Процедури ідентифікації і аутентифікації користувача можуть базуватися не лише на секретній інформації, яку має користувач (пароль, персональний идентификатор, секретний ключ і т. п.). Останнім часом все більшого поширення набуває біометрична аутентифікація користувача, що дозволяє упевнено аутентифицировать потенційного користувача шляхом виміру фізіологічних параметрів і характеристик людини, особливостей його поведінки.

Основні достоїнства біометричних методів:

- висока міра достовірності аутентифікації за біометричними ознаками (із-за їх унікальності);
- невід'ємність біометричних ознак від дієздатної особи;
- трудність фальсифікації біометричних ознак.

Активно використовуються наступні біометричні ознаки:

- відбитки пальців;
- геометрична форма кисті руки;
- форма і розміри особи;
- особливості голосу;
- візерунок райдужної оболонки і сітківки очей.

Розглянемо типову схему функціонування біометричної підсистеми аутентифікації. При реєстрації в системі користувач повинен продемонструвати один або кілька разів свої характерні біометричні ознаки. Ці ознаки (відомі як справжні) реєструються системою як контрольний «образ» (біометричний підпис) законного користувача. Цей образ користувача зберігається системою в електронній формі і використовується для перевірки ідентичності кожного, хто видає себе за відповідного законного користувача. Залежно від збігу або неспівпадання сукупності пред'явлених ознак із зареєстрованими в контрольному образі той, що пред'явив їх визнається законним користувачем (при збігу) або незаконним (при неспівпаданні).

З точки зору споживача, ефективність біометричної аутентифікаційної системи характеризується двома параметрами:

- коефіцієнтом помилкових відмов FRR (falsereject rate);
- коефіцієнтом помилкових підтверджень FAR (false alarm rate).

Помилкова відмова виникає, коли система не підтверджує особу законного користувача (типові значення FRR — порядку однієї помилки на 100). Помилкове підтвердження відбувається у разі підтвердження особи незаконного користувача (типові значення FAR — порядку однієї помилки на 10 000). Ці коефіцієнти пов'язані один з одним: кожному коефіцієнту помилкових відмов відповідає певний коефіцієнт помилкових підтверджень.

У досконалій біометричній системі обидва параметри помилки мають дорівнювати нулю. На жаль, біометричні системи теж не ідеальні. Зазвичай системні параметри настроюють так, щоб добитися необхідного коефіцієнта помилкових підтверджень, що визначає відповідний коефіцієнт помилкових відмов.

До теперішнього часу розроблені і продовжують удосконалюватися технології аутентифікації по відбитках пальців, веселковій оболонці ока, за формою кисті руки і долоні, за формою і розміром особи, по голосу і «клавіатурному почерку».

Найчастіше біометричні системи використовують як параметр ідентифікації відбитки пальців (дактилоскопічні системи аутентифікації). Такі системи прості і зручні, мають високу надійність аутентифікації.

Дактилоскопічні системи аутентифікації. Одна з головних причин широкого поширення таких систем — наявність великих банків цих відбитків пальців. Користувачами подібних систем головним чином є поліція, різні державні і деякі банківські організації.

У загальному випадку біометрична технологія розпізнавання відбитків пальців замінює захист доступу з використанням пароля. Більшість систем використовують відбиток одного пальця.

Основними елементами дактилоскопічної системи аутентифікації є:

- сканер;
- ПЗ ідентифікації, що формує ідентифікатор користувача;
- ПЗ аутентифікації, порівняння відсканованого відбитку пальця, що виробляє, з наявними у БД «паспортами» користувачів.

Дактилоскопічна система аутентифікації працює таким чином. Спочатку проходить реєстрація користувача. Як правило, робиться декілька варіантів сканування в різних положеннях пальця на сканері. Зрозуміло, що зразки трохи

відрізнятимуться, і тому вимагається сформувати деякий узагальнений зразок — «паспорт». Результати запам'ятовуються у БД аутентифікації. При аутентифікації робиться порівняння відсканованого відбитку пальця з «паспортами», що зберігаються у БД.

Завдання формування «паспорта» і завдання розпізнавання зразка, що пред'являється, — це завдання розпізнавання образів. Для їх вирішення використовуються різні алгоритми, що являються ноухау фірм виробників подібних пристроїв.

Сканери відбитків пальців. Багато виробників все частіше переходять від дактилоскопічного устаткування на базі оптики до продуктів, заснованих на інтегральних схемах. Останні мають значно менші розміри, ніж оптичні зчитувачі, і тому їх простіше реалізувати в широкому спектрі периферійних пристроїв.

Деякі виробники комбінують біометричні системи із смарткартами і картамиключами. Наприклад, у біометричній ідентифікаційній смарткарті Authentic реалізований наступний підхід. Зразок відбитку пальця користувача запам'ятовується в пам'яті карти в процесі внесення в списки ідентифікаторів користувачів, встановлюючи відповідність між зразком і особистим ключем шифрування. Потім, коли користувач вводить смарткарту в зчитувач і прикладає палець до сенсора, ключ засвідчує його особу. Комбінація біометричних пристроїв і смарткарт є вдалим рішенням, що підвищує надійність процесів аутентифікації і авторизації.

Невеликий розмір і невисока ціна датчиків відбитків пальців на базі інтегральних схем перетворює їх на ідеальний інтерфейс для систем захисту. Їх можна вбудувати у брелок для ключів, і користувачі отримають універсальний ключ, який забезпечить захищений доступ до всього, починаючи від комп'ютерів до вхідних дверей, дверей автомобілів і банкоматів.

Системи аутентифікації за формою долоні використовують сканери форми долоні, що зазвичай встановлюються на стінах. Слід зазначити, що переважна більшість користувачів віддають перевагу системам цього типу.

Облаштування прочитування форми долоні створюють об'ємне зображення долоні, вимірюючи довжину пальців, товщину і площу поверхні долоні. Наприклад, продукти компанії Recognition Systems виконують більше 90 вимірів, які перетворяться в 9разрядний зразок для подальших порівнянь. Цей зразок може бути збережений локально, на індивідуальному сканері долоні або в централізованій БД.

По рівню доходів облаштування сканування форми долоні, займають 2е місце серед біометричних пристроїв, але рідко застосовуються в мережевому середовищі изза високої вартості і розміру. Проте сканери форми долоні добре підходять для обчислювальних середовищ із строгим режимом безпеки і напруженим трафіком, включаючи серверні кімнати. Вони досить точні і мають досить низький коефіцієнт помилкової відмови FRR.

Системи аутентифікації по обличчю і голосу найбільш доступні изза їх дешевизни, оскільки більшість сучасних комп'ютерів мають відео і аудіозасоби. Системи цього класу застосовуються при видаленій ідентифікації суб'єкта доступу в телекомунікаційних мережах.

Технологія сканування рис обличчя підходить для тих застосувань, де інші біометричні технології непридатні. В цьому випадку для ідентифікації і верифікації

особи використовуються особливості очей, носа і губ. Виробники облаштувань розпізнавання рис обличчя застосовують власні математичні алгоритми для ідентифікації користувачів

Дослідження, що проводяться компанією International Biometric Group, говорять про те, що співробітники багатьох організацій не довіряють облаштуванням розпізнавання по рисах обличчя. Крім того, за даними цієї компанії, сканування рис обличчя — єдиний метод біометричної аутентифікації, який не вимагає згоди на виконання перевірки (і може здійснюватися прихованою камерою), а тому має негативний для користувачів підтекст.

Слід зазначити, що технології розпізнавання рис обличчя вимагають подальшого вдосконалення. Велика частина алгоритмів розпізнавання рис обличчя чутлива до коливань в освітленні, викликаною зміною інтенсивності сонячного світла впродовж дня. Зміна положення особи також може вплинути на впізнанність. Відмінність в положенні в 15 % між прошеним зображенням і зображенням, яке знаходиться у БД, безпосередньо позначається на ефективності: при відмінності в 45° розпізнавання стає неефективним.

Системи аутентифікації по голосу економічно вигідні з тих же причин, що і системи розпізнавання по рисах обличчя. Зокрема, їх можна встановлювати з устаткуванням (наприклад, мікрофонами), що поставляється в стандартній комплектації з багатьма ПК.

Системи аутентифікації по голосу при записі зразка і в процесі подальшої ідентифікації спираються на такі особливості голосу, як висота, модуляція і частота звуку. Ці показники визначаються фізичними характеристиками голосового тракту і унікальні для кожної людини. Розпізнавання голосу застосовується замість набору номера в певних системах Sprint. Технологія розпізнавання голосу відрізняється від розпізнавання мови: остання інтерпретує те, що говорить абонент, а технологія розпізнавання голосу абонента підтверджує особу того, що говорить.

Оскільки голос можна просто записати на плівку або інші носії, деякі виробники вбудовують у свої продукти операцію запиту відгуку. Ця функція пропонує користувачеві при вході відповісти на заздалегідь підготовлений і регулярно такий, що міняється запит, наприклад такий: «Повторіть числа 0, 1, 3».

Устаткування аутентифікації по голосу придатніше для інтеграції в додатки телефонії, чим для входу в мережу. Зазвичай воно дозволяє абонентам отримати доступ у фінансові або інші системи за допомогою телефонного зв'язку.

Технології розпізнавання того, що говорить мають деякі обмеження. Різні люди можуть говорити схожими голосами, а голос будь-якої людини може мінятися з часом залежно від самопочуття, емоційного стану і віку. Більше того, різниця в модифікації телефонних апаратів і якість телефонних з'єднань можуть серйозно ускладнити розпізнавання.

Оскільки голос сам по собі не забезпечує достатньої точності, розпізнавання по голосу слід поєднувати з іншими біометриками, такими як розпізнавання рис обличчя або відбитків пальців.

Системи аутентифікації по візерунку райдужної оболонки і сітківки очей можуть бути розділені на два класи:

- що використовують малюнок райдужної оболонки ока;
- що використовують малюнок кровоносних судин сітківки ока.

Сітківка людського ока є унікальним об'єктом для аутентифікації. Малюнок кровоносних судин очного дна відрізняється навіть у близнюків. Оскільки вірогідність повторення параметрів райдужної оболонки і сітківки ока має порядок 10" 78, такі системи являються найбільш надійними серед усіх біометричних систем і застосовуються там, де потрібно високий рівень безпеки (наприклад, в режимних зонах військових і оборонних об'єктів).

Біометричний підхід дозволяє спростити процес з'ясування «хто є хто». При використанні дактилоскопічних сканерів і облаштувань розпізнавання голосу для входу в мережі співробітники позбавляються від необхідності запам'ятовувати складні паролі. Ряд компаній інтегрує біометричні можливості в системи одноразової аутентифікації SSO (Single SignOn) масштабу підприємства. Подібна консолідація дозволяє мережевим адміністраторам замінити служби одноразової аутентифікації паролів біометричними технологіями.

Біометрична аутентифікація користувача може бути використана при шифруванні у вигляді модулів блокування доступу до секретного ключа, який дозволяє скористатися цією інформацією тільки істинному власникові приватного ключа. Власник може потім застосовувати свій секретний ключ для шифрування інформації, що передається по приватних мережах або по Internet. Ахілесовою п'ятою багатьох систем шифрування являється проблема безпечного зберігання самого криптографічного секретного ключа. Частенько доступ до ключа завдовжки 128 розрядів (або навіть більше) захищений лише паролем з 6 символів, т. е. 48 розрядів. Відбитки пальців забезпечують набагато більш високий рівень захисту і, на відміну від пароля, їх неможливо забути.

Лекція 8 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОПЕРАЦІЙНИХ СИСТЕМ

Розвиток глобальних комп'ютерних мереж, поява нових перспективних інформаційних технологій (ІТ) привертають все більшу увагу. Глобальні мережі застосовуються для передачі комерційної інформації різного рівня конфіденційності, наприклад для зв'язку головної штаб-квартири організації з видаленими офісами або створення Web-сайтів організації з розміщеною на них рекламою і діловими пропозиціями. Багато організацій приймають рішення про підключення своїх локальних і корпоративних мереж до відкритої глобальної мережі.

Проте підключення до відкритої глобальної мережі може мати і негативні наслідки, оскільки з'являються загрози неправомірного вторгнення із зовнішньої мережі у внутрішню мережу. Таке вторгнення може виконуватися як з метою несанкціонованого використання ресурсів внутрішньої мережі, наприклад розкрадання інформації, так і з метою порушення її працездатності. Кількість уразливостей мережевих ОС, застосовних програм і можливих атак постійно росте. Без відповідних засобів захисту вірогідність успішної реалізації таких загроз є досить високою.

Щорічні втрати, обумовлені недостатнім рівнем захищеності комп'ютерних мереж організацій, оцінюються мільярдами доларів. Тому при підключенні до Internet локальної або корпоративної мережі необхідно потурбуватися про забезпечення інформаційної безпеки цієї мережі.

Проблема захисту від несанкціонованих дій при взаємодії із зовнішніми мережами може бути успішно розв'язана тільки на основі комплексного захисту корпоративних комп'ютерних мереж. До базових засобів багаторівневого захисту міжмережевого обміну даними відносяться захищені ОС, МЕ, віртуальні захищені мережі VPN, протоколи захисту на канальному, транспортному і мережевому (протокол IPSec) рівнях.

8.1. Проблеми забезпечення безпеки ОС

Більшість програмних засобів захисту інформації є застосовними програмами. Для їх виконання потрібно підтримку ОС. Оточення, в якому функціонує ОС, називається довіреною обчислювальною базою (ДОБ). ДОБ включає повний набір елементів, що забезпечують інформаційну безпеку: ОС, програми, мережеве устаткування, засоби фізичного захисту і навіть організаційні процедури. Наріжним каменем цієї піраміди є захищена ОС.

8.1.1. Загрози безпеки ОС

Організація ефективного і надійного захисту ОС неможлива без попереднього аналізу можливих загроз її безпеки. Загрози безпеки ОС істотно залежать від умов експлуатації системи, від того, яка інформація зберігається і обробляється в системі, і т. д. Наприклад, якщо ОС використовується для організації електронного документообігу, найбільш небезпечні загрози, пов'язані з несанкціонованим доступом (НСД) до файлів. Якщо ж ОС використовується як

платформа провайдера Internet послуг, дуже небезпечні атаки на мережеве програмне забезпечення ОС.

Загрози безпеки ОС можна класифікувати по різних аспектах їх реалізації [56].

1. По меті атаки:
- несанкціоноване читання інформації;
- несанкціонована зміна інформації;
- несанкціоноване знищення інформації;
- повне або часткове руйнування ОС.

2. За принципом дії на операційну систему.
- використання відомих (легальних) каналів отримання інформації; наприклад загроза несанкціонованого читання файлу, доступ користувачів до якого визначений некоректно, т. е. дозволений доступ користувачеві, якому згідно з політикою безпеки доступ має бути заборонений;
- використання прихованих каналів отримання інформації; наприклад загроза використання зловмисником недокументованих можливостей ОС;
- створення нових каналів отримання інформації за допомогою програмних закладок.

3. За типом використовуваної зловмисником уразливості захисту:
- неадекватна політика безпеки, у тому числі і помилки адміністратора системи;
- помилки і недокументовані можливості програмного забезпечення ОС, у тому числі і так звані люки — випадково або навмисно вбудовані в систему «Службові входи», дозволяючі обходити систему захисту;
- раніше впроваджена програмна закладка.

4. За характером дії на операційну систему.
- активна дія — несанкціоновані дії зловмисника в системі;
- пасивна дія — несанкціоноване спостереження зловмисника за процесами, що відбуваються в системі.

Загрози безпеки ОС можна також класифікувати за такими ознаками, як: спосіб дій зловмисника, використовувані засоби атаки, об'єкт атаки, спосіб впливу на об'єкт атаки, стан об'єкту, що атакується, ОС на момент атаки.

ОС може піддатися наступним типовим атакам:
- скануванню файлової системи. Зловмисник переглядає файлову систему комп'ютера і намагається прочитати (чи скопіювати) усі файли підряд. Рано чи пізно виявляється хоч би одна помилка адміністратора. У результаті зловмисник дістає доступ до інформації, який має бути йому заборонений;
- підбору пароля. Існують декілька методів підбору паролів користувачів:
  — тотальний перебір;
  — тотальний перебір, оптимізований за статистикою тієї, що зустрічається символів або за допомогою словників;
  — підбір пароля з використанням знань про користувача (його імені, прізвища, дати народження, номера телефону і т. д.);
- крадіжці ключової інформації. Зловмисник може підглянути пароль, що набирає користувачем, або відновити пароль, що набирає користувачем, по

рухах його рук на клавіатурі. Носій з ключовою інформацією (смарт карта, Touch Memory і т. д.) може бути просто вкрадений;

- складанню сміття. У багато ОС інформація, знищена користувачем, не знищується фізично, а позначається як знищена (так зване сміття). Зловмисник відновлює цю інформацію, переглядає її і копіює фрагменти, що цікавлять його;
- перевищенню повноважень. Зловмисник, використовуючи помилки в програмному забезпеченні ОС або політиці безпеки, отримує повноваження, що перевищують ті, які йому надані відповідно до політики безпеки. Зазвичай це досягається шляхом запуску програми від імені іншого користувача;
- програмним закладкам. Програмні закладки, що впроваджуються в ОС, не мають істотних відмінностей від інших класів програмних закладок;
- жадібним програмам — це програми, навмисно захоплюючі значну частину ресурсів комп'ютера, внаслідок чого інші програми не можуть виконуватися або виконуються украй повільно. Запуск жадібної програми може привести до краху ОС [56].

8.1.2. Поняття захищеної ОС

Операційну систему називають захищеною, якщо вона передбачає засоби захисту від основних класів загроз. Захищена ОС обов'язково повинна містити засоби розподілення доступу користувачів до своїх ресурсів, а також засобу перевірки достовірності користувача, початкуючого роботу з ОС. Крім того, захищена ОС повинна містити засоби протидії випадковому або умисному виведенню ОС з ладу.

Якщо ОС передбачає захист не від усіх основних класів загроз, а тільки від деяких, таку ОС називають частково захищеною [56, 88].

Підходи до побудови захищених ОС

Існують два основні підходи до створення захищених ОС — фрагментарний і комплексний. При фрагментарному підході спочатку організовується захист від однієї загрози, потім від іншої і т. д. Прикладом фрагментарного підходу може служити ситуація, коли за основу береться незахищена ОС (наприклад, Windows 98), на неї встановлюються антивірусний пакет, система шифрування, система реєстрації дій користувачів і т. д.

При застосуванні фрагментарного підходу підсистема захисту ОС є набором розрізнених програмних продуктів, як правило, від різних виробників. Ці програмні засоби працюють незалежно один від одного, при цьому практично неможливо організувати їх тісну взаємодію. Крім того, окремі елементи такої підсистеми захисту можуть некоректно працювати в присутності один одного, що призводить до різкого зниження надійності системи.

При комплексному підході захисні функції вносяться в ОС на етапі проектування архітектури ОС і є її невід'ємною частиною. Окремі елементи підсистеми захисту, створеного на основі комплексного підходу, тісно взаємодіють один з одним при рішенні різних завдань, пов'язаних з організацією захисту інформації, тому конфлікти між її окремими компонентами практично неможливі. Підсистема захисту, створена на основі комплексного підходу, може бути влаштована так, що при фатальних збоях у функціонуванні її ключових елементів вона викликає крах ОС, що не дозволяє зловмисникові відключати захисні функції

системи. При фрагментарному підході така організація підсистеми захисту неможлива.

Як правило, підсистему захисту ОС, створену на основі комплексного підходу, проектують так, щоб окремі її елементи були замінювані. Відповідні програмні модулі можуть бути замінені іншими модулями.

Адміністративні заходи захисту

Програмно апаратні засоби захисту ОС обов'язково повинні доповнюватися адміністративними заходами захисту. Без постійної кваліфікованої підтримки з боку адміністратора навіть надійний програмно апаратний захист може давати збої. Перерахуємо основні адміністративні заходи захисту.

1. Постійний контроль коректності функціонування ОС, особливо її підсистеми захисту. Такий контроль зручно організувати, якщо ОС підтримує автоматичну реєстрацію найбільш важливих подій (event logging) в спеціальному журналі.
2. Організація і підтримка адекватної політики безпеки. Політики безпеки ОС повинна постійно коригуватися, оперативно реагуючи на спроби зловмисників здолати захист ОС, а також на зміни в конфігурації ОС, установку і видалення застосовних програм.
3. Інструктаж користувачів операційної системи про необхідність дотримання заходів безпеки при роботі з ОС і контроль за дотриманням цих заходів.
4. Регулярне створення і оновлення резервних копій програм і цих ОС.
5. Постійний контроль змін в конфігураційних даних і політиці безпеки ОС. Інформацію про ці зміни доцільно зберігати на неелектронних носіях інформації, для того, щоб зловмисникові, що здолав захист ОС, було важче замаскувати свої несанкціоновані дії.

У конкретних ОС можуть знадобитися і інші адміністративні заходи захисту інформації [56].

Адекватна політика безпеки

Вибір і підтримка адекватної політики безпеки є одним з найбільш важливих завдань адміністратора ОС. Якщо прийнята в ОС політика безпеки неадекватна, то це може привести до НСД зловмисника до ресурсів системи і до зниження надійності функціонування ОС.

Відоме твердження: чим краще захищена ОС, тим важче з нею працювати користувачам і адміністраторам. Це обумовлено наступними чинниками:

- система захисту не завжди здатна визначити, чи є деяка дія користувача зловмисною. Тому система захисту або не присікає деякі види НСД, або забороняє деякі цілком легальні дії користувачів. Чим вище захищеність системи, тим ширше клас тих легальних дій користувачів, які розглядаються підсистемою захисту як несанкціоновані;
- будь-яка система, в якій передбачені функції захисту інформації, вимагає від адміністраторів певних зусиль, спрямованих на підтримку адекватної політики безпеки. Чим більше в ОС захисних функцій, тим більше часу і засобів треба витрачати на підтримку захисту;
- підсистема захисту ОС, як і будь-який інший програмний пакет, споживає апаратні ресурси комп'ютера. Чим складніше влаштовані захисні функції ОС, тим більше ресурсів комп'ютера (процесорного часу, оперативної пам'яті та ін.)

витрачається на підтримку функціонування підсистеми захисту і тим менше ресурсів залишається на долю застосовних програм;

• підтримка занадто жорсткої політики безпеки може негативно позначитися на надійності функціонування ОС. Надмірно жорстка політика безпеки може привести до помилок, що важко виявляються, і збоїв в процесі функціонування ОС і навіть до її краху [56, 88].

Оптимальна адекватна політика безпеки — це така політика безпеки, яка не лише не дозволяє зловмисникам виконувати несанкціоновані дії, але і не призводить до описаних вище негативних ефектів.

Адекватна політика безпеки визначається не лише архітектурою ОС, але і її конфігурацією, встановленими застосовними програмами і т. д. Формування і підтримку адекватної політики безпеки ОС можна розділити на ряд етапів.

1. Аналіз загроз. Адміністратор ОС розглядає можливі загрози безпеки цього екземпляра ОС. Серед можливих загроз виділяються найбільш небезпечні, захисту від яких треба приділяти максимум засобів.

2. Формування вимог до політики безпеки. Адміністратор визначає, які засоби і методи застосовуватимуться для захисту від тих або інших загроз. Наприклад, захист від НСД до деякого об'єкту ОС можна вирішувати або засобами розмежування доступу, або криптографічними засобами, або використовуючи деяку комбінацію цих засобів.

3. Формальне визначення політики безпеки. Адміністратор визначає, як конкретно повинні виконуватися вимоги, сформульовані на попередньому етапі. Формулюються необхідні вимоги до конфігурації ОС, а також вимоги до конфігурації додаткових пакетів захисту, якщо установка таких пакетів потрібна. Результатом цього етапу є розгорнутий перелік налаштувань конфігурації ОС і додаткових пакетів захисту з вказівкою того, в яких ситуаціях, які налаштування мають бути встановлені.

4. Втілення в життя політики безпеки. Завданням цього етапу є приведення конфігурації ОС і додаткових пакетів захисту у відповідність з політикою безпеки, формально визначеної на попередньому етапі.

5. Підтримка і корекція політики безпеки. У завдання адміністратора на цьому етапі входить контроль дотримання політики безпеки і внесення в неї необхідних змін у міру появи змін у функціонуванні ОС.

Спеціальних стандартів захищеності ОС не існує. Для оцінки захищеності ОС використовуються стандарти, розроблені для комп'ютерних систем взагалі. Як правило, сертифікація ОС по деякому класу захисту супроводжується складанням вимог до адекватної політики безпеки, при безумовному виконанні якої захищеність конкретного екземпляра ОС відповідатиме вимогам відповідного класу захисту.

Визначаючи адекватну політику безпеки, адміністратор ОС повинен в першу чергу орієнтуватися на захист ОС від конкретних загроз її безпеки [56, 88].

8.2. Архітектура підсистеми захисту ОС

8.2.1. Основні функції підсистеми захисту ОС

Підсистема захисту ОС виконує наступні основні функції.

1. Ідентифікація і аутентифікація. Жоден користувач не може почати роботу з ОС, не ідентифікував себе і не надавши системі аутентифікуючу інформацію, що підтверджує, що користувач дійсно являється тим, ким він себе заявляє.

2. Розмежування доступу. Кожен користувач системи має доступ тільки до тих об'єктів ОС, до яких йому наданий доступ відповідно до поточної політики безпеки.

3. Аудит. ОС реєструє в спеціальному журналі події, потенційно небезпечні для підтримки безпеки системи.

4. Управління політикою безпеки. Політика безпеки повинна постійно підтримуватися в адекватному стані, т. е. повинна гнучко реагувати на зміни умов функціонування ОС. Управління політикою безпеки здійснюється адміністраторами системи з використанням відповідних засобів, вбудованих в ОС.

5. Криптографічні функції. Захист інформації немислимий без використання криптографічних засобів захисту. Шифрування використовується в ОС при зберіганні і передачі по каналах зв'язку паролів користувачів і деяких інших даних, критичних для безпеки системи.

6. Мережеві функції. Сучасні ОС, як правило, працюють не ізольовано, а у складі локальних і/або глобальних комп'ютерних мереж. ОС комп'ютерів, що входять в одну мережу, взаємодіють між собою для вирішення різних завдань, у тому числі і завдань, що мають пряме відношення до захисту інформації.

Підсистема захисту зазвичай не є єдиним програмним модулем. Як правило, кожна з перерахованих функцій підсистеми захисту вирішується одним або декількома програмними модулями. Деякі функції вбудовуються безпосередньо в ядро ОС. Між різними модулями підсистеми захисту повинен існувати чітко певний інтерфейс, використовуваний при взаємодії модулів для вирішення загальних завдань.

У таких ОС, як Windows, підсистема захисту чітко виділяється в загальній архітектурі ОС, в інших, як UNIX, захисні функції розподілені практично по усіх елементах ОС. Проте будь-яка ОС, що задовольняє стандарту захищеності, повинна містити підсистему захисту, що виконує усі вище перелічені функції. Зазвичай підсистема захисту ОС допускає розширення додатковими програмними модулями [56, 88].

8.2.2. Ідентифікація, аутентифікація і авторизація суб'єктів доступу

У захищеній ОС будь-який користувач (суб'єкт доступу), перш ніж почати роботу з системою, повинен пройти ідентифікацію, аутентифікацію і авторизацію. Суб'єктом доступу (чи просто суб'єктом) називають будь-яку суть, здатну ініціювати виконання операцій над елементами ОС. Зокрема, користувачі є суб'єктами доступу.

Ідентифікація суб'єкта доступу полягає в тому, що суб'єкт повідомляє ОС ідентифікуючу інформацію про себе (ім'я, обліковий номер і т. д.) і таким чином ідентифікує себе.

Для того, щоб встановити, що користувач саме той, за кого себе видає, в інформаційних системах передбачена процедура аутентифікації, завдання якої — запобігання доступу до системи небажаних осіб.

Аутентифікація суб'єкта доступу полягає в тому, що суб'єкт надає ОС окрім ідентифікуючої інформації ще і аутентифікуючу інформацію, що підтверджує, що він дійсно є тим суб'єктом доступу, до якого відноситься ідентифікуюча інформація (див. л. 7).

Авторизація суб'єкта доступу відбувається після успішної ідентифікації і аутентифікації. При авторизації суб'єкта ОС виконує дії, необхідні для того, щоб суб'єкт міг почати роботу в системі. Наприклад, авторизація користувача в операційній системі UNIX включає породження процесу, що є операційною оболонкою, з якою в подальшому працюватиме користувач. У ОС Windows NT авторизація користувача включає створення маркера доступу користувача, створення робочого столу і запуск на нім від імені авторизуючого користувача процесу Userinit, що ініціалізував індивідуальне програмне середовище користувача. Авторизація суб'єкта не відноситься безпосередньо до підсистеми зашиті ОС. В процесі авторизації вирішуються технічні завдання, пов'язані з організацією початку роботи в системі вже ідентифікованого і аутентифікованного суб'єкта доступу.

З точки зору забезпечення безпеки ОС процедури ідентифікації і аутентифікації є дуже відповідальними. Дійсно, якщо зловмисник зумів увійти до системи від імені іншого користувача, він легко дістає доступ до усіх об'єктів ОС, до яких має доступ цей користувач. Якщо при цьому підсистема аудиту генерує повідомлення про події, потенційно небезпечні для безпеки ОС, то в журнал аудиту записується не ім'я зловмисника, а ім'я користувача, від імені якого зловмисник працює в системі.

Методи ідентифікації і аутентифікації за допомогою імені і пароля, зовнішніх носіїв ключової інформації, біометричних характеристик користувачів детально розглянуті в л. 7.

8.2.3. Розмежування доступу до об'єктів ОС

Основними поняттями процесу розмежування доступу до об'єктів ОС є об'єкт доступу, метод доступу до об'єкту і суб'єкт доступу.

Об'єктом доступу (чи просто об'єктом) називають будь-який елемент ОС, доступ до якого користувачів і інших суб'єктів доступу може бути довільно обмежений. Можливість доступу до об'єктів ОС визначається не лише архітектурою ОС, але і поточною політикою безпеки. Під об'єктами доступу розуміють як ресурси устаткування (процесор, сегменти пам'яті, принтер, диски і стрічки), так і програмні ресурси (файли, програми, семафори), т. е. все те, доступ до чого контролюється. Кожен об'єкт має унікальне ім'я, що відрізняє його від інших об'єктів в системі, і кожен з них може бути доступний через добре певні і значимі операції.

Методом доступу до об'єкту називається операція, визначена для об'єкту. Тип операції залежить від об'єктів. Наприклад, процесор може тільки виконувати команди, сегменти пам'яті можуть бути записані і прочитані, считиватель магнітних карт може тільки читати, а для файлів можуть бути визначені методи доступу «читання», «запис» і «додавання» (дописування інформації в кінець файлу).

Суб'єктом доступу називають будь-яку суть, здатну ініціювати виконання операцій над об'єктами (звертатися до об'єктів по деяких методах доступу). Зазвичай вважають, що безліч суб'єктів доступу і безліч об'єктів доступу не перетинаються. Іноді до суб'єктів доступу відносять процеси, що виконуються в системі. Проте логічніше вважати суб'єктом доступу саме користувача, від імені якого виконується процес. Природно, під суб'єктом доступу мають на увазі не фізичного користувача, працюючого з комп'ютером, а «логічного» користувача, від імені якого виконуються процеси ОС.

Таким чином, об'єкт доступу — це те, до чого здійснюється доступ, суб'єкт доступу — це той, хто здійснює доступ, і метод доступу — це те, як здійснюється доступ.

Для об'єкту доступу може бути визначений власник — суб'єкт, якому належить цей об'єкт і який несе відповідальність за конфіденційність інформації, що міститься в об'єкті, а також за цілісність і доступність об'єкту.

Зазвичай власником об'єкту автоматично призначається суб'єкт, що створив цей об'єкт, надалі власник об'єкту може бути змінений з використанням відповідного методу доступу до об'єкту. На власника, як правило, покладається відповідальність за коректне обмеження прав доступу до цього об'єкту інших суб'єктів.

Правом доступу до об'єкту називають право на виконання доступу до об'єкту по деякому методу або групі методів. Наприклад, якщо користувач має можливість читати файл, говорять, що він має право на читання цього файлу. Говорять, що суб'єкт має деякий привілей, якщо він має право на доступ по деякому методу або групі методів до усіх об'єктів ОС, що підтримують цей метод доступу.

Розмежуванням доступу суб'єктів до об'єктів є сукупність правил, визначальна для кожної трійки суб'єкт-об'єкт-метод, чи дозволений доступ цього суб'єкта до даному об'єкту по цьому методу. При вибірковому розмежуванні доступу можливість доступу визначена однозначно для кожної трійки суб'єкт-об'єкт-метод, при повноважному розмежуванні доступу ситуація дещо складніша.

Суб'єкта доступу називають суперкористувачем, якщо він має можливість ігнорувати правила розмежування доступу до об'єктів.

Правила розмежування доступу, що діють в ОС, встановлюються адміністраторами системи при визначенні поточної політики безпеки. За дотриманням цих правил суб'єктами доступу стежить монітор посилань — частина підсистеми захисту ОС.

Правила розмежування доступу повинні задовольняти наступним вимогам.

1. Відповідати аналогічним правилам, прийнятим в організації, в якій встановлена ОС. Іншими словами, якщо згідно з правилами організації доступ користувача до деякої інформації вважається несанкціонованим, цей доступ має бути йому заборонений.
2. Не повинні допускати руйнівні дії суб'єктів доступу на ОС, що виражаються в несанкціонованій зміні, видаленні або іншій дії на об'єкти, життєво важливі для нормальної роботи ОС.
3. Будь-який об'єкт доступу повинен мати власника. Неприпустимо присутність нічийних об'єктів — об'єктів, що не мають власника.
4. Не допускати присутності недоступних об'єктів — об'єктів, до яких не може звернутися жоден суб'єкт доступу ні по одному методу доступу.

5. Не допускати просочування конфіденційної інформації.

Існують дві основні моделі розмежування доступу:

- вибіркове (дискреційне) розмежування доступу;
- повноважне (мандатне) розмежування доступу.

При вибірковому розмежуванні доступу певні операції над конкретним ресурсом забороняються або дозволяються суб'єктам або групам суб'єктів. Більшість ОС реалізують саме вибіркове розмежування доступу (discretionary access control).

Повноважне розмежування доступу полягає в тому, що усі об'єкти можуть мати рівні секретності, а усі суб'єкти діляться на групи, що утворюють ієрархію відповідно до урівноваження допуску до інформації. Іноді цю модель називають моделлю багаторівневої безпеки, призначеної для зберігання секретів.

Вибіркове розмежування доступу

Система правил вибіркового розмежування доступу формулюється таким чином.

1. Для будь-якого об'єкту ОС існує власник.
2. Власник об'єкту може довільно обмежувати доступ інших суб'єктів до цього об'єкту.
3. Для кожної трійки суб'єкт-об'єкт-метод можливість доступу визначена однозначно.
4. Існує хоч би один привілейований користувач (адміністратор), що має можливість звернутися до будь-якого об'єкту по будь-якому методу доступу.

Привілейований користувач не може ігнорувати розмежування доступу до об'єктів. Наприклад, в Windows адміністратор для звернення до чужого об'єкту (що належить іншому суб'єктові) повинен спочатку оголосити себе власником цього об'єкту, використавши привілей адміністратора оголошувати себе власником будь-якого об'єкту, потім надати собі необхідні права і тільки після цього може звернутися до об'єкту. Остання вимога введена для реалізації механізму видалення потенційно недоступних об'єктів.

При створенні об'єкту його власником призначається суб'єкт, що створив цей об'єкт. Надалі суб'єкт, що має необхідні права, може призначити об'єкту нового власника. При цьому суб'єкт, що змінює власника об'єкту, може призначити новим власником об'єкту тільки себе. Таке обмеження вводиться для того, щоб власник об'єкту не міг віддати «володіння» об'єктом іншому суб'єктові і тим самим зняти з себе відповідальність за некоректні дії з об'єктом.

Для визначення прав доступу суб'єктів до об'єктів при вибірковому розмежуванні доступу використовуються такі поняття, як матриця доступу і домен безпеки.

З концептуальної точки зору поточний стан прав доступу при вибірковому розмежуванні доступу описується матрицею, в рядках якої перераховані суб'єкти доступу, в стовпцях — об'єкти доступу, а в комірках — операції, які суб'єкт може виконати над об'єктом.

Домен безпеки (protection domain) визначає набір об'єктів і типів операцій, які можуть робитися над кожним об'єктом ОС.

Можливість виконувати операції над об'єктом є право доступу, кожне з яких є впорядкована пара <objectname, rightsset>. Таким чином, домен є набір прав доступу. Наприклад, якщо домен D має право доступу <file F, (read, write}>, це

означає, що процес, що виконується в домені D, може читати або писати у файл F, але не може виконувати інших операцій над цим об'єктом (Рис. 8.1).

Об'єкт / Домен	F1	F2	F3	Printer
D1	read		execute	
D2		read		
D3				print
D4	read write		read write	

Рис. 8.1. Специфікація прав доступу до ресурсів

Зв'язок конкретних суб'єктів, що функціонують в ОС, може бути організований таким чином:

- кожен користувач може бути доменом. В цьому випадку набір об'єктів, до яких може бути організований доступ, залежить від ідентифікації користувача;
- кожен процес може бути доменом. В цьому випадку набір доступних об'єктів визначається ідентифікацією процесу;
- кожна процедура може бути доменом. В цьому випадку набір доступних об'єктів відповідає локальним змінним, визначеним усередині процедури. Помітимо, що, коли процедура виконана, відбувається зміна домена.

Модель безпеки, специфікована вище (див. Рис. 8.1), має вигляд матриці і називається матрицею доступу. Стовпці цієї матриці є об'єктами, рядками — суб'єкти. У кожному осередку матриці зберігається сукупність прав доступу, наданих цьому суб'єктові на цей об'єкт.

Оскільки реальна матриця доступу дуже велика (типовий об'єм для сучасної ОС складає декілька десятків мегабайтів), матрицю доступу ніколи не зберігають в системі в явному виді. У загальному випадку ця матриця буде розрідженою, т. е. більшість її клітин будуть порожніми. Матрицю доступу можна розкласти по стовпцях, внаслідок чого виходять списки прав доступу ACL (access control list). В результаті розкладання матриці по рядках виходять мандати можливостей (capability list, або capability tickets).

Список прав доступу ACL. Кожна колонка в матриці може бути реалізована як список доступу для одного об'єкту. Очевидно, що порожні клітини можуть не враховуватися. В результаті для кожного об'єкту маємо список впорядкованих пар <domain, rightsset>, який визначає усі домени з непорожніми наборами прав для цього об'єкту.

Елементами списку прав доступу ACL можуть бути процеси, користувачі або групи користувачів. При реалізації широко застосовується надання доступу за умовчанням для користувачів, права яких не вказані. Наприклад, в ОС Unix усі субъекти користувачі розділені на три групи (власник, група і інші), і для членів кожної групи контролюються операції читання, записи і виконання (rwx). У результаті маємо ACL — 9битний код, який є атрибутом різноманітних об'єктів Unix.

Мандати можливостей. Як відзначалося вище, якщо матрицю доступу зберігати по рядках, т. е. якщо кожен суб'єкт зберігає список об'єктів і для кожного об'єкту — список допустимих операцій, то такий спосіб зберігання називається «Мандати можливостей» або «переліки можливостей» (capability list). Кожен користувач має декілька мандатів і може мати право передавати їх іншим. Мандати можуть бути розсіяні по системі і внаслідок цього представляти велику загрозу для безпеки, чим списки контролю доступу. Їх зберігання має бути ретельно продумане.

Вибіркове розмежування доступу — найбільш поширений спосіб розмежування доступу. Це обумовлено порівняльною простотою його реалізації і необтяжливістю правил такого розмежування доступу для користувачів. Головне достоїнство вибіркового розмежування доступу — гнучкість; основні недоліки — розосередженість управління і складність централізованого контролю.

В той же час, захищеність ОС, підсистема захисту якої реалізує тільки вибіркове розмежування доступу, в деяких випадках може виявитися недостатньою. Зокрема, в США заборонено зберігати інформацію, що містить державну таємницю, в комп'ютерних системах, що підтримують тільки вибіркове розмежування доступу.

Розширенням моделі вибіркового розмежування доступу є ізольоване (чи замкнута) програмне середовище.

При використанні ізольованого програмного середовища права суб'єкта на доступ до об'єкту визначаються не лише правами і привілеями суб'єкта, але і процесом, за допомогою якого суб'єкт звертається до об'єкту. Можна, наприклад, дозволити звертатися до файлів з розширенням .doc тільки програмам Word, Word Viewer і WPview.

Ізольоване програмне середовище істотно підвищує захищеність операційної системи від руйнівних програмних дій, включаючи програмні закладки і комп'ютерні віруси. Крім того, при використанні цієї моделі підвищується захищеність цілісності даних, що зберігаються в системі.

Повноважне розмежування доступу з контролем інформаційних потоків

Повноважне, або мандатне, розмежування доступу (mandatory access control) зазвичай застосовується в сукупності з виборчим розмежуванням доступу. Розглянемо саме такий випадок [56]. Правила розмежування доступу в цій моделі формулюються таким чином.

1. Для будь-якого об'єкту ОС існує власник.
2. Власник об'єкту може довільно обмежувати доступ інших суб'єктів до цього об'єкту.
3. Для кожної четвірки суб'єкт-об'єкт-метод-процес можливість доступу визначена однозначно в кожен момент часу. При зміні стану процесу з часом можливість надання доступу також може змінитися. В той же час, в кожен момент часу можливість доступу визначена однозначно. Оскільки права процесу на доступ до об'єкту міняються з часом, вони повинні перевірятися не лише при відкритті об'єкту, але і перед виконанням над об'єктом таких операцій, як читання і запис.
4. Існує хоч би один привілейований користувач (адміністратор), що має можливість видалити будь-який об'єкт.
5. У безлічі об'єктів виділяється безліч об'єктів повноважного розмежування доступу. Кожен об'єкт повноважного розмежування доступу має

гриф секретності. Чим вище числове значення грифа секретності, тим секретніший об'єкт. Нульове значення грифа секретності означає, що об'єкт несекретний. Якщо об'єкт не є об'єктом повноважного розмежування доступу або якщо об'єкт несекретний, адміністратор може звернутися до нього по будь-якому методу, як і в попередній моделі розмежування доступу.

6. Кожен суб'єкт доступу має рівень допуску. Чим вище числове значення рівня допуску, тим більший допуск має суб'єкт. Нульове значення рівня допуску означає, що суб'єкт не має допуску. Зазвичай ненульове значення допуску призначається тільки суб’єкту користувачу і не призначається суб'єктам, від імені яких виконуються системні процеси.

7. Доступ суб'єкта до об'єкту має бути заборонений незалежно від стану матриці доступу, якщо:

- об'єкт є об'єктом повноважного розмежування доступу;
- гриф секретності об'єкту строго вище за рівень допуску суб'єкта, що звертається до нього;
- суб'єкт відкриває об'єкт в режимі, що допускає читання інформації.

Це правило називають правилом NRU (Not Read Up — не читати вище).

8. Кожен процес ОС має рівень конфіденційності, рівний максимуму з грифів секретності об'єктів, відкритих процесом упродовж свого існування. Рівень конфіденційності фактично є гриф секретності інформації, що зберігається в оперативній пам'яті процесу.

9. Доступ суб'єкта до об'єкту має бути заборонений незалежно від стану матриці доступу, якщо:

- об'єкт є об'єктом повноважного розмежування доступу;
- гриф секретності об'єкту строго нижче рівня конфіденційності процесу, що звертається до нього;
- суб'єкт збирається записувати в об'єкт інформацію

Це правило запобігає просочуванню секретної інформації; його називають правило NWD (Not Write Down — не записувати нижче).

10. Знизити гриф секретності об'єкту повноважного розмежування доступу може тільки суб'єкт, який:

- має доступ до об'єкту згідно з правилом 7;
- має спеціальний привілей, що дозволяє йому знижувати грифи секретності об'єктів.

При використанні цієї моделі розмежування доступу істотно страждає продуктивність ОС, оскільки права доступу до об'єкту повинні перевірятися не лише при відкритті об'єкту, але і при кожній операції читання/запис. Крім того, ця модель створює користувачам певні незручності: якщо рівень конфіденційності процесу строго вище за нуль, то уся інформація в пам'яті процесу фактично є секретною і не може бути записана в несекретний об'єкт.

Якщо процес одночасно працює з двома об'єктами, тільки один з яких є секретним, то він не може записувати інформацію з пам'яті в другий об'єкт. Ця проблема вирішується за допомогою використання спеціального програмного інтерфейсу API для роботи з пам'яттю. Області пам'яті, що виділяються процесам, можуть бути описані як об'єкти повноважного розмежування доступу, після чого їм можуть призначатися грифи секретності.

При читанні секретного файлу процес повинен рахувати вміст такого файлу в секретну область пам'яті, використовуючи для цього функції ОС, просочування інформації, що гарантують неможливість. Для роботи з секретною областю пам'яті процес також повинен використати спеціальні функції. Оскільки просочування інформації з секретних областей пам'яті в пам'ять процесу неможливе, читання процесом секретної інформації в секретні області пам'яті не відображається на рівні конфіденційності процесу. Якщо ж процес читає секретну інформацію в область пам'яті, не описану як об'єкт повноважного розмежування доступу, підвищується рівень конфіденційності процесу.

З вищевикладеного виходить, що користувачі ОС, що реалізовують цю модель розмежування доступу, вимушені використати ПЗ, розроблене з урахуванням цієї моделі. Інакше вони зазнаватимуть серйозні проблеми в

процесі роботи з об'єктами ОС, що мають ненульовий гриф секретності.

Кожна з розглянутих моделей розмежування доступу має свої достоїнства і недоліки.

У більшості ситуацій застосування вибіркового розмежування доступу найефективніше. Ізольоване програмне середовище доцільно використати у випадках, коли важливо забезпечити цілісність програм і цих ОС. Повноважне розмежування доступу з контролем інформаційних потоків слід застосовувати в тих випадках, коли для організації надзвичайно важливе забезпечення захищеності системи від несанкціонованого просочування інформації. У інших ситуаціях застосування цієї моделі недоцільне изза різкого погіршення експлуатаційних якостей ОС.

8.2.4. Аудит

Процедура аудиту стосовно ОС полягає в реєстрації в спеціальному журналі, що називається журналом аудиту або журналом безпеки, подій, які можуть представляти небезпеку для ОС. Користувачі системи, що мають право читання журнал аудиту, називаються аудиторами.

Необхідність включення в захищену ОС функцій аудиту обумовлена наступними обставинами:

- виявлення спроб вторгнення є найважливішим завданням системи захисту, оскільки її рішення дозволяє мінімізувати збиток від злому і збирати інформацію про методи вторгнення;
- підсистема захисту ОС може не відрізнити випадкові помилки користувачів від зловмисних дій. Адміністратор, переглядаючи журнал аудиту, зможе встановити, що сталося при введенні користувачем неправильного пароля — помилка легального користувача або атака зловмисника. Якщо користувач намагався вгадати пароль 20-30 разів, то це явна спроба підбору пароля;
- адміністратори ОС повинні мати можливість отримувати інформацію не лише про поточний стан системи, але і про те, як ОС функціонувала в недавньому минулому. Таку можливість забезпечує журнал аудиту;
- якщо адміністратор ОС виявив, що проти системи проведена успішна атака, йому важливо з'ясувати, коли була розпочата атака і яким чином вона здійснювалася. Журнал аудиту може містити усю необхідну інформацію.

До числа подій, які можуть представляти небезпеку для ОС, зазвичай відносять наступні:

- вхід або вихід з системи;
- операції з файлами (відкрити, закрити, перейменувати, видалити);
- звернення до видаленої системи;
- зміну привілеїв або інших атрибутів безпеки (режиму доступу, рівня благонадійності користувача і т. д.).

Якщо фіксувати в журналі аудиту усі події, об'єм реєстраційної інформації буде рости занадто швидко, що утруднить її ефективний аналіз. Необхідно передбачити вибіркове протоколювання як відносно користувачів, так і відносно подій.

Вимоги до аудиту. Підсистема аудиту ОС повинна задовольняти наступним вимогам.

1. Додавати запису в журнал аудиту може тільки ОС. Якщо надати це право какомуто фізичному користувачеві, цей користувач отримає можливість компрометувати інших користувачів, додаючи в журнал аудиту відповідні записи.
2. Редагувати або видаляти окремі записи в журналі аудиту не може жоден суб'єкт доступу, у тому числі і сама ОС.
3. Переглядати журнал аудиту можуть тільки користувачі, що мають відповідний привілей.
4. Очищати журнал аудиту можуть тільки пользователиаудитори. Після очищення журналу в нього автоматично вноситься запис про те, що журнал аудиту був очищений, з вказівкою часу очищення журналу і імені користувача, що очистив журнал. ОС повинна підтримувати можливість збереження журналу аудиту перед очищенням в іншому файлі.
5. При переповнюванні журналу аудиту ОС аварійно завершує роботу («зависає»). Після перезавантаження працювати з системою можуть тільки аудитори. ОС переходить до звичайного режиму роботи тільки після очищення журналу аудиту.

Для обмеження доступу до журналу аудиту повинні застосовуватися спеціальні засоби захисту.

Політика аудиту — це сукупність правил, визначальних, які події повинні реєструватися в журналі аудиту. Для забезпечення надійного захисту ОС в журналі аудиту повинні обов'язково реєструватися наступні події:

- спроби входу/виходу користувачів з системи;
- спроби зміни списку користувачів;
- спроби зміни політики безпеки, у тому числі і політики аудиту.

Остаточний вибір подій, які повинні реєструватися в журналі аудиту, покладається на аудиторів. При виборі оптимальної політики аудиту слід враховувати очікувану швидкість заповнення журналу аудиту. Політика аудиту повинна оперативно реагувати на зміни в конфігурації ОС, в характері інформації, що зберігається і оброблюваної, і особливо на виявлені спроби атаки ОС.

У деяких ОС підсистема аудиту окрім запису інформації про зареєстровані події в спеціальний журнал передбачає можливість інтерактивного сповіщення аудиторів про ці події.

Лекція 9 ТЕХНОЛОГІЙ МІЖМЕРЕЖЕВИХ ЕКРАНІВ

Міжмережевий екран (МЕ) — це спеціалізований комплекс міжмережевого захисту, що називається також брандмауером або системою firewall. МЕ дозволяє розділити загальну мережу на дві частини (чи більше) і реалізувати набір правил, що визначають умови проходження пакетів з даними через кордон з однієї частини загальної мережі в іншу. Як правило, ця межа проводиться між корпоративною (локальною) мережею підприємства і глобальною мережею Internet.

Зазвичай МЕ захищають внутрішню мережу підприємства від «вторгнень» з глобальної мережі Internet, хоча вони можуть використовуватися і для захисту від «нападів» з корпоративної інтрамережі, до якої підключена локальна мережа підприємства. Технологія МЕ одна з найперших технологій захисту корпоративних мереж від зовнішніх загроз.

Для більшості організацій установка МЕ є необхідною умовою забезпечення безпеки внутрішньої мережі.

9.1. Функції МЕ

Для протидії несанкціонованому міжмережевому доступу МЕ повинен розташовуватися між мережею організації, внутрішньої, що являється, що захищається, і потенційно ворожою зовнішньою мережею (Рис. 9.1). При цьому усі взаємодії між цими мережами повинні здійснюватися тільки через МЕ. Організаційно МЕ входить до складу мережі, що захищається.

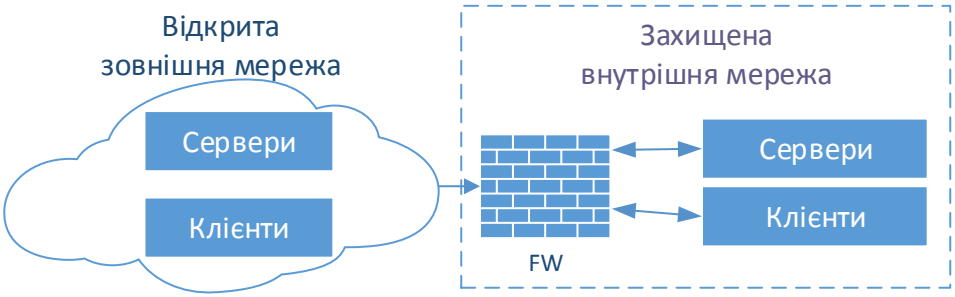

Рис. 9.1. Схема підключення міжмережевого екрану МЕ

МЕ, що захищає відразу безліч вузлів внутрішньої мережі, покликаний вирішити:

- завдання обмеження доступу зовнішніх (по відношенню до мережі, що захищається) користувачів до внутрішніх ресурсів корпоративній мережі. До таких користувачів можуть бути віднесені партнери, видалені користувачі, хакери і навіть співробітники самої компанії, що намагаються отримати доступ до серверів баз даних, МЕ, що захищаються;
- завдання розмежування доступу користувачів мережі, що захищається, до зовнішніх ресурсів. Рішення цієї задачі дозволяє, наприклад, регулювати доступ до серверів, що не вимагаються для виконання службових обов'язків.

Досі не існує єдиної загальновизнаної класифікації МЕ. Їх можна класифікувати, наприклад, за наступними основними ознаками [32].

По функціонуванню на рівнях моделі OSI:

- пакетний фільтр (екрануючий маршрутизатор — screening router);
- шлюз сеансового рівня (екрануючий транспорт);
- прикладний шлюз (application gateway);
- шлюз експертного рівня (stateful inspection firewall).

За використовуваною технологією:

- контроль стану протоколу (stateful inspection);
- на основі модулів посередників (proxy).

По виконанню:

- апаратно програмний;
- програмний.

За схемою підключення:

- схема єдиного захисту мережі;
- схема із закритим, що захищається, і відкритим, що не захищається, сегментами мережі;
- схема з роздільним захистом закритого і відкритого сегментів мережі.

9.1.1. Фільтрація трафіку

Фільтрація інформаційних потоків полягає в їх вибірковому пропусканні через екран, можливо, з виконанням деяких перетворень [9, 32]. Фільтрація здійснюється на основі набору заздалегідь завантажених в МЕ правил, таких, що відповідають прийнятій політиці безпеки. Тому МЕ зручно представляти як послідовність фільтрів, оброблювальних інформаційний потік (Рис. 9.2).

Рис. 9.2. Структура міжмережевого екрану

Кожен з фільтрів призначений для інтерпретації окремих правил фільтрації шляхом:

1) аналізу інформації за заданими в правилах, що інтерпретуються, критеріями, наприклад по адресах одержувача і відправника або за типом додатка, для якого ця інформація призначена;

2) прийняття на основі правил одного з наступних рішень, що інтерпритуються:

- не пропустити дані;
- обробити дані від імені одержувача і повернути результат відправнику;
- передати дані на наступний фільтр для продовження аналізу;
- пропустити дані, ігноруючи наступні фільтри.

Правила фільтрації можуть задавати і додаткові дії, які відносяться до функцій посередництва, напри заходів перетворення даних, реєстрація подій та ін. Відповідно правила фільтрації визначають перелік умов, по яких здійснюється:

- дозвіл або заборона подальшої передачі даних;
- виконання додаткових захисних функцій.

Як критерії аналізу інформаційного потоку можуть використовуватися наступні параметри:

- службові поля пакетів повідомлень, що містять мережеві адреси, ідентифікатори, адреси інтерфейсів, номери портів і інші значимі дані;
- безпосередній вміст пакетів повідомлень, що перевіряється, наприклад, на наявність комп'ютерних вірусів;
- зовнішні характеристики потоку інформації, наприклад, тимчасові, частотні характеристики, об'єм даних і т. д.

Використовувані критерії аналізу залежать від рівнів моделі OSI, на яких здійснюється фільтрація. У загальному випадку, чим вище рівень моделі OSI, на якому МЕ фільтрує пакети, тим вище і забезпечуваний ним рівень захисту.

9.1.2. Виконання функцій посередництва

Функції посередництва МЕ виконує за допомогою спеціальних програм, що називаються екрануючими агентами або програмами посередники. Ці програми є резидентними і забороняють безпосередню передачу пакетів повідомлень між зовнішньою і внутрішньою мережею.

При необхідності доступу з внутрішньої мережі в зовнішню мережу або навпаки спочатку має бути встановлене логічне з'єднання з програмою посередником, що функціонує на комп'ютері МЕ. Програма посередник перевіряє допустимість запрошеної міжмережевої взаємодії і при його дозволі сама встановлює окреме з'єднання з необхідним комп'ютером. Далі обмін інформацією між комп'ютерами внутрішньої і зовнішньої мережі здійснюється через програмного посередника, який може виконувати фільтрацію потоку повідомлень, а також здійснювати інші захисні функції.

Слід мати на увазі, що МЕ може виконувати функції фільтрації без застосування програм посередників, забезпечуючи прозору взаємодію між внутрішньою і зовнішньою мережею. В той же час програмні посередники можуть і не здійснювати фільтрацію потоку повідомлень.

У загальному випадку програми посередники, блокуючи прозору передачу потоку повідомлень, можуть виконувати наступні функції:

- перевірку достовірності передаваних даних;
- фільтрацію і перетворення потоку повідомлень, наприклад, динамічний пошук вірусів і прозоре шифрування інформації;
- розмежування доступу до ресурсів внутрішньої мережі;
- розмежування доступу до ресурсів зовнішньої мережі;
- кешування даних, що просяться із зовнішньої мережі;
- ідентифікацію і аутентифікацію користувачів;
- трансляцію внутрішніх мережевих адрес для витікаючих пакетів повідомлень;

- реєстрацію подій, реагування на події, що задаються, а також аналіз зареєстрованої інформації і генерацію звітів [9, 32].

Програми посередники можуть здійснювати перевірку достовірності отримуваних і передаваних даних. Це актуально не лише для аутентифікації електронних повідомлень, але і мігруючих програм (Java, ActiveX Controls), по відношенню до яких може бути виконана підробка. Перевірка достовірності повідомлень і програм полягає в контролі їх цифрових підписів.

Програми посередники можуть виконувати розмежування доступу до ресурсів внутрішньої або зовнішньої мережі, використовуючи результати ідентифікації і аутентифікації користувачів при їх зверненні до МЕ.

Способи розмежування доступу до ресурсів внутрішньої мережі практично не відрізняються від способів розмежування, підтримуваних на рівні операційної системи.

При розмежуванні доступу до ресурсів зовнішньої мережі найчастіше використовується один з наступних підходів:

- дозвіл доступу тільки по заданих адресах в зовнішній мережі;
- фільтрація запитів на основі оновлюваних списків неприпустимих адрес і блокування пошуку інформаційних ресурсів за небажаними ключовими словами;
- накопичення і оновлення адміністратором санкціонованих інформаційних ресурсів зовнішньої мережі в дискової пам'яті МЕ і повна заборона доступу в зовнішню мережу.

За допомогою спеціальних посередників підтримується також кешування даних, що просяться із зовнішньої мережі. При доступі користувачів внутрішньої мережі до інформаційних ресурсів зовнішньої мережі уся інформація накопичується на просторі жорсткого диска МЕ, що називається в цьому випадку proxy сервером. Тому якщо при черговому запиті потрібна інформація виявиться на proxy сервер, то посередник надає її без звернення до зовнішньої мережі, що істотно прискорює доступ. Адміністраторові слід потурбуватися тільки про періодичне оновлення вмісту proxy сервера.

Функція кешування успішно може використовуватися для обмеження доступу до інформаційних ресурсів зовнішньої мережі. В цьому випадку усі санкціоновані інформаційні ресурси зовнішньої мережі накопичуються і оновлюються адміністратором на proxy сервері. Користувачам внутрішньої мережі дозволяється доступ тільки до інформаційних ресурсів proxy сервера, а безпосередній доступ до ресурсів зовнішньої мережі забороняється.

Фільтрація і перетворення потоку повідомлень виконується посередником на основі заданого набору правил. Тут слід розрізняти два види програм посередників:

- екрануючі агенти, орієнтовані на аналіз потоку повідомлень для певних видів сервісу, наприклад FTP, HTTP, Telnet;
- універсальні екрануючі агенти, оброблювальні увесь потік повідомлень, наприклад агенти, орієнтовані на пошук і знешкодження комп'ютерних вірусів, або прозоре шифрування даних.

Програмний посередник аналізує пакети даних, що поступають до нього, і, якщо будь-якої об'єкт не відповідає заданим критеріям, то або блокує його подальше просування, або виконує відповідні перетворення, наприклад

знешкоджує виявлені комп'ютерні віруси. При аналізі вмісту пакетів важливо, щоб екрануючий агент міг автоматично розпаковувати файлові архіви.

МЕ з посередниками дозволяють також організовувати захищені віртуальні мережі VPN (Virtual Private Network), наприклад безпечно об'єднувати декілька локальних мереж, підключених до Internet, в одну віртуальну мережу.

9.1.3. Додаткові можливості МЕ

Окрім виконання фільтрації трафіку і функцій посередництва деякі МЕ дозволяють реалізовувати інші, не менш важливі функції, без яких забезпечення захисту периметра внутрішньої мережі було б неповним .

Ідентифікація і аутентифікація користувачів. Окрім дозволу або заборони допуску різних застосувань в мережу, МЕ можуть також виконувати аналогічні дії і для користувачів, які бажають отримати доступ до зовнішніх або внутрішніх ресурсів, МЕ, що розділяється.

Перш ніж користувачеві буде надано право використання будь-якого сервісу, необхідно переконатися, що він дійсно той, за кого себе видає. Ідентифікація і аутентифікація користувачів є важливими компонентами концепції МЕ. Авторизація користувача зазвичай розглядається в контексті аутентифікації — як тільки користувач аутентифікований, для нього визначаються дозволені йому сервіси.

Ідентифікація і аутентифікація користувача іноді здійснюються при пред'явленні звичайного ідентифікатора (імені) і пароля. Проте ця схема уразлива з точки зору безпеки — пароль може бути перехоплений і використаний іншою особою. Багато інцидентів в мережі Internet сталися частково через уразливості традиційних багаторазових паролів. Зловмисники можуть спостерігати за каналами в мережі Internet і перехоплювати ті, що передаються в них відкритим текстом паролі, тому така схема аутентифікації вважається неефективною. Пароль слід передавати через загальнодоступні комунікації в зашифрованому виді (Рис. 9.3). Це дозволяє запобігти діставанню несанкціонованого доступу шляхом перехоплення мережевих пакетів.

Надійнішим методом аутентифікації є використання одноразових паролів. Широке поширення отримала технологія аутентифікації на основі одноразових паролів SecurID (див. л. 7 і 13).

Зручно і надійно також застосування цифрових сертифікатів, що видаються довіреними органами, наприклад центром розподілу ключів. Більшість програм посередників розробляються так, щоб користувач аутентифікувався тільки на початку сеансу роботи з МЕ. Після цього від нього не потрібно додаткової аутентифікації впродовж часу, визначуваного адміністратором.

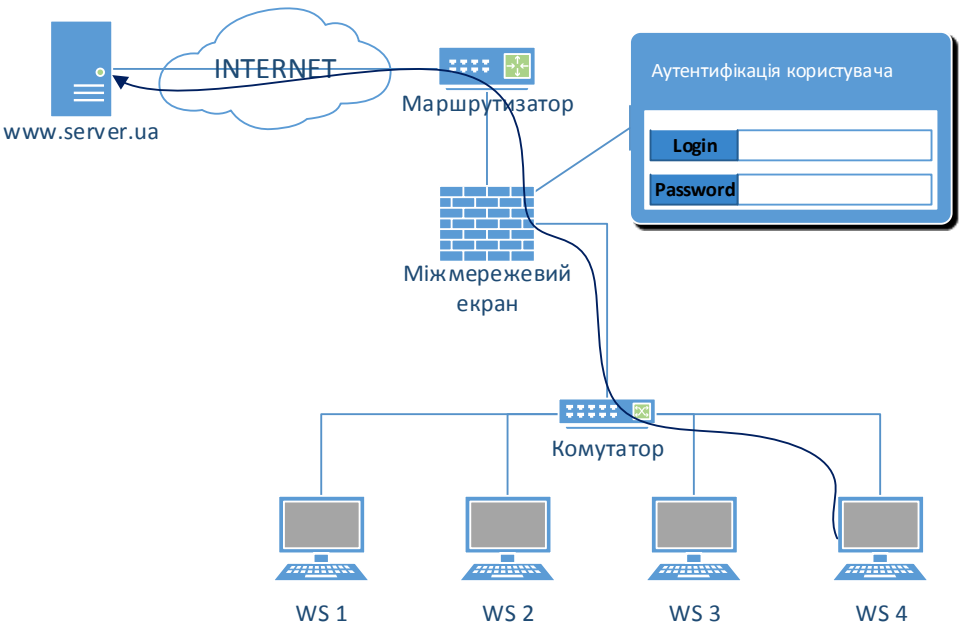

Рис. 9.3. Схема аутентифікації користувача по паролю

Оскільки МЕ можуть централізувати управління доступом в мережі, вони є відповідним місцем для установки програм або облаштувань посиленої аутентифікації. Хоча засоби посиленої аутентифікації можуть використовуватися на кожному хості, більше практичне їх розміщення на МЕ. За відсутності МЕ, що використовує заходи посиленої аутентифікації, неаутентифікований трафік таких застосувань, як Telnet або FTP, може безпосередньо проходити до внутрішніх систем в мережі.

Ряд МЕ підтримують Kerberos — один з поширених методів аутентифікації. Як правило, більшість комерційних МЕ підтримують декілька різних схем аутентифікації, дозволяючи адміністраторові мережевої безпеки зробити вибір найбільш прийнятної схеми для своїх умов.

Трансляція мережевих адрес. Для реалізації багатьох атак зловмисникові необхідно знати адресу своєї жертви. Щоб приховати ці адреси, а також топологію усієї мережі, МЕ виконують дуже важливу функцію — трансляцію внутрішніх мережевих адрес (Рис. 9.4).

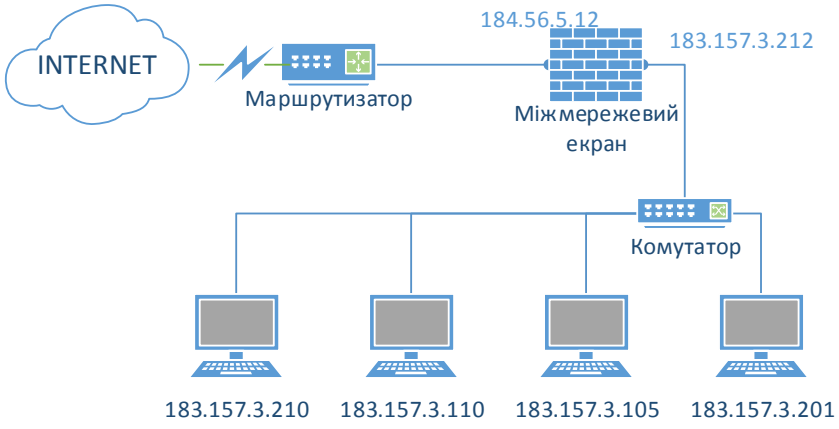

Рис. 9.4. Трансляція мережевих адрес

Ця функція реалізується по відношенню до усіх пакетів, що виходять з внутрішньої мережі в зовнішню. Для цих пакетів виконується автоматичне перетворення IP-адрес комп'ютерів відправників в один «надійний» IP-адрес.

Трансляція внутрішніх мережевих адрес може здійснюватися двома способами — динамічно і статично. У першому випадку адреса виділяється вузлу у момент звернення до МЕ. Після завершення з'єднання адреса звільняється і може бути використаний будь-яким іншим вузлом корпоративної мережі. У другому випадку адреса вузла завжди прив'язується до однієї адреси МЕ, з якої передаються усі вихідні пакети. IPадрес МЕ стає єдиним активним IP-адресом, який потрапляє в зовнішню мережу. В результаті усі пакети, що виходять з внутрішньої мережі, виявляються відправленими МЕ, що виключає прямий контакт між авторизованою внутрішньою мережею і що є потенційно небезпечною зовнішньою мережею.

При такому підході топологія внутрішньої мережі прихована від зовнішніх користувачів, що ускладнює завдання несанкціонованого доступу. Окрім підвищення безпеки трансляція адрес дозволяє мати усередині мережі власну систему адресації, не погоджену з адресацією в зовнішній мережі, наприклад в мережі Internet. Це ефективно вирішує проблему розширення адресного простору внутрішньої мережі і дефіциту адрес зовнішньої мережі.

Адміністрування, реєстрація подій і генерація звітів.

Простота і зручність адміністрування є одним з ключових аспектів в створенні ефективної і надійної системи захисту. Помилки при визначенні правил доступу можуть утворити діру, через яку можливий злом системи. Тому у більшості МЕ реалізовані сервісні утиліти, що полегшують введення, видалення, перегляд набору правил. Наявність цих утиліт дозволяє також робити перевірки на синтаксичні або логічні помилки при введенні або редагування правил. Як правило, утиліти дозволяють переглядати інформацію, згруповану за будь-яким критеріями, наприклад все, що відноситься до конкретного користувача або сервісу.

Важливими функціями МЕ є реєстрація подій, реагування на події, що задаються, а також аналіз зареєстрованої інформації і складання звітів. МЕ, будучи критичним елементом системи захисту корпоративної мережі, має можливість реєстрації усіх дій, їм що фіксуються. До таких дій відносяться не лише пропуск або блокування мережевих пакетів, але і зміна правил розмежування доступу адміністратором безпеки і інші дії. Така реєстрація дозволяє звертатися до створюваних журналів в міру необхідності (у разі виникнення інциденту безпеки або збору доказів для надання їх в судові інстанції або для внутрішнього розслідування).

При правильно налагодженій системі фіксації сигналів про підозрілі події (alarm) МЕ може дати детальну інформацію про те, чи були МЕ або мережа атаковані або зондовані. Збирати статистику використання мережі і доказу її зондування важливо з кількох причин. Передусім треба знати напевно, що МЕ стійкий до зондування і атак, і визначити, чи адекватні заходи захисту МЕ. Крім того, статистика використання мережі важлива в якості початкових даних при проведенні досліджень і аналізі ризику для формулювання вимог до мережевого устаткування і програм.

Багато МЕ містять потужну систему реєстрації, збору і аналізу статистики. Облік може вестися по адресах клієнта і сервера, ідентифікаторах користувачів, часу сеансів, часу з'єднань, кількості переданих/прийнятих даних, діях

адміністратора і користувачів. Системи обліку позволяют зробити аналіз статистики і надають адміністраторам детальні звіти. За рахунок використання спеціальних протоколів МЕ можуть виконати видалене сповіщення про певні події в режимі реального часу.

В якості обов'язкової реакції на виявлення спроб виконання несанкціонованих дій має бути визначене повідомлення адміністратора, т. е. видача попереджувальних сигналів. Будь-який МЕ, який не здатний посилати попереджувальні сигнали при виявленні нападу, не можна вважати ефективним засобом міжмережевого захисту.

9.2. Особливості функціонування МЕ на різних рівнях моделі OSI

МЕ підтримують безпеку міжмережевої взаємодії на різних рівнях моделі OSI. При цьому функції захисту, що виконуються на різних рівнях еталонної моделі, істотно відрізняються один від одного. Тому комплексний МЕ зручно представити у вигляді сукупності неділимих екранів, кожен з яких орієнтований на окремий рівень моделі OSI.

Найчастіше комплексний екран функціонує на мережевому, сеансовому і прикладному рівнях еталонної моделі. Відповідно розрізняють такі неділимі МЕ (Рис. 9.5), як:

- екрануючий маршрутизатор;
- шлюз сеансового рівня (екрануючий транспорт);
- шлюз прикладного рівня (екрануючий шлюз) [9, 32].

Використовувані в мережах протоколи (TCP/IP, SPX/IPX) не повністю відповідають еталонній моделі OSI, тому екрани перерахованих типів при виконанні своїх функцій можуть охоплювати і сусідні рівні еталонної моделі. Наприклад, прикладний екран може здійснювати автоматичне зашифровування повідомлень при їх передачі в зовнішню мережу, а також автоматичну розшифровку криптографічний закритих даних, що приймаються. В цьому випадку такий екран функціонує не лише на прикладному рівні моделі OSI, але і на рівні представлення.

Шлюз сеансового рівня при своєму функціонуванні охоплює транспортний і мережевий рівні моделі OS1. Екрануючий маршрутизатор при аналізі пакетів повідомлень перевіряє їх заголовки не лише мережевого, але і транспортного рівня.

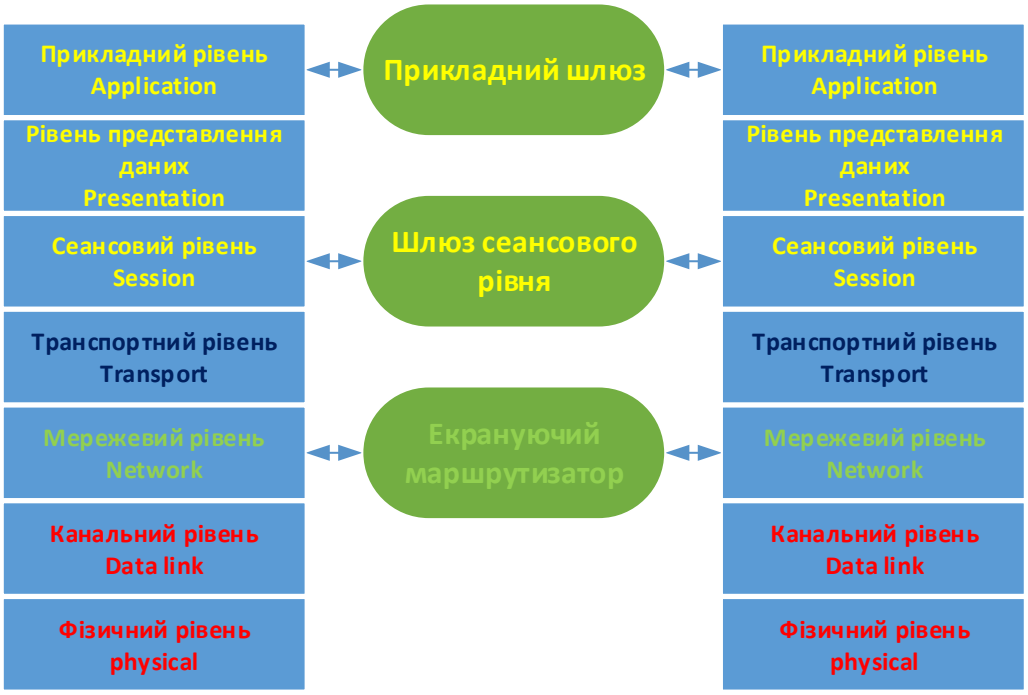

Рис. 9.5. Типи міжмережевих екранів, що функціонують на окремих рівнях моделі OSI

МЕ вказаних типів мають свої Переваги і недоліки. Багато хто з використовуваних МЕ є або прикладними шлюзами, або екрануючими маршрутизаторами, не забезпечуючи повну безпеку міжмережевої взаємодії. Надійний захист забезпечують тільки комплексні міжмережеві екрани, кожен з яких об'єднує екрануючий маршрутизатор, шлюз сеансового рівня, а також прикладний шлюз.

Розглянемо функціонування прикладного шлюзу.

9.2.1. Прикладний шлюз

Прикладний шлюз, що називається також екрануючим шлюзом, функціонує на прикладному рівні моделі OSI, охоплюючи також рівень представлення, і забезпечує найбільш надійний захист міжмережевих взаємодій [9, 32]. Захисні функції прикладного шлюзу, як і шлюзу сеансового рівня, відносяться до функцій посередництва. Проте прикладний шлюз, на відміну від шлюзу сеансового рівня, може виконувати істотно більшу кількість функцій захисту, до яких відносяться наступні:

- ідентифікація і аутентифікація користувачів при спробі встановлення з'єднань через МЕ;
- перевірка достовірності інформації, що передається через шлюз;
- розмежування доступу до ресурсів внутрішньої і зовнішньої мереж;
- фільтрація і перетворення потоку повідомлень, наприклад динамічний пошук вірусів і прозоре шифрування інформації;
- реєстрація подій, реагування на події, що задаються, а також аналіз зареєстрованої інформації і генерація звітів;
- кешування даних, що просяться із зовнішньої мережі.

Оскільки функції прикладного шлюзу відносяться до функцій посередництва, цей шлюз є універсальним комп'ютером, на якому функціонують

програмні посередники (екрануючі агенти), — по одному для кожного обслуговуваного прикладного протоколу (HTTP, FTP, SMTP, NNTP та ін.). Програмний посередник (application proxy) кожної служби TCP/IP орієнтований на обробку повідомлень і виконання функцій захисту, що відносяться саме до цієї служби.

Прикладний шлюз перехоплює за допомогою відповідних екрануючих агентів пакети, що входять та виходять, копіює і перенаправляє інформацію, т. е. функціонує в якості сервера посередника, виключаючи прямі з'єднання між внутрішньою і зовнішньою мережею (Рис. 9.6).

Посередники, використовувані прикладним шлюзом, мають важливі відмінності від канальних посередників шлюзів сеансового рівня

Рис. 9.6. Схема функціонування прикладного шлюзу

Поперше, посередники прикладного шлюзу пов'язані з конкретними застосуваннями (програмними серверами), подруге, вони можуть фільтрувати потік повідомлень на прикладному рівні моделі OSI.

Прикладні шлюзи використовують як посередників спеціально розроблені для цієї мети програмні сервери конкретних служб TCP/IP — сервери HTTP, FTP, SMTP, NNTP та ін. Ці програмні сервери функціонують на МЕ в резидентному режимі і реалізують функції захисту, що відносяться до відповідних служб TCP/IP.

Шлюз прикладного рівня має наступні переваги:

- забезпечує високий рівень захисту локальної мережі завдяки можливості виконання більшості функцій посередництва;
- захист на рівні додатків дозволяє здійснювати велике число додаткових перевірок, зменшуючи тим самим вірогідність проведення успішних атак, можливих через недоліки програмного забезпечення;
- при порушенні його працездатності блокується наскрізне проходження пакетів між мережами, що розділяються, внаслідок чого безпека мережі, що захищається, не знижується через виникнення відмов.

До недоліків прикладного шлюзу відносяться:

- високі вимоги до продуктивності і ресурсоємності комп'ютерної платформи;
- відсутність «прозорості» для користувачів і зниження пропускної спроможності при реалізації міжмережевих взаємодій.

9.2.2. Варіанти виконання МЕ

Існує два основні варіанти виконання МЕ — програмний і програмно апаратний. У свою чергу програмно апаратний варіант має два різновиди — у вигляді спеціалізованого пристрою і у вигляді модуля в маршрутизаторі або комутаторі.

Нині частіше використовується програмне рішення, яке на перший погляд виглядає привабливішим. Це пов'язано з тим, що для його застосування досить, тільки придбати програмне забезпечення (ПЗ) МЕ і встановити на будь-який комп'ютер, наявний в організації. Проте на практиці далеко не завжди в організації знаходиться вільний комп'ютер, що задовольняє досить високим вимогам по системних ресурсах. Тому одночасно з придбанням ПЗ отримується і комп'ютер для його установки. Потім слідує процес установки на комп'ютер операційної системи (ОС) і її налаштування, що також вимагає часу і оплати роботи установників. І тільки після цього встановлюється і настроюється ПЗ системи виявлення атак. Неважко помітити, що використання звичайного персонального комп'ютера далеке не так просто, як здається на перший погляд.

Тому останніми роками значно зріс інтерес до програмно апаратним рішень [9, 32], які поступово витісняють «чисто» програмні системи. Широкого поширення стали набувати спеціалізовані програмно апаратні рішення, що називаються security appliance. Програмно апаратний комплекс міжмережевого екранування зазвичай складається з комп'ютера, а також ОС, що функціонують на нім, і спеціального ПЗ. Слід зазначити, що це спеціальне ПЗ часто називають firewall. Використовуваний комп'ютер має бути досить потужним і фізично захищеним, наприклад знаходитися в спеціально відведеному приміщенні, що охороняється. Крім того, він повинен мати засоби захисту від завантаження ОС з несанкціонованого носія. Програмноапаратні комплекси використовують спеціалізовані або звичайні ПЗ (як правило, на базі FreeBSD, Linux або Microsoft Windows, «урізані» для виконання заданих функцій і задовольняючі ряду вимог:

- мати засоби розмежування доступу до ресурсів системи;
- блокувати доступ до комп'ютерних ресурсів в обхід програмного інтерфейсу, що надається;
- забороняти привілейований доступ до своїх ресурсів з локальної мережі;
- містити засоби моніторингу/аудиту будь-яких адміністративних дій.

Переваги спеціалізованих програмно-апаратних рішень:

- простота впровадження в технологію обробки інформації. Такі засоби поставляються із заздалегідь встановленою і налагодженою ОС і захисними механізмами, тому необхідно тільки підключити їх до мережі, що виконується впродовж декількох хвилин;
- простота управління. Ці засоби можуть управлятися з будь-якої робочої станції Windows 9x, NT, 2000 або Unix. Взаємодія консолі управління з пристроєм здійснюється або по стандартних протоколах, наприклад Telnet або SNMP, або за допомогою спеціалізованих або захищених протоколів, наприклад SSH або SSL;
- відмовостійкість і висока доступність. Виконання МЕ у вигляді спеціалізованого програмноапаратного комплексу дозволяє реалізувати механізми

забезпечення не лише програмної, але і апаратної відмовостійкості і високої доступності;

- висока продуктивність і надійність. За рахунок виключення з ОС усіх «непотрібних» сервісів і підсистем, програмноапаратний комплекс працює ефективніше з точки зору продуктивності і надійності;
- спеціалізація на захисті. Рішення тільки завдань забезпечення мережевої безпеки не призводить до витрат ресурсів на виконання інших функцій, наприклад маршрутизації і т. п.

9.3. Схеми мережевого захисту на базі МЕ

При підключенні корпоративної або локальної мережі до глобальних мереж потрібні:

- захист корпоративної або локальної мережі від віддаленого НСД з боку глобальної мережі;
- приховання інформації про структуру мережі і її компонентів від користувачів глобальної мережі;
- розмежування доступу в мережу, що захищається, з глобальної мережі і з мережі, що захищається, в глобальну мережу.

Для ефективного захисту міжмережевої взаємодії система МЕ має бути правильно встановлена і конфігурована. Цей процес полягає:

- з формування політики міжмережевої взаємодії;
- вибору схеми підключення і налаштування параметрів функціонування МЕ.

9.3.1. Формування політики міжмережевої взаємодії

Політика міжмережевої взаємодії є складовою частиною загальної політики безпеки в організації. Вона визначає вимоги до безпеки інформаційного обміну організації із зовнішнім світом і повинна відбивати два аспекти [9, 32]:

- політику доступу до мережевих сервісів;
- політикові роботи МЕ.

Політика доступу до мережевих сервісів визначає правила надання і використання усіх можливих сервісів комп'ютерної мережі, що захищається. У рамках цієї політики мають бути задані усі сервіси, що надаються через МЕ, і допустимі адреси клієнтів для кожного сервісу. Крім того, для користувачів мають бути вказані правила, що описують, коли, хто, яким сервісом і на якому комп'ютері може скористатися. Задаються також обмеження на методи доступу, наприклад на використання протоколів SLIP (Serial Line Internet Protocol) і PPP (PointtoPoint Protocol). Обмеження методів доступу потрібне для того, щоб користувачі не могли звертатися до «заборонених» сервісів Internet обхідними шляхами. Правила аутентифікації користувачів і комп'ютерів, а також умови роботи користувачів поза локальною мережею організації мають бути визначені окремо.

Для того, щоб МЕ успішно захищав ресурси організації, політика доступу користувачів до мережевих сервісів має бути реалістичною. Реалістичною вважається така політика, при якій знайдений баланс між захистом мережі організації від відомих ризиків і необхідним доступом користувачів до мережевих сервісів.

Політика роботи МЕ задає базовий принцип управління міжмережевою взаємодією, покладений в основу функціонування МЕ. Може бути вибраний один з двох принципів:

1) заборонено все, що явно не дозволене;
2) дозволено все, що явно не заборонене.

Фактично вибір принципу встановлює, наскільки «підозрілою» або «довірчою» має бути система захисту. Залежно від вибору, рішення може бути прийняте як на користь безпеки і на шкоду зручності використання мережевих сервісів, так і навпаки.

При виборі принципу 1 МЕ настроюється так, щоб блокувати будь-які явно не дозволені міжмережеві взаємодії. Цей принцип відповідає класичній моделі доступу, використовуваної в усіх областях інформаційної безпеки. Такий підхід дозволяє адекватно реалізувати принцип мінімізації привілеїв, тому з точки зору безпеки він є кращим. Адміністратор безпеки повинен на кожен тип дозволеної взаємодії задавати правила доступу (одне і більше). Адміністратор не зможе по забудькуватості залишити дозволеними будьякі повноваження, оскільки за умовчанням вони будуть заборонені. Доступні зайві сервіси можуть бути використані на шкоду безпеці, що особливо характерно для закритого і складного ПЗ, в якому можуть бути різні помилки і некоректності. Принцип 1, по суті, є визнанням факту, що незнання може завдати шкоди. Слід зазначити, що правила доступу, сформульовані відповідно до цього принципу, можуть доставляти користувачам певні незручності.

При виборі принципу 2 МЕ настроюється так, щоб блокувати тільки явно заборонені міжмережеві взаємодії. В цьому випадку підвищується зручність використання мережевих сервісів з боку користувачів, але знижується безпека міжмережевої взаємодії. Користувачі мають більше можливостей обійти МЕ, наприклад, можуть отримати доступ до нових сервісів, що не забороняються політикою (або навіть не вказаним в політиці), або запустити заборонені сервіси на нестандартних портах TCP/UDP, які не заборонені політикою. Адміністратор може врахувати не усі дії, які заборонені користувачам. Йому доводиться працювати в режимі реагування, передбачаючи і забороняючи ті міжмережеві взаємодії, які негативно впливають на безпеку мережі. При реалізації принципу 2 внутрішня мережа виявляється менш захищеною від нападів хакерів, тому виробники МЕ зазвичай відмовляються від його використання.

МЕ є симетричним. Для нього окремо задаються правила, що обмежують доступ з внутрішньої мережі в зовнішню мережу, і навпаки. У загальному випадку його робота заснована на динамічному виконанні двох функцій:

- фільтрації інформаційних потоків, що проходять через нього;
- посередництва при реалізації міжмережевих взаємодій.

Залежно від типу екрану ці функції можуть виконуватися з різною повнотою. Прості МЕ орієнтовані на виконання тільки одній з них. Комплексні МЕ забезпечують спільне виконання вказаних функцій захисту. Власна захищеність МЕ досягається за допомогою тих же засобів, що і захищеність універсальних систем [9].

Щоб ефективно забезпечувати безпеку мережі, комплексний МЕ зобов'язаний управляти усім потоком, що проходить через нього, і відстежувати свій стан. Для ухвалення рішень, що управляють, по використовуваних сервісах

МЕ повинен отримувати, запам'ятовувати, вибирати і обробляти інформацію, отриману від усіх комунікаційних рівнів і від інших застосувань.

Недостатньо просто перевіряти пакети окремо. Інформація про стан з'єднання, отримана з інспекції з'єднань у минулому і інших застосувань — головний чинник в ухваленні рішення, що управляє, при встановленні нового з'єднання. При ухваленні рішення враховуються як стан з'єднання (отримане з минулого потоку даних), так і стан додатка (отримане з інших застосувань). Повнота і правильність управління вимагають, щоб комплексний МЕ мав можливість аналізу і використання наступних елементів:

- інформації про з'єднання — інформацію від усіх семи рівнів в пакеті;
- історії з'єднань — інформація, отримана від попередніх з'єднань;
- стану рівня додатка — інформація про стан, отриманого з інших застосувань. Наприклад, аутентифікованому користувачеві можна надати доступ через МЕ тільки для авторизованих видів сервісу;
- агрегуючих елементів — обчислення різноманітних виразів, заснованих на усіх вищеперелічених чинниках.

9.3.2. Основні схеми підключення МЕ

При підключенні корпоративної мережі до глобальних мереж необхідно розмежувати доступ в мережу, що захищається, з глобальної мережі і з мережі, що захищається, в глобальну мережу, а також забезпечить захист мережі, що підключається, від видаленого НСД з боку глобальної мережі. При цьому організація зацікавлена в прихованні інформації про структуру своєї мережі і її компонентів від користувачів глобальної мережі. Робота з видаленими користувачами вимагає встановлення жорстких обмежень доступу до інформаційних ресурсів мережі, що захищається.

Часто виникає потреба мати у складі корпоративної мережі декілька сегментів з різними рівнями захищеності:

- вільно доступні сегменти (наприклад, рекламний WWW сервер);
- сегмент з обмеженим доступом (наприклад, для доступу співробітникам організації з видалених вузлів);
- закриті сегменти (наприклад, фінансова локальна підмережа організації).

Для підключення МЕ можуть використовуватися різні схеми, які залежать від умов функціонування мережі, що захищається, а також від кількості мережевих інтерфейсів і інших характеристик, використовуваних МЕ. Широке поширення отримали схеми:

- захисту мережі з використанням екрануючого маршрутизатора;
- єдиного захисту локальної мережі;
- із закритою, що захищається, і відкритою, що не захищається, підмережами;
- з роздільним захистом закритої і відкритої підмереж [9, 32].

Розглянемо детальніше схему із закритою, що захищається, і не

відкритою, що захищається, підмережами. Якщо у складі локальної мережі є загальнодоступні відкриті сервери, то їх доцільно винести як відкриту підмережу

до МЕ (Рис. 9.7). Цей спосіб має високу захищеність закритої частини локальної мережі, але забезпечує знижену безпеку відкритих серверів, розташованих до МЕ.

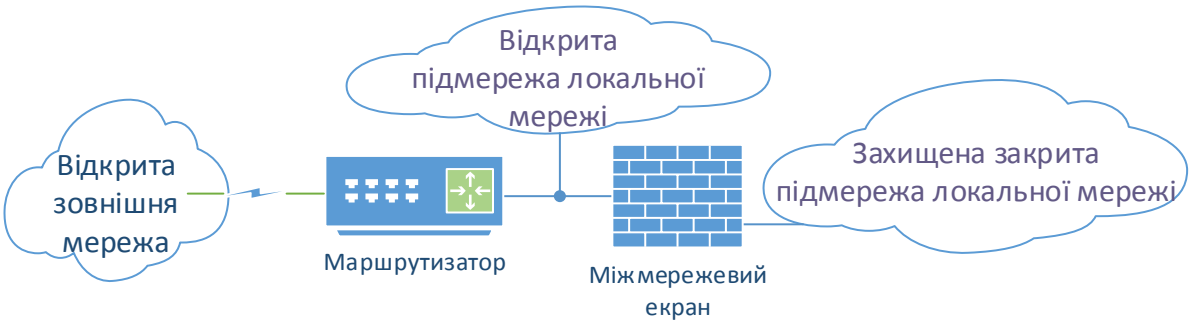

Рис. 9.7. Схема із закритою, що захищається, і відкритою, що не захищається, під мережами

Деякі МЕ дозволяють розмістити ці сервери на собі. Проте таке рішення не є кращим з точки зору безпеки самого МЕ і завантаження комп'ютера. Схему підключення МЕ із закритою підмережею, що захищається, і відкритою підмережею, що не захищається, доцільно використати лише при невисоких вимогах по безпеці до відкритої підмережі.

Якщо ж до безпеки відкритих серверів пред'являються підвищені вимоги, тоді необхідно використати схему з роздільною зашитою закритою і відкритою підмереж.

9.3.3. Персональні і розподілені мережеві екрани

За останні декілька років в структурі корпоративних мереж сталися певні зміни. Якщо раніше межі таких мереж можна було чітко обкреслити, то зараз це практично неможливо. Ще нещодавно така межа проходила через усі маршрутизатори або інші пристрої (наприклад, модеми), через які здійснювався вихід в зовнішні мережі. У видалених офісах організації ситуація була схожа. Проте зараз повноправним користувачем МЕ мережі, що захищається, є співробітник, що знаходиться за межами периметра, що захищається. До таких співробітників відносяться користувачі, працюючі вдома або що знаходяться у відрядженні. Поза сумнівом їм також потрібно захист. Але все традиційні МЕ побудовані так, що користувачі, що захищаються, і ресурси повинні знаходитися під їх зашитою з внутрішньої сторони корпоративної або локальної мережі, що є неможливим для мобільних користувачів.

Для вирішення цієї проблеми були запропоновані наступні підходи:

- застосування розподілених МЕ (distributed firewall);
- використання можливостей віртуальних приватних мереж VPN (л. 10).

Розподілений міжмережевий екран (distributed firewall) — централізована керована сукупність мережевих мініекранів, що захищають окремі комп'ютери мережі.

Для індивідуальних користувачів представляє інтерес технологія персонального мережевого екранування. В цьому випадку мережевий екран встановлюється на персональний комп'ютер, що захищається. Такий екран, що

називається персональним екраном комп'ютера (personal firewall) або системою мережевого екранування, контролює увесь вихідний трафік, що входить, незалежно від усіх інших системних захисних засобів. При екрануванні окремого комп'ютера підтримується доступність мережевих сервісів, але зменшується навантаження, що створюється зовнішньою активністю. В результаті знижується уразливість внутрішніх сервісів комп'ютера, що захищається таким чином, оскільки спочатку сторонній зловмисник повинен здолати екран, де захисні засоби конфігуровані особливо ретельно і жорстко.

Ці засоби не лише захищають від зовнішніх атак комп'ютери, на яких вони встановлені, але і забезпечують захист трафіку, що передається за межі цього вузла (т. е. організовують захищені канали VPN). Саме таке рішення дозволило забезпечити захист мереж з нечітко обкресленими межами.

Наявність функції централізованого управління у розподіленого МЕ — його головна відмінність від персонального екрану. Якщо персональні мережеві екрани управляються тільки з комп'ютера, на якому вони встановлені, і ідеально підходять для домашнього застосування, то розподілені МЕ можуть управлятися централізований, з єдиної консолі управління, встановленої в головному офісі організації. Це дозволило деяким виробникам випускати МЕ в двох версіях:

- персональною (для індивідуальних користувачів);
- розподіленою (для корпоративних користувачів).

У сучасних умовах більше 50 % різних атак і спроб доступу до інформації здійснюється зсередини локальних мереж, тому класичний «периметровий» підхід до створення системи захисту корпоративної мережі стає недостатньо ефективним. Корпоративну мережу можна вважати дійсно захищеною від НСД тільки за наявності в ній засобів захисту точок входу з боку Internet і рішень, що забезпечують безпеку окремих комп'ютерів, корпоративних серверів і фрагментів локальної мережі підприємства. Рішення на основі розподілених або персональних МЕ най

кращим чином забезпечують безпеку окремих комп'ютерів, корпоративних серверів і фрагментів локальної мережі підприємства [64].

9.3.4. Проблеми безпеки МЕ

МЕ не вирішує усі проблеми безпеки корпоративної мережі. Окрім описаних вище достоїнств МЕ, існують обмеження в їх використанні і загрози безпеки, від яких МЕ не можуть захистити. Відмітимо найбільш суттєві з цих обмежень [9, 43]:

- можливе обмеження пропускної спроможності. Традиційні МЕ є потенційно вузьким місцем мережі, оскільки усі з'єднання повинні проходити через МЕ і в деяких випадках вивчатися МЕ;
- відсутність вбудованих механізмів захисту від вірусів. Традиційні МЕ не можуть захистити від користувачів, що завантажують заражені вірусами програми для ПЕВМ з інтернетівських архівів або при передачі таких програм в якості додатків до листа, оскільки ці програми можуть бути зашифровані або стислі великим числом способів;
- відсутність ефективного захисту від отримуваного з Internet небезпечного вмісту (аплети Java, елементи ActiveX, що управляють, сценарії

JavaScript і т. д.). Специфіка мобільного коду така, що він може бути використаний як засіб для проведення атак. Мобільний код може бути реалізований у виді:

— вірусу, який вторгається в ІС і знищує дані на локальних дисках, постійно модифікуючи свій код і утрудняючи тим самим своє виявлення і видалення;

— агента, що перехоплює паролі, номери кредитних карт і т. д.;

— програми, що копіює конфіденційні файли, що містять ділову і фінансову інформацію і ін.;

• МЕ не може захистити від помилок і некомпетентності адміністраторів і користувачів;

• традиційні МЕ є по суті засобами, тільки блокуючими атаки. У більшості випадків вони захищають від атак, які вже знаходяться в процесі створення. Ефективнішим було б не лише блокування, але і попередження атак, т. е. усунення передумов реалізації вторгнень. Для організації попередження атак необхідно використати засоби виявлення атак і пошуку вразливості, які своєчасно виявлятимуть і рекомендуватимуть заходи по усуненню «слабких місць» в системі захисту. Технології виявлення атак і аналізу захищеності мереж розглядаються в л. 14.

Для захисту інформаційних ресурсів розподілених корпоративних систем потрібне застосування комплексної системи інформаційної безпеки, яка дозволить ефективно використати Переваги МЕ і компенсувати їх недоліки за допомогою інших засобів безпеки.

Лекція 10 ОСНОВИ ТЕХНОЛОГІЇ ВІРТУАЛЬНИХ ЗАХИЩЕНИХ МЕРЕЖ VPN

Завдання створення комп'ютерної мережі підприємства в межах однієї будівлі може бути вирішене відносно легко. Проте сучасна інфраструктура корпорацій включає географічно розподілені підрозділи самої корпорації, її партнерів, клієнтів і постачальників. Тому створення корпоративної мережі стало істотно складнішим завданням.

З бурхливим розвитком Internet і мереж колективного доступу стався якісний стрибок в поширенні і доступності інформації. Користувачі отримали дешеві і доступні канали Internet. Підприємства прагнуть використати такі канали для передачі критичної комерційної і управлінської інформації.

Для ефективної протидії мережевим атакам і забезпечення можливості активного і безпечного використання у бізнесі відкритих мереж на початку 1990х рр. народилася і активно розвивається концепція побудови віртуальних приватних мереж — VPN (Virtual Private Network).

10.1. Концепція побудови віртуальних захищених мереж VPN

У основі концепції побудови віртуальних мереж VPN лежить досить проста ідея: якщо в глобальній мережі є два вузли, якими треба обмінятися інформацією, то між цими двома вузлами необхідно побудувати віртуальний захищений тунель для забезпечення конфіденційності і цілісності інформації, що передається через відкриті мережі; доступ до цього віртуального тунелю має бути надзвичайно ускладнений усім можливим активним і пасивним зовнішнім спостерігачам.

Переваги, що отримуються компанією від створення таких віртуальних тунелів, полягають передусім в значній економії фінансових коштів, оскільки в цьому випадку компанія може відмовитися від побудови або оренди дорогих виділених каналів зв'язку для створення власних intranet/extranet мереж і використати для цього дешеві Інтернет канали, надійність і швидкість передачі яких у більшості своєму вже не поступається виділеним лініям. Очевидна економічна ефективність від впровадження VPN технологій стимулює підприємства до активного їх впровадження.

10.1.1. Основні поняття і функції мережі VPN

При підключенні корпоративної локальної мережі до відкритої мережі виникають загрози безпеки двох основних типів:

- НСД до внутрішніх ресурсів корпоративної локальної мережі, отримуваний зловмисником в результаті несанкціонованого входу в цю мережу;
- НСД до корпоративних даних в процесі їх передачі по відкритій мережі.

Забезпечення безпеки інформаційної взаємодії локальних мереж і окремих комп'ютерів через відкриті мережі, зокрема через мережу Інтернет, можливо шляхом ефективного рішення наступних завдань:

- захист підключених до відкритих каналів зв'язку локальних мереж і окремих комп'ютерів від несанкціонованих дій з боку зовнішнього середовища;

- захист інформації в процесі її передачі по відкритих каналах зв'язку.

Як вже відзначалося вище, для захисту локальних мереж і окремих комп'ютерів від несанкціонованих дій з боку зовнішнього середовища зазвичай використовують МЕ, що підтримують безпеку інформаційної взаємодії шляхом фільтрації двостороннього потоку повідомлень, а також виконання функцій посередництва при обміні інформацією. МЕ розташовують на стику між локальною і відкритою мережею. Для захисту окремого віддаленого комп'ютера, підключеного до відкритої мережі, на цьому комп'ютері встановлюють ПЗ мережевого екрану, і такий мережевий екран називається персональним.

Захист інформації в процесі її передачі по відкритих каналах заснований на використанні віртуальних захищених мереж VPN. Віртуальною захищеною мережею VPN (Virtual Private Network) називають об'єднання локальних мереж і окремих комп'ютерів через відкрите зовнішнє середовище передачі інформації в єдину віртуальну корпоративну мережу, що забезпечує безпеку циркулюючих даних. Віртуальна захищена мережа VPN формується шляхом побудови віртуальних захищених каналів зв'язку, що створюються на базі відкритих каналів зв'язку загальнодоступної мережі. Ці віртуальні захищені канали зв'язку називаються тунелями VPN. Мережа VPN дозволяє за допомогою тунелів VPN з'єднати центральний офіс, офіси філій, офіси бізнес партнерів і видалених користувачів і безпечно передавати інформацію через Інтернет (Рис. 10.1).

Тунель VPN є з'єднанням, проведеним через відкриту мережу, по якому передаються криптографічно захищені пакети даних віртуальної мережі. Захист інформації в процесі її передачі по тунелю VPN заснований:

- на аутентифікації взаємодіючих сторін;
- криптографічному закритті (шифруванні) передаваних даних;
- перевірці достовірності і цілісності інформації, що доставляється.

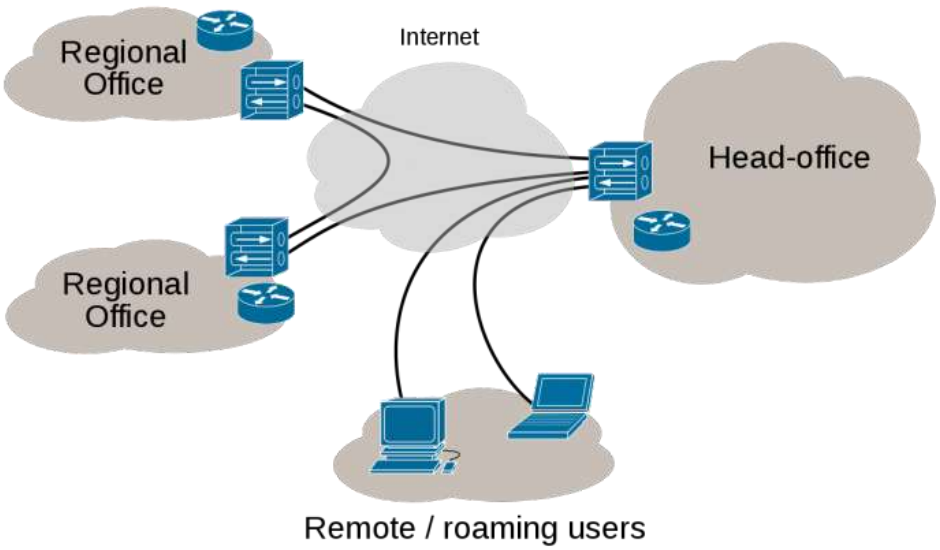

Рис. 10.1. Віртуальна захищена мережа VPN

Для цих функцій характерний взаємозв'язок сторін. При їх реалізації використовуються криптографічні методи захисту інформації. Ефективність такого захисту забезпечується за рахунок спільного використання симетричних і

асиметричних криптографічних систем. Тунель VPN, що формується облаштуваннями VPN, має властивості захищеної виділеної лінії, яка розгортається у рамках загальнодоступної мережі, наприклад Інтернету. Пристрої VPN можуть грати у віртуальних приватних мережах роль VPN клієнта, VPN сервера або шлюзу безпеки VPN.

VPN клієнт є програмним або програмно-апаратним комплексом, що виконується зазвичай на базі персонального комп'ютера. Його мережеве ПЗ модифікується для виконання шифрування і аутентифікації трафіку, яким цей пристрій обмінюється з іншими VPN клієнтами, VPN серверами або шлюзами безпеки VPN. Зазвичай реалізація VPN клієнта є програмним рішенням, що доповнює стандартну ОС, — Windows 2000/XP/7 або Unix.

VPN сервер є програмним або програмно-апаратним комплексом, що встановлюється на комп'ютері, що виконує функції сервера. VPN сервер забезпечує захист серверів від НСД із зовнішніх мереж, а також організацію захищених з'єднань (асоціацій) з окремими комп'ютерами і з комп'ютерами з сегментів локальних мереж, захищених відповідними VPN продуктами. VPN сервер є функціональним аналогом продукту VPN клієнт для серверних платформ. Він відрізняється передусім розширеними ресурсами для підтримки множинних з'єднань з VPN клієнтами. VPN сервер може підтримувати захищені з'єднання з мобільними користувачами.

Шлюз безпеки VPN (security gateway) — цей мережевий пристрій, що підключається до двох мереж і виконує функції шифрування і аутентифікації для численних хостів, розташованих за ним. Розміщений шлюз безпеки VPN так, щоб через нього проходив увесь трафік, призначений для внутрішньої корпоративної мережі. Мережеве з'єднання шлюзу VPN прозоро для користувачів позаду шлюзу, представляється ним виділеною лінією, хоча насправді прокладається через відкриту мережу з комутацією пакетів. Адреса шлюзу безпеки VPN вказується як зовнішню адресу тунелює пакет, що входить, а внутрішня адреса пакету є адресою конкретного хоста позаду шлюзу. Шлюз безпеки VPN може бути реалізований у вигляді окремого програмного рішення, окремого апаратного пристрою, а також у вигляді маршрутизатора або МЕ, доповнених функціями VPN.

Відкрите зовнішнє середовище передачі інформації включає як канали швидкісної передачі даних, як яка використовується мережа Інтернет, так і повільніші загальнодоступні канали зв'язки, в якості яких зазвичай застосовуються канали телефонної мережі. Ефективність віртуальної приватної мережі VPN визначається мірою захищеності інформації, циркулюючої по відкритих каналах зв'язку. Для безпечної передачі даних через відкриті мережі широко використовують інкапсуляцію і тунелювання. За допомогою методики тунелювання пакети даних передаються через загальнодоступну мережу, як по звичайному двоточковому з'єднанню. Між кожною парою «посилач — одержувач даних» встановлюється своєрідний тунель — логічне з'єднання, що дозволяє інкапсулювати дані одного протоколу в пакети іншого.

Суть тунелювання полягає в тому, щоб інкапсулювати, «упакувати», передавану порцію даних, разом із службовими полями, в новий «конверт». При цьому пакет протоколу нижчого рівня поміщається в поле даних пакету протоколу більш високого або такого ж рівня. Слід зазначити, що тунелювання саме по собі не захищає дані від НСД або спотворення, але завдяки тунелюванню з'являється

можливість повного криптографічного захисту початкових пакетів, що інкапсулюються. Щоб забезпечити конфіденційність передаваних даних, посилач шифрує початкові пакети, упаковує їх в зовнішній пакет з новим IP заголовком і відправляє по транзитній мережі (Рис. 10.2).

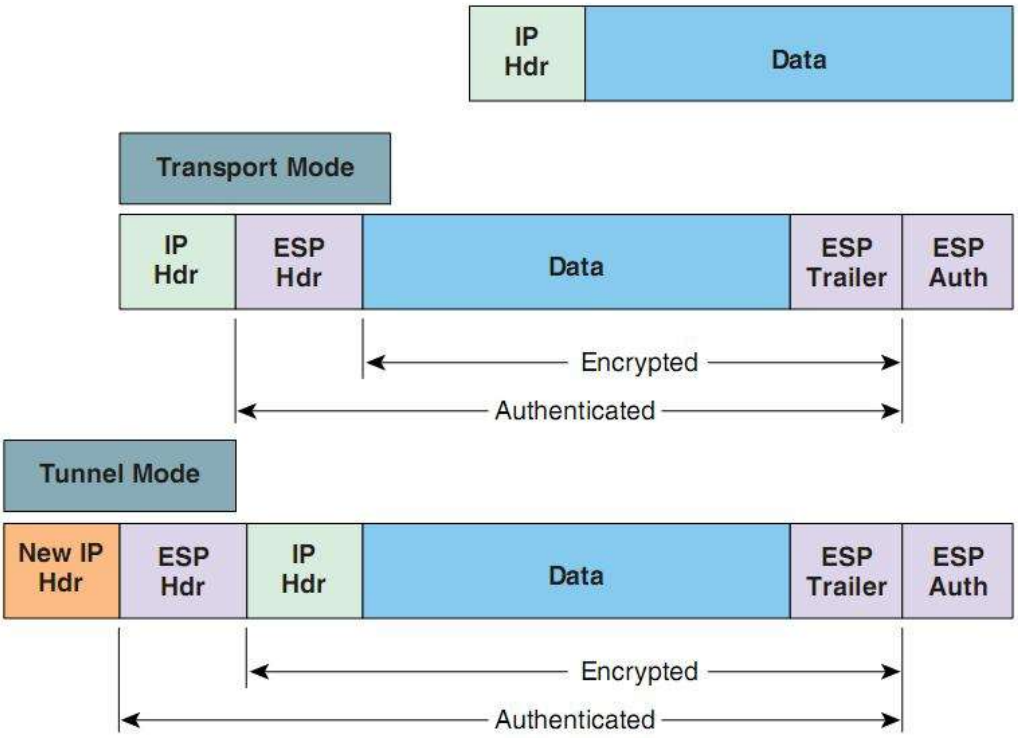

Рис. 10.2. Приклад пакету, підготовленого для тунелювання

Особливість технології тунелювання в тому, що вона дозволяє зашифровувати початковий пакет цілком, разом із заголовком, а не тільки його поле даних. Це важливо, оскільки деякі поля заголовка містять інформацію, яка може бути використана зловмисником. Зокрема, із заголовка початкового пакету можна витягнути відомості про внутрішню структуру мережі — дані про кількість підмереж і вузлів і їх IP адресах. Зловмисник може використати таку інформацію при організації атак на корпоративну мережу. Початковий пакет із зашифрованим заголовком не може бути використаний для організації транспортування по мережі. Тому для захисту початкового пакету застосовують його інкапсуляцію і тунелювання. Початковий пакет зашифровують повністю, разом із заголовком, і потім цей зашифрований пакет поміщають в інший зовнішній пакет з відкритим заголовком. Для транспортування даних по відкритій мережі використовуються відкриті поля заголовка зовнішнього пакету.

Після прибуття в кінцеву точку захищеного каналу із зовнішнього пакету витягають внутрішній початковий пакет, розшифровують його і використовують його відновлений заголовок для подальшої передачі по внутрішній мережі (Рис. 10.3).

Тунелювання може бути використане для захисту не лише конфіденційності вмісту пакету, але і його цілісності і автентичності, при цьому електронний цифровий підпис можна розповсюдити на усі поля пакету.

На додаток до приховання мережевої структури між двома точками, тунелювання може також запобігти можливий конфлікт адрес між двома

локальними мережами. При створенні локальної мережі, не пов'язаної з Internet, компанія може використати будь-які IP адреси для своїх мережевих пристроїв і комп'ютерів. При об'єднанні раніше ізольованих мереж ці адреси можуть почати конфліктувати один з одним і з адресами, які вже використовуються в Internet. Інкапсуляція пакетів вирішує цю проблему, оскільки дозволяє приховати первинні адреси і додати нові, унікальні в просторі IP адресів Internet, які потім використовуються для пересилки даних по мережах, що розділяються. Сюди ж входить завдання налаштування IP адреса і інших параметрів для мобільних користувачів, що підключаються до локальної мережі.

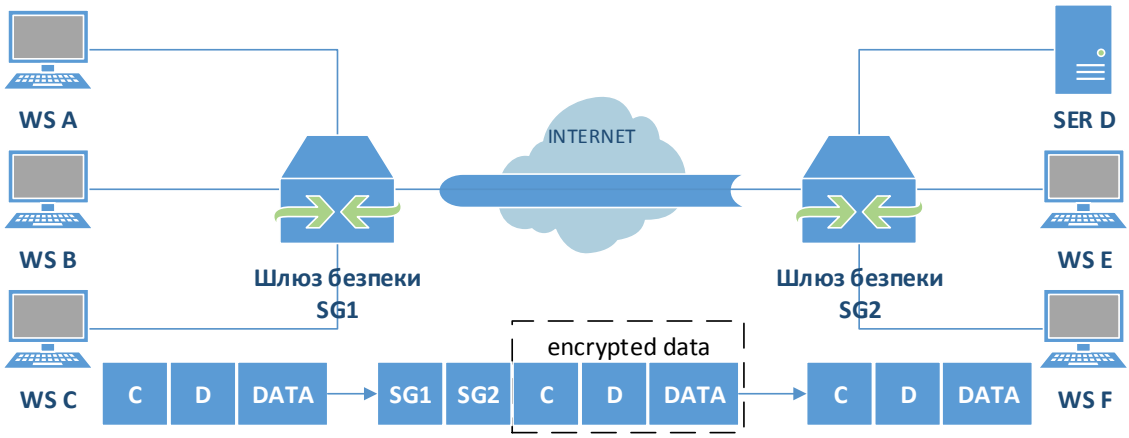

Рис. 10.3. Схема віртуального захищеного тунеля

Механізм тунелювання широко застосовується в різних протоколах формування захищеного каналу. Зазвичай тунель створюється тільки на ділянці відкритої мережі, де існує загроза порушення конфіденційності і цілісності даних, наприклад між точкою входу у відкритий Інтернет і точкою входу в корпоративну мережу. При цьому для зовнішніх пакетів використовуються адреси пограничних маршрутизаторів, встановлених в цих двох точках, а внутрішні адреси кінцевих вузлів містяться у внутрішніх початкових пакетах в захищеному виді. Слід зазначити, що сам механізм тунелювання не залежить від того, з якою метою застосовується тунелювання. Тунелювання може застосовуватися не лише для забезпечення конфіденційності і цілісності усієї передаваної порції даних, але і для організації переходу між мережами з різними протоколами (наприклад, IPv4 і IPv6). Тунелювання дозволяє організувати передачу пакетів одного протоколу в логічному середовищі, що використовує інший протокол. В результаті з'являється можливість вирішити проблеми взаємодії декількох різнотипних мереж, починаючи з необхідності забезпечення цілісності і конфіденційності передаваних даних і закінчуючи подоланням невідповідностей зовнішніх протоколів або схем адресації.

Реалізацію механізму тунелювання можна представити як результат роботи протоколів трьох типів: протоколу «пасажира», протоколу, що несе, і протоколу тунелювання. Наприклад, в якості протоколу «пасажира» може бути використаний транспортний протокол IPX, що переносить дані в локальних мережах філій одного підприємства. Найбільш поширеним варіантом протоколу, що несе, є протокол IP мережі Інтернет. В якості протоколів тунелювання можуть бути використані протоколи канального рівня PPTP і L2TP, а також протокол мережевого рівня

IPSec. Завдяки тунелюванню стає можливим приховання інфраструктури Internet від VPN додатків.

Тунелі VPN можуть створюватися для різних типів кінцевих користувачів — або це локальна мережа LAN (local area network) з шлюзом безпеки, або окремі комп'ютери видалених і мобільних користувачів. Для створення віртуальної приватної мережі великого підприємства потрібні VPN шлюзи, VPN сервери і VPN клієнти. VPN шлюзи доцільно використати для захисту локальних мереж підприємства, VPN сервери і VPN клієнти використовують для організації захищених з'єднань видалених і мобільних користувачів з корпоративною мережею через Інтернет.

10.1.2. Варіанти побудови віртуальних захищених каналів

Безпеку інформаційного обміну необхідно забезпечувати як у разі об'єднання локальних мереж, так і у разі доступу до локальних мереж видалених або мобільних користувачів [62]. При проектуванні VPN зазвичай розглядаються дві основні схеми:

1) віртуальний захищений канал між локальними мережами (канал ЛВС-ЛВС);

2) віртуальний захищений канал між вузлом і локальною мережею (Рис. 10.4).

Схема 1 з'єднання дозволяє замінити дорогі виділені лінії між окремими офісами і створити постійно доступні захищені канали між ними. В цьому випадку шлюз безпеки служить інтерфейсом між тунелем і локальною мережею, при цьому користувачі локальних мереж використовують тунель для спілкування один з одним. Багато компаній використовують цей вид VPN як заміну або доповнення до наявних з'єднань глобальної мережі, таким як frame relay.

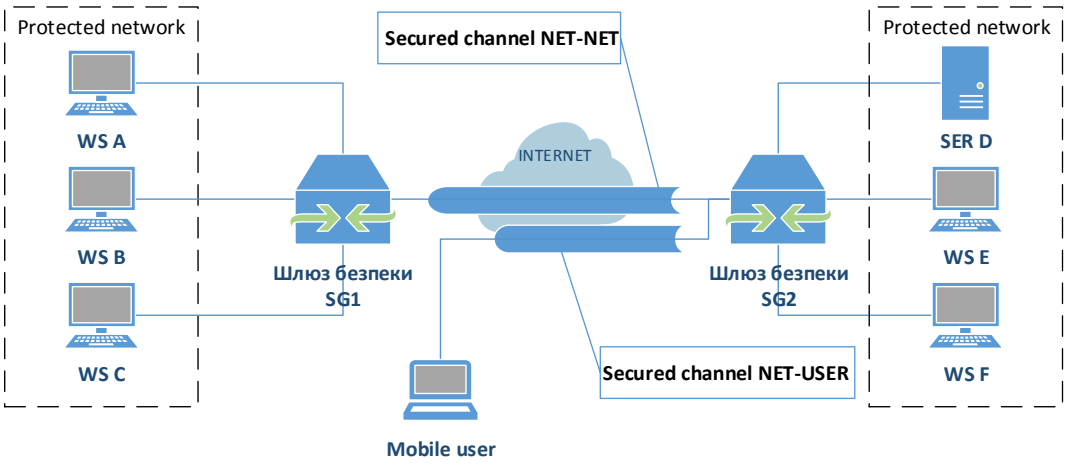

Рис. 10.4. Віртуальні захищені канали типу Мережа – Мережа, і Клієнт - Мережа

Схема 2 захищені канали VPN призначена для встановлення з'єднань з віддаленими або мобільними користувачами. Створення тунеля ініціює клієнт (видалений користувач). Для зв'язку з шлюзом, що захищає видалену мережу, він запускає на своєму комп'ютері спеціальне клієнтське ПЗ.

Цей вид VPN замінює собою комутовані з'єднання і може використовуватися разом з традиційними методами віддаленого доступу.

Існують варіанти схем віртуальних захищених каналів. В принципі будь-який з двох вузлів віртуальної корпоративної мережі, між якими формується віртуальний захищений канал, може належати кінцевій або проміжній точці потоку повідомлень, що захищається.

З точки зору забезпечення інформаційної безпеки кращим є варіант, при якому кінцеві точки захищеного тунеля співпадають з кінцевими точками потоку повідомлень, що захищається. В цьому випадку забезпечується захищеність каналу уздовж усього шляху дотримання пакетів повідомлень. Проте такий варіант веде до децентралізації управління і надмірності ресурсних витрат. В цьому випадку потрібна установка засобів створення VPN на кожному клієнтському комп'ютері локальної мережі. Це ускладнює централізоване управління доступом до комп'ютерних ресурсів і не завжди виправдано економічно. Окреме адміністрування кожного клієнтського комп'ютера з метою конфігурації в нім засобів захисту є досить трудомісткою процедурою у великій мережі.

Якщо усередині локальної мережі, що входить у віртуальну мережу, не потрібно захист трафіку, тоді в якості кінцевої точки захищеного тунеля можна вибрати МЕ або пограничний маршрутизатор цієї локальної мережі. Якщо ж потік повідомлень усередині локальної мережі має бути захищений, тоді в якості кінцевої точки тунеля в цій мережі повинен виступати комп'ютер, який бере участь в захищеній взаємодії. При доступі до локальної мережі віддаленого користувача комп'ютер цього користувача має бути кінцевою точкою віртуального захищеного каналу.

Досить поширеним є варіант, коли захищений тунель прокладається тільки усередині відкритої мережі з комутацією пакетів, наприклад усередині Інтернету. Цей варіант відрізняється зручністю застосування, але має порівняно низьку безпеку. Кінцевими точками такого тунеля зазвичай виступають провайдери Інтернету або пограничні маршрутизатори (міжмережеві екрани) локальної мережі.

При об'єднанні локальних мереж тунель формується тільки між пограничними провайдерами Інтернету, або маршрутизаторами (міжмережевими екранами) локальної мережі. При віддаленому доступі до локальної мережі тунель створюється між сервером віддаленого доступу провайдера Інтернету, а також пограничним провайдером Інтернету або маршрутизатором (міжмережевим екраном) локальної мережі. Побудовані по цьому варіанту віртуальні корпоративні мережі мають хорошу масштабованість і керованість. Сформовані захищені тунелі повністю прозорі для клієнтських комп'ютерів і серверів локальної мережі, що входить в таку віртуальну мережу. ПЗ цих вузлів залишається без змін. Проте цей варіант характеризується порівняно низькою безпекою інформаційної взаємодії, оскільки частково трафік проходить по відкритих каналах зв'язку в незахищеному виді. Якщо створення і експлуатацію такої VPN бере на себе провайдер ISP, тоді уся віртуальна приватна мережа може бути побудована на його шлюзах прозоро для локальних мереж і видалених користувачів підприємства. Але в цьому випадку виникають проблеми довіри до провайдера і постійної оплати його послуг.

Захищений тунель створюється компонентами віртуальної мережі, що функціонують на вузлах, між якими формується тунель. Ці компоненти прийнято називати **ініціатором тунеля** і **термінатором тунеля.**

Ініціатор тунеля інкапсулює початковий пакет в новий пакет, що містить новий заголовок з інформацією про відправники і одержувачі. Пакети, що

інкапсулюються, можуть належати до протоколу будь-якого типу, включаючи пакети протоколів, що не маршрутизуються, наприклад NetBEUI. Усі передавані по тунелю пакети є пакетами IP. Маршрут між ініціатором і термінатором тунеля визначає звичайна мережа IP, що маршрутизується, яка може бути мережею, відмінною від Інтернету.

Ініціювати і розривати тунель можуть різні мережеві пристрої і ПЗ. Наприклад, тунель може бути ініційований ноутбуком мобільного користувача, обладнаним модемом і відповідним ПЗ для встановлення з'єднань віддаленого доступу. В якості ініціатора може виступити також маршрутизатор локальної мережі, наділений відповідними функціональними можливостями. Тунель зазвичай завершується комутатором мережі або шлюзом провайдера послуг.

Термінатор тунеля виконує процес, зворотний інкапсуляції. Термінатор видаляє нові заголовки і направляє кожен початковий пакет адресатові в локальній мережі.

Конфіденційність пакетів, що інкапсулюються, забезпечується шляхом їх шифрування, а цілісність і достовірність — шляхом формування електронного цифрового підпису. Існує безліч методів і алгоритмів криптографічного захисту даних, тому необхідно, щоб ініціатор і термінатор тунеля своєчасно погоджували один з одним і використали одні і ті ж методи і алгоритми захисту. Для забезпечення можливості розшифровки даних і перевірки цифрового підпису при прийомі ініціатор і термінатор тунеля повинні також підтримувати функції безпечного обміну ключами. Крім того, кінцеві сторони інформаційної взаємодії повинні пройти аутентифікацію, щоб гарантувати створення тунелів VPN тільки між уповноваженими користувачами.

Існуюча мережева інфраструктура корпорації може бути підготовлена до використання VPN як за допомогою програмного, так і за допомогою апаратного забезпечення.

10.1.3. Засоби забезпечення безпеки VPN

При побудові захищеної віртуальної мережі VPN первинне значення має завдання забезпечення інформаційної безпеки. Згідно із загальноприйнятим визначенням, під безпекою даних розуміють їх конфіденційність, цілісність і доступність. Стосовно завдань VPN критерії безпеки даних можуть бути визначені таким чином:

- конфіденційність — гарантія того, що в процесі передачі даних по захищених каналах VPN ці дані можуть бути відомі тільки легальному відправнику і одержувачеві;
- цілісність — гарантія збереження передаваних даних під час проходження по захищеному каналу VPN. Будь-які спроби зміни, модифицикації, руйнування або створення нових даних будуть виявлені і стануть відомі легальним користувачам;
- доступність — гарантія того, що засоби, що виконують функції VPN, постійно доступні легальним користувачам. Доступність засобів VPN є комплексним показником, який залежить від надійності реалізації, якості обслуговування і міри захищеності самого засобу від зовнішніх атак.

Конфіденційність забезпечується за допомогою різних методів і алгоритмів симетричного і асиметричного шифрування. Цілісність передаваних даних зазвичай досягається за допомогою різних варіантів технології електронного підпису, заснованих на асиметричних методах шифрування і односторонніх функціях.

Аутентифікація здійснюється на основі багаторазових і одноразових паролів, цифрових сертифікатів, смарткарт, протоколів строгої аутентифікації, забезпечує встановлення VPN з'єднань тільки між легальними користувачами і запобігає доступу до засобів VPN небажаних осіб.

Авторизація має на увазі надання абонентам, що довели свою легальність (автентичність), різних видів обслуговування, зокрема різних способів шифрування їх трафіку. Авторизація і управління доступом часто реалізуються одними і тими ж засобами.

Для забезпечення безпеки передаваних даних у віртуальних захищених мережах мають бути вирішені наступні основні завдання мережевої безпеки:

- взаємна аутентифікація абонентів при встановленні з'єднання;
- забезпечення конфіденційності, цілісності і автентичності передаваної інформації;
- авторизація і управління доступом;
- безпека периметра мережі і виявлення вторгнень;
- управління безпекою мережі.

Аутентифікація абонентів. Процедура аутентифікації (встановлення достовірності) дозволяє вхід для легальних користувачів і запобігає доступу до мережі небажаних осіб.

Методи, алгоритми і ряд протоколів аутентифікації детально розглянуті в л. 7; протоколи і системи аутентифікації видалених користувачів приведені в л. 13.

Забезпечення конфіденційності, цілісності і автентичності інформації. Завдання забезпечення конфіденційності інформації полягає в захисті передаваних даних від несанкціонованого читання і копіювання. Основним засобом забезпечення конфіденційності інформації є шифрування.

Алгоритми шифрування і електронного цифрового підпису розглянуті в л. 6.

Авторизація і управління доступом. Ключовим компонентом безпеки VPN є гарантія того, що доступ до комп'ютерних ресурсів дістають авторизовані користувачі, тоді як для неавторизованих користувачів мережа повністю закрита.

При побудові програмних засобів авторизації застосовуються:

- централізована схема авторизації;
- децентралізована схема авторизації.

Основне призначення централізованої системи авторизації — реалізувати принцип єдиного входу. Управління процесом надання ресурсів користувачеві здійснюється сервером. Централізований підхід до процесу авторизації реалізований в системах Kerberos, RADIUS і TACACS.

Останнім часом активно розвивається так зване ролеве управління доступом. Воно вирішує не стільки проблеми безпеки, скільки покращує керованість систем. Суть ролевого управління доступом полягає в тому, що між користувачами і їх привілеями поміщають проміжні сутності - ролі. Для кожного користувача одночасно можуть бути активними декілька ролей, кожна з яких надає йому цілком певні права.

Оскільки ролей багато менше, ніж користувачів і привілеїв, використання ролей сприяє пониженню складності і, отже, поліпшенню керованості системи. Крім того, на підставі ролевої моделі управління доступом можна реалізувати такий важливий принцип, як розділення обов'язків (наприклад, неможливість самостійно скомпрометувати критично важливий процес).

Управління доступом і організація захищеного віддаленого доступу розглядаються в л. 13.

Безпека периметра мережі і виявлення вторгнень. Суворий контроль доступу до додатків, сервісів і ресурсів мережі, що захищається, є важливою функцією правильно побудованої мережі. Використання таких засобів безпеки, як МЕ, системи виявлення вторгнень, системи аудиту безпеки, антивірусні комплекси забезпечує системний захист переміщуваних по мережі даних.

Важливою частиною загального рішення безпеки мережі є МЕ, які контролюють трафік, що перетинає периметр мережі, що захищається, і накладають обмеження на пропуск трафіку відповідно до політики безпеки організації (див. л. 3).

Додатковим елементом гарантії безпеки периметра мережі є система виявлення вторгнень IDS (Intrusion Detection System), працююча в реальному часі і призначена для виявлення, фіксації і припинення неавторизованої мережевої активності як від зовнішніх, так і від внутрішніх джерел.

Системи аналізу захищеності сканують корпоративну мережу з метою виявлення потенційних уразливостей безпеці, даючи можливість адміністраторам мережі краще захистити мережу від атак.

Системи антивірусного захисту описані в л. 14, системи виявлення вторгнень і системи аналізу захищеності розглядаються в л. 15.

Управління безпекою мережі. Мережі VPN інтегрують як самі мережеві пристрої, так і численні сервіси управління безпекою і пропускною спроможністю. Компаніям потрібне цілісне управління цими пристроями і сервісами через інфраструктуру VPN, включаючи користувачів віддаленого доступу і засобів extranet. У зв'язку з цим управління засобами VPN стає одному з найважливіших завдань забезпечення ефективного функціонування VPN. Система управління корпоративною мережею повинна включати необхідний набір засобів для управління політиками безпеки, пристроями і сервісами VPN будь-якого масштабу.

Система управління безпекою мережі є наріжним каменем сімейства продуктів, що забезпечують наскрізну безпеку VPN. Для забезпечення високого рівня безпеки і керованості VPN, і зокрема системи розподілу криптографічних ключів і сертифікатів, необхідно забезпечити централізоване скоординоване управління безпекою усієї корпоративної мережі, що захищається.

Методи і засоби управління мережевою безпекою розглядаються в л. 16.

10.2. VPN рішення для побудови захищених мереж

Сьогодні технології побудови віртуальних захищених приватних мереж (VPN) привертають все більше уваги з боку великих компаній (банків, відомств, великих державних структур і т. д.). Причина такого інтересу полягає в тому, що VPN технології дійсно дають можливість не лише істотно скоротити витрати на

утримування виділених каналів зв'язку з віддаленими підрозділами (філіями), але і підвищити конфіденційність обміну інформацією.

VPN технології дозволяють організовувати захищені тунелі як між офісами компанії, так і до окремих робітників станціям і серверам. Потенційним клієнтам пропонується широкий спектр устаткування і ПЗ для створення віртуальних захищених мереж — від інтегрованих багатофункціональних і спеціалізованих пристроїв до чисто програмних продуктів.

10.2.1. Класифікація мереж VPN

Завдяки технології VPN багато компаній починають будувати свою стратегію з урахуванням використання Інтернету як головного засобу передачі інформації, причому навіть тій, яка є уразливою або життєво важливою.

Існують різні ознаки класифікації VPN. Найчастіше використовуються:

- «робочий« рівень моделі OSI;
- архітектура технічного рішення VPN;
- спосіб технічної реалізації VPN.

Класифікація VPN за «робочим» рівнем моделі OSI

Для технологій безпечної передачі даних по загальнодоступній (незахищеною) мережі застосовують узагальнену назву — захищений канал (secure channel). Термін «канал» підкреслює той факт, що захист даних забезпечується між двома вузлами мережі (хостами або шлюзами) уздовж деякого віртуального шляху, прокладеного в мережі з комутацією пакетів.

Захищений канал можна побудувати за допомогою системних засобів, реалізованих на різних рівнях моделі взаємодії відкритих систем OSI (Рис. 10.5).

<table>
<tr><td rowspan="7">Протоколи захищеного доступу</td><td>прикладний</td><td rowspan="3">Впливають на додатки</td></tr>
<tr><td>представлення</td></tr>
<tr><td>сеансовий</td></tr>
<tr><td>транспортний</td><td></td></tr>
<tr><td>мережевий</td><td rowspan="3">Не впливають на додатки</td></tr>
<tr><td>канальний</td></tr>
<tr><td>фізичний</td></tr>
</table>

Рис. 10.5. Рівні протоколів захищеного каналу

Класифікація VPN по «робочому» рівню моделі OSI представляє значний інтерес, оскільки від вибраного рівня OSI багато в чому залежить функціональність VPN, що реалізовується, і її сумісність з додатками, а також з іншими засобами захисту.

За ознакою «робочого» рівня моделі OSI розрізняють наступні групи VPN:

- VPN канального рівня;
- VPN мережевого рівня;
- VPN сеансового рівня.

VPN канального рівня. Засоби VPN, використовувані на канальному рівні моделі OSI, дозволяють забезпечити інкапсуляцію різних видів трафіку третього рівня (і вище) і побудову віртуальних тунелів типу «точка-точка» (від

маршрутизатора до маршрутизатора або від персонального комп'ютера до шлюзу ЛВС). До цієї групи відносяться VPN продукти, які використовують протоколи L2F (Layer 2 Forwarding) і PPTP (PointtoPoint Tunneling Protocol), а також стандарт L2TP (Layer 2 Tunneling Protocol), розроблений спільно фірмами Cisco Systems і Microsoft.

VPN мережевого рівня. VPN продукти мережевого рівня виконують інкапсуляцію IP в IP. Одним з широко відомих протоколів на цьому рівні є протокол IPSec (IP Security), призначеним для аутентифікації, тунелювання і шифрування IP пакетів. Стандартизованний консорціумом Internet Engineering Task Force (IETF) протокол IPSec увібрав в себе усі кращі рішення по шифруванню пакетів і повинен увійти в якості обов'язкового компонента в протокол IPv6.

З протоколом IPSec пов'язаний протокол IKE (Internet Key Exchange), вирішальний завдання безпечного управління і обміну криптографічними ключами між віддаленими пристроями. Протокол IKE автоматизує обмін ключами і встановлює захищене з'єднання, тоді як IPSec кодує і «підписує» пакети. Крім того, IKE дозволяє змінювати ключ для вже встановленого з'єднання, що підвищує конфіденційність передаваної інформації.

VPN сеансового рівня. Деякі VPN використовують інший підхід під назвою «посередники каналів» (circuit proxy). Цей метод функціонує над транспортним рівнем і ретранслює трафік із захищеної мережі в загальнодоступну мережу Internet для кожного сокета окремо. (Сокет IP ідентифікується комбінацією TCP з’єднання і конкретного порту або заданим портом UDP. Стек TCP/IP не має п'ятого — сеансового — рівня, проте орієнтовані на сокети операції часто називають операціями сеансового рівня.)

Шифрування інформації, що передається між ініціатором і термінатором тунеля, часто здійснюється за допомогою захисту транспортного рівня TLS (Transport Layer Security). Для стандартизації аутентифікованного проходу через МЕ консорціум IETF визначив протокол під назвою SOCKS, і в теперішній час протокол SOCKS v.5 застосовується для стандартизованої реалізації посередників каналів.

Протоколи захисту на канальному, транспортному і сеансовому рівнях детально розглядаються в л. 11. Особливості захисту на мережевому рівні за допомогою протоколів IPSec і IKE розбираються в л. 12.

Класифікація VPN за архітектурою технічного рішення

По архітектурі технічного рішення прийнято виділяти три основні види віртуальних приватних мереж:

- внутрішньокорпоративні VPN (Intranet VPN);
- VPN з віддаленим доступом (Remote Access VPN);
- міжкорпоративні VPN (Extranet VPN).

Внутрішньокорпоративні мережі VPN призначені для забезпечення захищеної взаємодії між підрозділами усередині підприємства або між групою підприємств, об'єднаних корпоративними мережами зв'язку, включаючи виділені лінії.

VPN з віддаленим доступом призначені для забезпечення захищеного віддаленого доступу до корпоративних інформаційних ресурсів мобільним і/або віддаленим (homeoffice) співробітникам компанії.

Міжкорпоративні мережі VPN призначені для забезпечення захищеного обміну інформацією із стратегічними партнерами по бізнесу, постачальниками, великими замовниками, користувачами, клієнтами і т. д. Extranet VPN забезпечує прямий доступ з мережі однієї компанії до мережі іншої компанії і тим самим сприяє підвищенню надійності зв'язку, підтримуваного в ході ділової співпраці.

Слід зазначити, що останнім часом спостерігається тенденція до конвергенції різних конфігурацій VPN.

Класифікація VPN за способом технічної реалізації

Конфігурація і характеристики віртуальної приватної мережі багато в чому визначаються типом вживаних VPNпристроїв.

За способом технічної реалізації розрізняють VPN на основі:

- маршрутизаторів;
- міжмережевих екранів;
- програмних рішень;
- спеціалізованих апаратних засобів зі вбудованими шифропроцесорами.

VPN на основі маршрутизаторів. Цей спосіб побудови VPN припускає застосування маршрутизаторів для створення захищених каналів. Оскільки уся інформація, що виходить з локальної мережі, проходить через маршрутизатор, то цілком природно покласти на нього і завдання шифрування. Приклад устаткування для VPN на маршрутизаторах — облаштування компанії Cisco Systems.

VPN на основі міжмережевих екранів. МЕ більшості виробників підтримують функції тунелювання і шифрування даних, наприклад продукт Fire Wall1 компанії Check Point Software Technologies. При використанні МЕ на базі ПК треба пам'ятати, що подібне рішення підходить тільки для невеликих мереж з невеликим об'ємом передаваної інформації. Недоліками цього методу є висока вартість рішення в перерахунку на одне робоче місце і залежність продуктивності від апаратного забезпечення, на якому працює МЕ.

VPN на основі програмного забезпечення. VPN продукти, реалізовані програмним способом, з точки зору продуктивності поступаються спеціалізованим пристроям, проте мають достатню потужність для реалізації VPN мереж. Слід зазначити, що у разі віддаленого доступу вимоги до необхідної смуги пропускання невеликі. Тому чисто програмні продукти легко забезпечують продуктивність, достатню для віддаленого доступу. Безперечною перевагою програмних продуктів є гнучкість і зручність в застосуванні, а також відносно невисока вартість.

VPN на основі спеціалізованих апаратних засобів. Головна перевага таких VPN — висока продуктивність, оскільки швидкодія обумовлена тим, що шифрування в них здійснюється спеціалізованими мікросхемами. Спеціалізовані VPN пристроїв забезпечують високий рівень безпеки, проте вони дорогі.

10.2.2. Основні варіанти архітектури VPN

Існує безліч різновидів віртуальних приватних мереж. Їх спектр варіює від провайдерських мереж, що дозволяють управляти обслуговуванням клієнтів безпосередньо на їх площах, до корпоративних мереж VPN, що розгортаються і керованих самими компаніями. Проте, прийнято виділяти три основні види віртуальних приватних мереж:

1. VPN з віддаленим доступом (Remote Access VPN),

2. внутрішньокорпоративні VPN (Intranet VPN) і
3. міжкорпоративні VPN (Extranet VPN) [9].

VPN з віддаленим доступом (Рис. 10.6) дозволяють значно скоротити щомісячні витрати на використання комутованих і виділених ліній. Принцип їх роботи простий: користувачі встановлюють з'єднання з місцевою точкою доступу до глобальної мережі, після чого їх виклики тунелюють через Інтернет, що позбавляє від плати за міжміський і міжнародний зв'язок або виставляння рахунків власникам безкоштовних міжміських номерів; потім усі виклики концентруються на відповідних вузлах і передаються в корпоративні мережі.

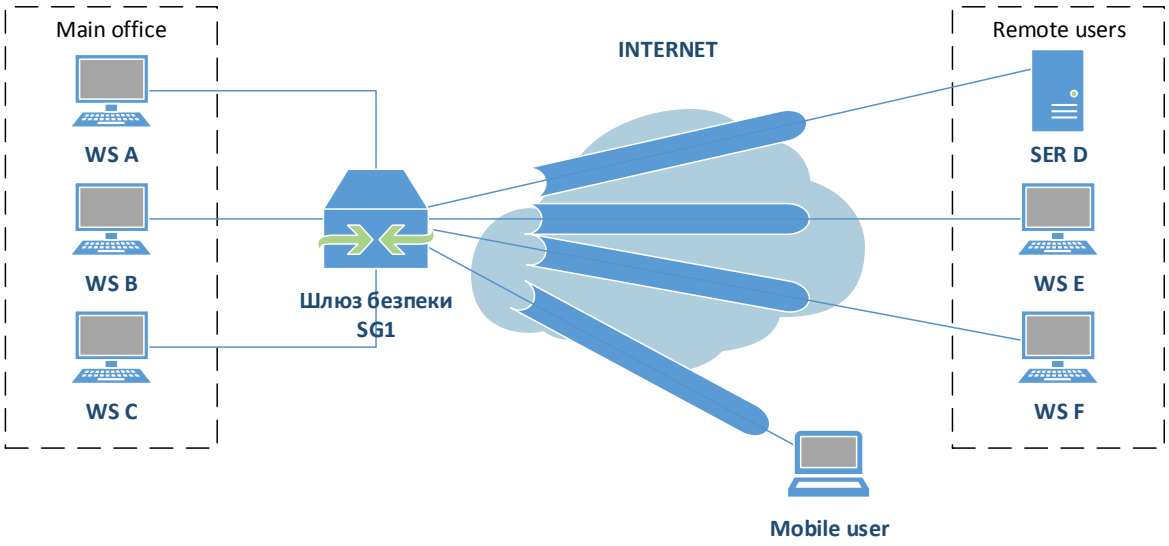

Рис. 10.6. Віртуальна приватна мережа з віддаленим доступом

Переваги переходу від приватно керованих dial networks до Remote Access VPN:

- можливість використання місцевих dialin numbers замість міжміських дозволяє значно понизити витрати на міжміські телекомунікації;
- ефективна система встановлення достовірності видалених і мобільних користувачів забезпечує надійне проведення процедури аутентифікації;
- висока масштабованість і простота розгортання для нових користувачів, що додаються до мережі;
- зосередження уваги компанії на основних корпоративних бизнесцілях замість відвернення на проблеми забезпечення роботи мережі.

Істотна економія при використанні Remote Access VPN є потужним стимулом, проте застосування відкритого Internet в якості об'єднуючої магістралі для транспорту чутливого корпоративного трафіку стає усе більш масштабним, що робить механізми захисту інформації життєво важливими елементами цієї технології.

Внутрішньокорпоративні мережі VPN (Рис. 10.7) будуються з використанням Internet або мережевих інфраструктур, що розділяються, сервіс провайдерами, що надаються. Компанії досить відмовитися від використання дорогих виділених ліній, замінивши їх дешевшим зв'язком через Internet. Це істотно скорочує витрати на використання смуги пропускання, оскільки в Internet відстань ніяк не впливає на вартість з'єднання.

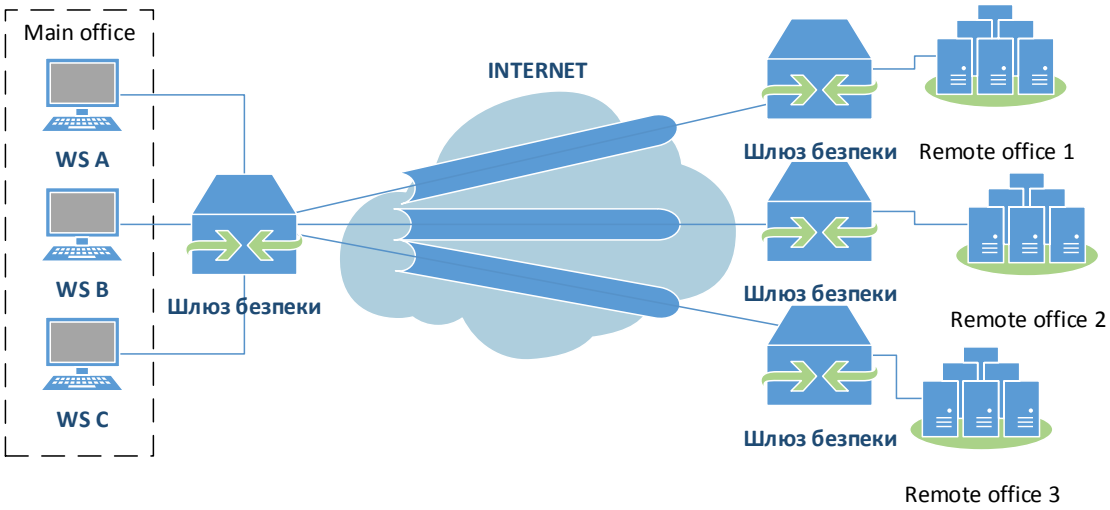

Рис. 10.7. З'єднання вузлів мережі за допомогою технології Intranet VPN

Переваги Intranet VPN:

- застосування потужних криптографічних протоколів шифрування даних для захисту конфіденційної інформації;
- надійність функціонування при виконанні таких критичних застосувань, як системи автоматизованого продажу і системи управління базами даних;
- гнучкість управління ефективним розміщенням швидко зростаючого числа нових користувачів, нових офісів і нових програмних застосувань.

Побудова Intranet VPN, використовуючи Internet, є найрентабельнішим способом реалізації VPNтехнології. Проте в Internet рівні сервісу взагалі не гарантуються. Компанії, яким потрібно гарантовані рівні сервісу, повинні розглянути можливість розгортання своїх VPN з використанням мережевих інфраструктур, що розділяються, сервіс провайдерами, що надаються.

Міжкорпоративна мережа VPN (Рис. 10.8) — це мережева технологія, яка забезпечує прямий доступ з мережі однієї компанії до мережі іншої компанії і, таким чином, сприяє підвищенню надійності зв'язку, підтримуваного в ході ділової співпраці.

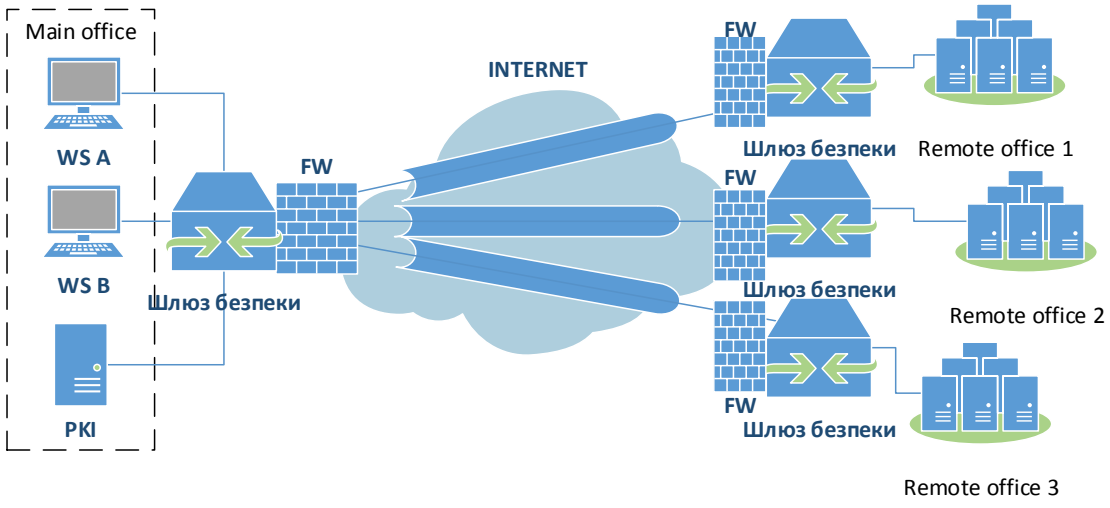

Рис. 10.8. Міжкорпоративна мережа Extranet VPN

Мережі Extranet VPN в цілому схожі на внутрішньокорпоративні віртуальні приватні мережі з тією лише різницею, що проблема захисту інформації є для них гострішою. Для Extranet VPN характерне використання стандартизованих VPN продуктів, що гарантують здатність до взаємодії з різними VPN рішеннями, які ділові партнери могли б застосовувати у своїх мережах.

Коли декілька компаній приймають рішення працювати разом і відкривають один для одного свої мережі, вони повинні потурбуватися про те, щоб їх нові партнери мали доступ тільки до певної інформації. При цьому конфіденційна інформація має бути надійно захищена від несанкціонованого використання. Саме тому в міжкорпоративних мережах велике значення надається контролю доступу з відкритої мережі за допомогою МЕ. Важлива і аутентифікація користувачів, покликана гарантувати, що доступ до інформації дістають тільки ті, кому він дійсно дозволений. В той же час, розгорнута система захисту від несанкціонованого доступу не повинна залучати до себе уваги.

З'єднання Extranet VPN розгортаються, використовуючи ті ж архітектуру і протоколи, які застосовуються при реалізації Intranet VPN і Remote Access VPN. Основна відмінність полягає в тому, що дозвіл доступу, який дається користувачам Extranet VPN, пов'язаний з мережею їх партнера.

Іноді в окрему групу виділяють локальний варіант мережі VPN (Localnet VPN). Локальна мережа Localnet VPN забезпечує захист інформаційних потоків, циркулюючих усередині локальних мереж компанії (як правило, Центрального офісу), від НСД з боку «надмірно цікавих» співробітників самої компанії. Нині спостерігається тенденція до конвергенції різних способів реалізацій VPN [9, 65].

10.3. Переваги застосування технологій VPN

Ефективне застосування ИТ у поєднанні з технологіями в області інформаційної безпеки є найважливішим стратегічним чинником підвищення конкурентоспроможності сучасних підприємств і організацій. Технологія віртуальних приватних мереж VPN дозволяє вирішувати ці завдання, забезпечуючи зв'язок між мережами, а також між віддаленим користувачем і корпоративною мережею за допомогою захищеного каналу (тунеля), «прокладеного» в загальнодоступній мережі Інтернет.

Переваги використання VPN технологій для захисту інформації в розподілених мережевих ІС масштабу підприємства:

- можливість захисту усієї корпоративної мережі — від великих локальних мереж офісів до окремих робітників місць. Захист може бути поширений на усі ланки мережі — від сегментів локальних мереж до комунікаційних каналів глобальних мереж, у тому числі виділених і комутованих ліній;
- масштабованість системи захисту, т. е. для захисту об'єктів різної складності і продуктивності можна використати адекватні по рівню складнощі, продуктивності і вартості програмні або програмно апаратні засоби захисту;
- використання ресурсів відкритих мереж як окремих комунікаційних ланок корпоративної мережі; усі загрози, що виникають при використанні мереж загального користування, компенсуватимуться засобами захисту інформації;

- забезпечення підконтрольності роботи мережі і достовірна ідентифікація усіх джерел інформації. При необхідності може бути забезпечена аутентифікація трафіку на рівні окремих користувачів;
- сегментація ІС і організація безпечної експлуатації системи, оброблювальної інформацію різних рівнів конфіденційності, програмними і програмно апаратними засобами захисту інформації.

Технологія VPN входить до числа найважливіших технологій, які планують використати підприємства в найближчому майбутньому.

Лекція 11 ЗАХИСТ НА КАНАЛЬНОМУ І СЕАНСОВОМУ РІВНЯХ

Віртуальний захищений канал можна побудувати за допомогою системних засобів, реалізованих на різних рівнях моделі взаємодії відкритих систем OSI. Від вибраного рівня OSI залежить функціональність VPN, що реалізовується, і її сумісність із застосуваннями КІС, а також з іншими засобами захисту.

Засоби VPN, вживані на канальному рівні моделі OSI, дозволяють забезпечити інкапсуляцію різних видів трафіку третього рівня (і вище) і побудову віртуальних тунелів типу «точка-точка» (від маршрутизатора до маршрутизатора або від персонального комп'ютера до шлюзу ЛВС).

При побудові захищених віртуальних мереж на сеансовому рівні з'являється можливість криптографічного захисту інформаційного обміну, включаючи аутентифікацію, а також реалізації ряду функцій посередництва між взаємодіючими сторонами.

11.1. Протоколи формування захищених каналів на канальному рівні

Протоколи PPTP (Point — to — Point Tunneling Protocol), L2F (Layer — 2 Forwarding) і L2TP (Layer — 2 Tunneling Protocol) — це протоколи тунелювання канального рівня моделі OSI. Загальною властивістю цих протоколів є те, що вони використовуються для організації захищеного багатопротокольного віддаленого доступу до ресурсів корпоративної мережі через відкриту мережу, наприклад через Інтернет.

Усі три протоколи — PPTP, L2F і L2TP — зазвичай відносять до протоколів формування захищеного каналу, проте цьому визначенню точно відповідає тільки протокол PPTP, який забезпечує тунелювання і шифрування передаваних даних. Протоколи L2F і L2TP підтримують тільки функції тунелювання. Для захисту даних, що тунелюють, в цих протоколах необхідно використати деякий додатковий протокол, зокрема IPSec.

Клієнтське ПЗ зазвичай використовує для віддаленого доступу стандартний протокол канального рівня PPP (Point — to — Point Protocol). Протоколи PPTP, L2F і L2TP грунтуються на протоколі PPP і є його розширеннями. Спочатку протокол PPP, розташований на канальному рівні, був розроблений для інкапсуляції даних і їх доставки по з'єднаннях типу «точка-точка». Цей протокол служить також для організації асинхронних (наприклад, комутованих) з'єднань. Зокрема, в налаштуваннях комутованого доступу видалених систем Windows 2000 або Windows 9x зазвичай вказується підключення до сервера по протоколу PPP.

У набір PPP входять протокол управління з'єднанням LCP (Link Control Protocol), відповідальний за конфігурацію, установку, роботу і завершення з'єднання «точка-точка», і протокол управління мережею NCP (Network Control Protocol), здатний інкапсулювати в PPP протоколи мережевого рівня для транспортування через з'єднання «точка-точка». Це дозволяє одночасно передавати пакети Novell IPX і Microsoft IP по одному з'єднанню PPP.

Для доставки конфіденційних даних з однієї точки в іншу через мережі загального користування спочатку проводиться інкапсуляція даних за допомогою протоколу PPP, потім протоколи PPTP і L2TP виконують шифрування даних і

власну інкапсуляцію. Після того, як тунельний протокол доставляє пакети з початкової точки тунеля в кінцеву, виконується деінкапсуляція.

На фізичному і канальному рівнях протоколи PPTP і L2TP ідентичні, але на цьому їх схожість закінчується і починаються відмінності.

11.1.1. Протокол PPTP

Протокол PPTP (Point - to - Point Tunneling Protocol), розроблений компанією Microsoft за підтримки інших компаній, призначений для створення захищених віртуальних каналів при доступі видалених користувачів до локальних мереж через Інтернет. Він припускає створення криптозахищеного тунеля на канальному рівні моделі OSI як для випадку прямого з'єднання віддаленого комп'ютера з відкритою мережею, так і для випадку під'єднування його до відкритої мережі по телефонній лінії через провайдера [9, 32].

Протокол PPTP отримав практичне поширення завдяки компанії Microsoft, що реалізувала його у своїх ОС Windows NT/2000. Деякі виробники шлюзів VPN також підтримують цей протокол. Протокол PPTP дозволяє створювати захищені канали для обміну даними по протоколах IP, IPX або NetBEUI. Дані цих протоколів упаковуються в кадри PPP і потім інкапсулюються за допомогою протоколу PPTP в пакети протоколу IP, за допомогою якого переносяться в зашифрованому виді через будь-яку мережу TCP/IP.

Пакети, що передаються у рамках сесії PPTP, мають наступну структуру (Рис. 11.1):

- заголовок канального рівня, використовуваний усередині Інтернету, наприклад заголовок кадру Ethernet;
- заголовок IP, що містить адреси відправника і одержувача пакету;
- заголовок загального методу інкапсуляції для маршрутизації GRE (Generic Routing Encapsulation);
- початковий пакет PPP, включаючий пакет IP, IPX або NetBEUI.

Заголовок кадра передачі	IP-заголовок	GRE - заголовок	PPP - заголовок	Зашифровані дані PPP	Закінчення кадра передачі

Рис. 11.1. Структура пакету для пересилки по тунелю PPTP

Приймаючий вузол мережі витягає з пакетів IP кадри PPP, а потім витягає з кадру PPP початковий пакет IP, IPX або NetBEUI і відправляє його по локальній мережі конкретному адресатові. Багатопротокольність інкапсулюючих протоколів канального рівня, до яких відноситься протокол PPTP, є їх важливою перевагою перед протоколами захищеного каналу більш високих рівнів. Наприклад, якщо в корпоративній мережі використовуються IPX або NetBEUI, застосування протоколів IPSec або SSL просто неможливе, оскільки вони орієнтовані тільки на один протокол мережевого рівня IP.

Такий спосіб інкапсуляції забезпечує незалежність від протоколів мережевого рівня моделі OSI і дозволяє здійснювати захищений віддалений доступ через відкриті IP- мережі до будь-яких локальних мереж (IP, IPX або NetBEUI), Згідно з протоколом PPTP при створенні захищеного віртуального каналу

проводиться аутентифікація віддаленого користувача і шифрування передаваних даних (Рис. 11.2).

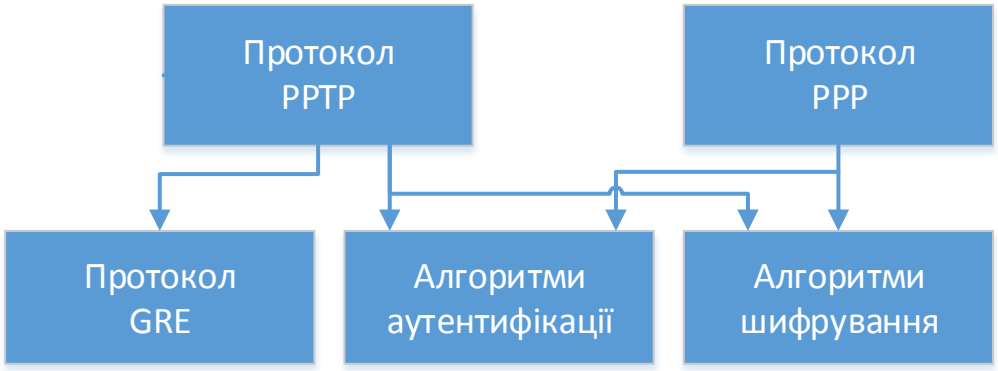

Рис. 11.2. Архітектура протоколу PPTP

Для аутентифікації віддаленого користувача можуть використовуватися різні протоколи, вживані для PPP. У реалізації PPTP, включеною компанією Microsoft в Windows 98/ NT/2000, підтримуються наступні протоколи аутентифікації: протокол розпізнавання по паролю PAP (Password Authentication Protocol), протокол розпізнавання при рукостисканні MSCHAP (Microsoft Challenge — Handshaking Authentication Protocol) і протокол розпізнавання EAP — TLS (Extensible Authentication Protocol — Transport Layer Security). При використанні протоколу PAP ідентифікатори і паролі передаються по лінії зв'язку в незашифрованому виді, при цьому тільки сервер проводить аутентифікацію клієнта. При використанні протоколів MSCHAP і EAP — TLS забезпечуються захист від повторного використання зловмисником перехоплених пакетів із зашифрованим паролем і взаємна аутентифікація клієнта і VPN— сервера.

Шифрування за допомогою PPTP гарантує, що ніхто не зможе отримати доступ до даних при пересилці через Internet. Протокол шифрування MPPE (Microsoft Point - to - Point Encryption) сумісний тільки з MSCHAP (версії 1 і 2) і EAP - TLS і уміє автоматично вибирати довжину ключа шифрування при узгодженні параметрів між клієнтом і сервером. Протокол MPPE підтримує роботу з ключами завдовжки 40, 56 або 128 біт. Протокол PPTP змінює значення ключа шифрування після кожного прийнятого пакету.

Для протоколу PPTP визначені дві основні схеми застосування:

1) схема тунелювання при прямому з'єднанні віддаленого комп'ютера з Інтернетом;

2) схема тунелювання при підключенні віддаленого комп'ютера до Інтернету по телефонній лінії через провайдера [32, 45].

Розглянемо реалізацію 1-ої схеми тунелювання (Рис. 11.3). Віддалений користувач встановлює видалене з'єднання з локальною мережею за допомогою клієнтської частини сервісу віддаленого доступу RAS (Remote Access Service), що входить до складу Windows 98/NT. Потім користувач звертається до сервера віддаленого доступу локальної мережі, вказуючи його IP- адреса, і встановлює з ним зв'язок по протоколу PPTP.

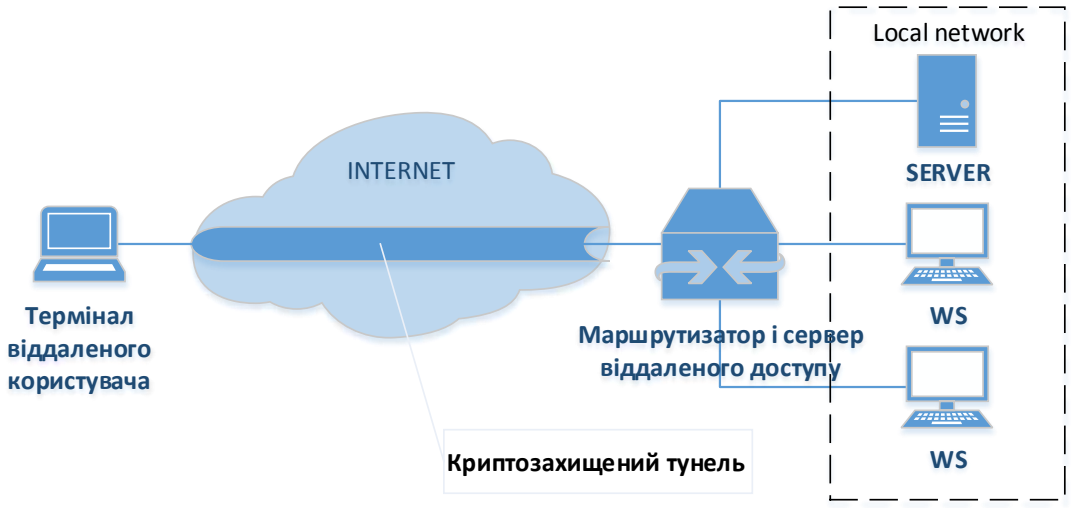

Рис. 11.3. Схема тунелювання при прямому під’єднанні комп'ютера віддаленого користувача до Internet

Функції сервера віддаленого доступу може виконувати пограничний маршрутизатор локальної мережі. На комп'ютері віддаленого користувача мають бути встановлені клієнтська частина сервісу RAS і драйвер PPTP, які входять до складу Windows, а на сервері віддаленого доступу локальної мережі — сервер RAS і драйвер PPTP, що входять до складу Windows NT Server. Протокол PPTP визначає декілька службових повідомлень, якими обмінюються взаємодіючі сторони. Службові повідомлення передаються по протоколу TCP. Після успішної аутентифікації починається процес захищеного інформаційного обміну. Внутрішні сервери локальної мережі можуть не підтримувати протокол PPTP, оскільки пограничний маршрутизатор витягає кадри PPP з пакетів IP і посилає їх по локальній мережі в необхідному форматі — IP, IPX або NetBIOS.

11.1.2. Протокол L2TP

Протокол L2F (Layer - 2 Forwarding) був розроблений компанією Cisco Systems для побудови захищених віртуальних мереж на канальному рівні моделі OSI як альтернатива протоколу PPTP.

Проте нині він фактично поглинений протоколом L2TP, тому далі розглядатимуться основні можливості і властивості протоколу L2TP.

Протокол L2TP (Layer - 2 Tunneling Protocol) розроблений в організації IETF (Internet Engineering Task Force) за підтримки компаній Microsoft і Cisco Systems. Протокол L2TP розроблявся як протокол захищеного тунелювання PPP-трафіку через мережі загального призначення з довільним середовищем. Робота над цим протоколом велася на основі протоколів PPTP і L2F, і в результаті він увібрав в себе кращі якості початкових протоколів [9].

На відміну від PPTP, протокол L2TP не прив'язаний до протоколу IP, тому він може бути використаний в мережах з комутацією пакетів, наприклад в мережах ATM (Asynchronous Transfer Mode) або в мережах з ретрансляцією кадрів (frame relay). Крім того, в протокол L2TP додана важлива функція управління потоками даних, а також ряд відсутніх в специфікації протоколу PPTP функцій захисту, зокрема, включена можливість роботи з протоколами AH і ESP стека протоколів IPSec (Рис. 11.4).

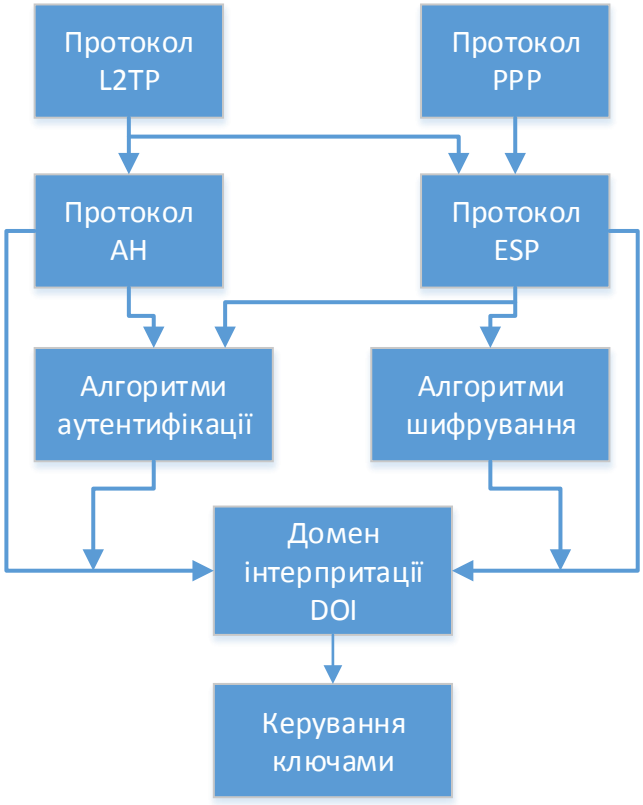

Рис. 11.4. Архітектура протоколу L2TP

По суті, гібридний протокол L2TP є розширенням протоколу PPP функціями аутентифікації видалених користувачів, створення захищеного віртуального з'єднання і управління потоками даних.

Протокол L2TP застосовує в якості транспорту протокол UDP і використовує однаковий формат повідомлень як для управління тунелем, так і для пересилки даних.

Хоча протокол PPTP забезпечує достатню міру безпеки, але все таки протокол L2TP (поверх IPSec) надійніший. Протокол L2TP (поверх IPSec) забезпечує аутентифікацію на рівнях «користувач» і «комп'ютер», а також виконує аутентифікацію і шифрування даних.

Після того, як L2TP (поверх IPSec) завершує процес аутентифікації комп'ютера, виконується аутентифікація на рівні користувача.

На відміну від своїх попередників — протоколів PPTP і L2F, протокол L2TP надає можливість відкривати між кінцевими абонентами відразу декілька тунелів, кожен з яких може бути виділений для окремого застосування. Ці особливості забезпечують гнучкість і безпеку тунелювання.

Згідно специфікації протоколу L2TP роль сервера віддаленого доступу провайдера повинен виконувати концентратор доступу LAC (L2TP Access Concentrator), який забезпечує видаленому користувачеві мережевий доступ до його локальної мережі через Інтернет. Сервером віддаленого доступу локальної мережі повинен виступати мережевий сервер LNS (L2TP Network Server), що функціонує на сумісних з протоколом PPP платформах (Рис. 11.5).

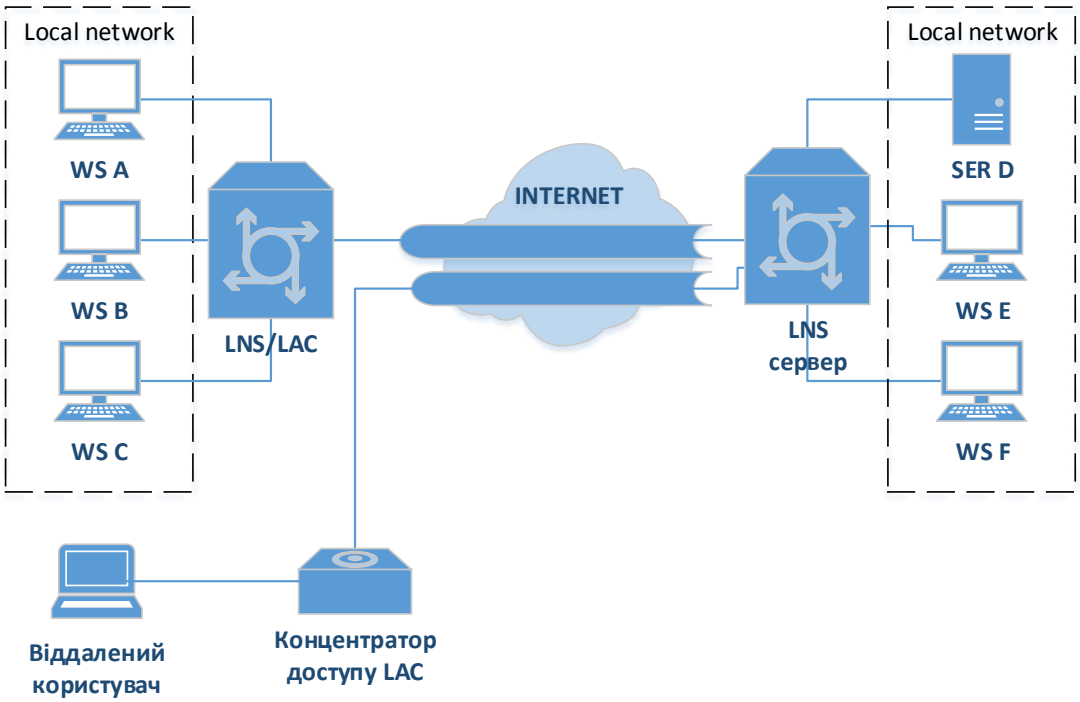

Рис. 11.5. Схеми тунелювання по протоколу L2TP

Формування захищеного віртуального каналу в протоколі L2TP здійснюється в три етапи:

- встановлення з'єднання з сервером віддаленого доступу локальної мережі;
- аутентифікація користувача;
- конфігурація захищеного тунеля [9].

Слід зазначити, що протокол L2TP не визначає конкретних методів криптозахисту і припускає можливість застосування різних стандартів шифрування. Якщо захищений тунель планується сформувати в IP- мережах, тоді для реалізація криптозахисту використовується протокол IPSec. Протокол L2TP поверх IPSec забезпечує більш високу міру захисту даних, чим PPTP, оскільки використовує алгоритм шифрування 3DES або AES. Якщо такий високий рівень захисту не потрібний, можна використати алгоритм DES з одним 56-розрядним ключем. Крім того, за допомогою алгоритму HMAC (Hash Message Authentication Code) протокол L2TP забезпечує аутентифікацію даних, для чого цей алгоритм створює хеш довжиною 128 розрядів.

Таким чином, функціональні можливості протоколів PPTP і L2TP різні. Протокол PPTP може застосовуватися тільки в IP- мережах. Протокол L2TP може використовуватися не лише в IP- мережах. Протокол L2TP поверх IPSec пропонує більше рівнів безпеки, чим PPTP, і може гарантувати майже 100% -у безпеку важливих для організації даних.

Проте при усіх своїх достоїнствах протокол L2TP не зміг здолати ряд недоліків тунельної передачі даних на канальному рівні:

- для реалізації протоколу L2TP потрібна підтримка провайдерів ISP;
- протокол L2TP обмежує трафік рамками вибраного тунеля і позбавляє користувачів доступу до інших частин Інтернету;
- специфікація L2TP забезпечує стандартне шифрування тільки в IP-мережах за допомогою протоколу IPSec.

11.2. Протоколи формування захищених каналів на сеансовому рівні

Найвищим рівнем моделі OSI, на якому можливе формування захищених віртуальних каналів, являється п'ятий — сеансовий рівень, При побудові захищених віртуальних мереж на сеансовому рівні з'являється можливість криптографічного захисту інформаційного обміну, включаючи аутентифікацію, а також реалізації ряду функцій посередництва між взаємодіючими сторонами.

Дійсно, сеансовий рівень моделі OSI відповідає за установку логічних з'єднань і управління цими з'єднаннями. Тому існує можливість застосування на цьому рівні програм-посередників, перевіряючих допустимість запрошених з'єднань і таких, що забезпечують виконання інших функцій захисту міжмережевої взаємодії.

Проте на сеансовому рівні починається безпосередня залежність від застосувань, що реалізовують високорівневі протоколи. Тому реалізація протоколів захисту інформаційного обміну, що відповідають цьому рівню, у більшості випадків вимагає внесення змін до високорівневих мережевих застосувань.

Для захисту інформаційного обміну на сеансовому рівні широке поширення отримав протокол SSL (Secure Sockets Layer). Для виконання на сеансовому рівні функцій посередництва між взаємодіючими сторонами організацією IETF (Internet Engineering Task Force) як стандарт прийнятий протокол SOCKS [9].

11.2.1. Протоколи SSL/TLS

Протокол SSL застосовується в якості протоколу захищеного каналу, працюючого на сеансовому рівні моделі OSI. Цей протокол використовує криптографічні методи захисту інформації для забезпечення безпеки інформаційного обміну. Протокол SSL виконує усі функції по створенню захищеного каналу між двома абонентами мережі, включаючи їх взаємну аутентифікацію, забезпечення конфіденційності, цілісності і автентичності передаваних даних. Ядром протоколу SSL є технологія комплексного використання асиметричних і симетричних криптосистем.

Взаємна аутентифікація обох сторін в SSL виконується шляхом обміну цифровими сертифікатами відкритих ключів користувачів (клієнта і сервера), завіреними цифровим підписом спеціальних сертифікаційних центрів. Протокол SSL підтримує сертифікати, що відповідають загальноприйнятому стандарту X. 509, а також стандарти інфраструктури відкритих ключів PKI (Public Key Infrastructure), за допомогою якої організовується видача і перевірка достовірності сертифікатів.

Конфіденційність забезпечується шифруванням передаваних повідомлень з використанням симетричних сесійних ключів, якими сторони обмінюються при встановленні з'єднання. Сесійні ключі передаються також в зашифрованому виді, при цьому вони шифруються за допомогою відкритих ключів, витягнутих з сертифікатів абонентів. Використання для захисту повідомлень симетричних ключів пов'язане з тим, що швидкість процесів шифрування і розшифрування на основі симетричного ключа істотно вища, ніж при використанні несиметричних ключів. Достовірність і цілісність циркулюючої інформації забезпечується за рахунок формування і перевірки електронного цифрового підпису.

В якості алгоритмів асиметричного шифрування використовуються алгоритм RSA, а також алгоритм Діффі — Хеллмана. Допустимими алгоритмами симетричного шифрування є RC2, RC4, DES, 3DES і AES. Для обчислення хеш-функцій можуть застосовуватися стандарти MD5 і SHA — 1. У протоколі SSL версії 3.0 набір криптографічних алгоритмів є розширюваним.

Згідно з протоколом SSL криптозахищенні тунелі створюються між кінцевими точками віртуальної мережі. Ініціаторами кожного захищеного тунеля є клієнт і сервер, що функціонують на комп'ютерах в кінцевих точках тунеля (Рис. 11.6).

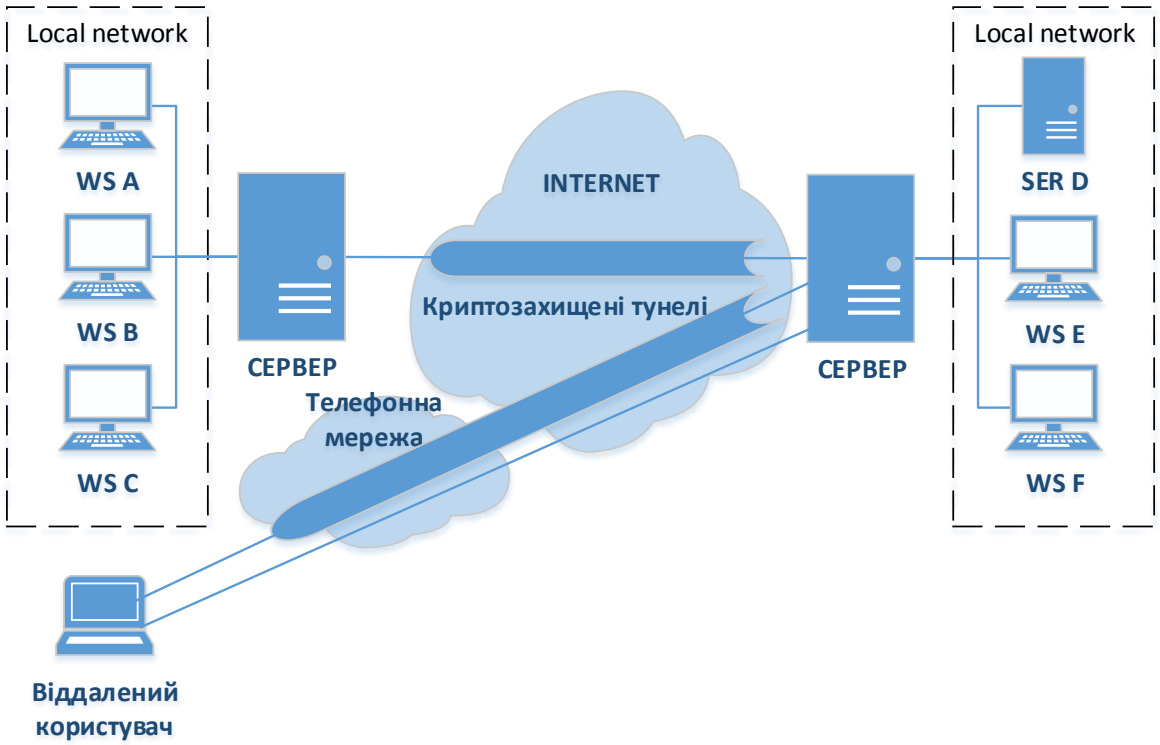

Рис. 11.6. Криптозахист тунелів, сформованих на основі протоколу SSL

Протокол SSL передбачає наступні етапи взаємодії клієнта і сервера при формуванні і підтримці з'єднання, що захищається:

- встановлення SSL- сесії;
- захищена взаємодія.

В процесі встановлення SSL- сесії вирішуються наступні завдання:

- аутентифікація сторін;
- узгодження криптографічних алгоритмів і алгоритмів стискування, які використовуватимуться при захищеному інформаційному обміні;
- формування загального секретного мастер-ключа;
- генерація на основі сформованого мастер-ключа загальних секретних сеансових ключів для криптозахисту інформаційного обміну [9, 65].

Процедура встановлення SSL- сесії, що називається також процедурою рукостискання, відпрацьовується перед безпосереднім захистом інформаційного

обміну і виконується по протоколу початкового (Handshake Protocol), SSL, що входить до складу протоколу.

При встановленні повторних з'єднань між клієнтом і сервером сторони можуть, за взаємною угодою, формувати нові сеансові ключі на основі «старого» загального «секрету» (ця процедура називається «продовженням» SSL сесії).

Протокол SSL 3.0 підтримує три режими аутентифікації:

- взаємну аутентифікацію сторін;
- одностороннюю аутентифікацію сервера без аутентифікації клієнта;
- повну анонімність.

При використанні останнього варіанту забезпечується захист інформаційного обміну без яких-небудь гарантій відносно достовірності сторін. В цьому випадку взаємодіючі сторони не захищені від атак, пов'язаних з підміною учасників взаємодії.

У реалізаціях протоколу SSL для аутентифікації взаємодіючих сторін і формування загальних секретних ключів зазвичай використовують алгоритм RSA.

Відповідність між відкритими ключами і їх власниками встановлюється за допомогою цифрових сертифікатів, що видаються спеціальними центрами сертифікації (див. л. 13).

Протокол SSL пройшов перевірку часом, працюючи в популярних браузерах Netscape Navigator і Internet Explorer, а також Web- серверах провідних виробників. У січні 1999 р. на зміну версії SSL 3.0 прийшов протокол TLS (Transport Layer Security), який базується на протоколі SSL і нині є стандартом Інтернету. Відмінності між протоколами SSL 3.0 і TLS 1.0 не занадто істотні. Протокол SSL став промисловим протоколом, Internet, що розвивається і просувається поза технічними координуючими інститутами.

Протокол SSL підтримується ПЗ серверів і клієнтів, що випускаються провідними західними компаніями. Істотним недоліком протоколу SSL є те, що практично усі продукти, підтримувальні SSL, через експортні обмеження доступні за межами США лише в усіченому варіанті (з довжиною сеансового ключа 40 біт для алгоритмів симетричного шифрування і 512 біт для алгоритму RSA, використовуваного на етапі встановлення SSL- сесії).

До недоліків протоколів SSL і TLS можна віднести те, що для транспортування своїх повідомлень вони використовують тільки один протокол мережевого рівня — IP, і, отже, можуть працювати тільки в IP-мережах.

Крім того, в SSL для аутентифікації і шифрування використовуються однакові ключі, що за певних умов може привести до потенційної уразливості. Подібне рішення дає можливість зібрати більше статистичного матеріалу, чим при аутентифікації і шифруванні різними ключами.

11.2.2. Протокол SOCKS

Протокол SOCKS організовує процедуру взаємодії клієнт-серверних застосувань на сеансовому рівні моделі OSI через сервер-посередник, або ргоху-сервер [9].

У загальному випадку програми-посередники, які традиційно використовуються в МЕ, можуть виконувати наступні функції:

- ідентифікацію і аутентифікацію користувачів;

- криптозахист передаваних даних;
- розмежування доступу до ресурсів внутрішньої мережі;
- розмежування доступу до ресурсів зовнішньої мережі;
- фільтрацію і перетворення потоку повідомлень, наприклад пошук вірусів і прозоре шифрування інформації;
- трансляцію внутрішніх мережевих адрес для вихідних потоків повідомлень.

Спочатку протокол SOCKS розроблявся тільки для перенаправлення запитів до серверів з боку клієнтських застосувань, а також повернення цим застосуванням отриманих відповідей. Перенаправлення запитів і відповідей між клієнт-серверними застосуваннями вже дозволяє реалізувати функцію трансляції мережевих IP- адрес NAT (Network Address Translation). Заміна у вихідних пакетів внутрішніх IP- адрес відправників одним IP- адресою шлюзу дозволяє приховати топологію внутрішньої мережі від зовнішніх користувачів і тим самим ускладнити завдання НСД.

На основі протоколу SOCKS можуть бути реалізовані і інші функції посередництва по захисту мережевої взаємодії. Наприклад, протокол SOCKS може застосовуватися для контролю над напрямами інформаційних потоків і розмежування доступу залежно від атрибутів користувачів і інформації. Ефективність використання протоколу SOCKS для виконання функцій посередництва забезпечується його орієнтацією на сеансовий рівень моделі OSI. В порівнянні з посередниками прикладного рівня на сеансовому рівні досягається більш висока швидкодія і незалежність від високорівневих протоколів (HTTP, FTP, POP3, SMTP та ін.). Крім того, протокол SOCKS не прив'язаний до протоколу IP і не залежить від ОС. Наприклад, для обміну інформацією між клієнтськими застосуваннями і посередником може використовуватися протокол IPX.

Завдяки протоколу SOCKS ME і віртуальні приватні мережі можуть організувати безпечну взаємодію і обмін інформацією між різними мережами. Протокол SOCKS дозволяє реалізувати безпечне управління цими системами на основі уніфікованої стратегії. Слід зазначити, що на основі протоколу SOCKS можуть створюватися захищені тунелі для кожного застосування і сеансу окремо.

Згідно специфікації протоколу SOCKS розрізняють SOCKS - сервер, який доцільно встановлювати на шлюз (ME) мережі, і SOCKS- клієнт, якого встановлюють на кожен призначений для користувача комп'ютер. SOCKS- сервер забезпечує взаємодію з будь-яким прикладним сервером від імені того, що відповідає цьому серверу прикладного клієнта. SOCKS- клієнт призначений для перехоплення усіх запитів до прикладного сервера з боку клієнта і передачі їх SOCKS- серверу. Слід зазначити, що SOCKS- клієнти, що виконують перехоплення запитів клієнтських застосувань і взаємодію з SOCKS- сервером, можуть бути вбудовані в універсальні клієнтські програми. SOCKS- серверу відомо про трафік на рівні сеансу (сокета), тому він може здійснювати ретельний контроль і, зокрема, блокувати роботу конкретних застосувань користувачів, якщо вони не мають необхідних повноважень на інформаційний обмін.

Протокол SOCKS v5 схвалений організацією IETF (Internet Engineering Task Force) в якості стандарту Internet і включений в RFC 1928 [9].

Загальна схема встановлення з'єднання по протоколу SOCKS v5 може бути описана таким чином:

- запит прикладного клієнта, що бажає встановити з'єднання з яким-небудь прикладним сервером в мережі, перехоплює встановлений на цьому ж комп'ютері SOCKS - клієнт;
- з'єднавшись з SOCKS- сервером, SOCKS- клієнт повідомляє йому ідентифікатори усіх методів аутентифікації, які він підтримує;
- SOCKS- сервер вирішує, яким методом аутентифікації скористатися (якщо SOCKS- сервер не підтримує жоден з методів аутентифікації, запропонованих SOCKS - клієнтом, з'єднання розривається);
- за підтримки яких-небудь запропонованих методів аутентифікації SOCKS- сервер відповідно до вибраного методу аутентифікації користувача, від імені якого виступає SOCKS- клієнт; у разі безуспішної аутентифікації SOCKS-сервер розриває з'єднання;
- після успішної аутентифікації SOCKS- клієнт передає SOCKS- серверу DNS- ім'я або IP- адреса прошеного прикладного сервера в мережі і далі SOCKS-сервер на основі наявних правил розмежування доступу приймає рішення про встановлення з'єднання з цим прикладним сервером;
- у разі встановлення з'єднання прикладний клієнт і прикладний сервер взаємодіють один з одним по ланцюжку з'єднань, в якій SOCKS- сервер ретранслює дані, а також може виконувати функції посередництва по захисту мережевої взаємодії; наприклад, якщо в ході аутентифікації SOCKS- клієнт і SOCKS- сервер обмінялися сеансовим ключем, то увесь трафік між ними може шифруватися.

Аутентифікація користувача, виконувана SOCKS- сервером, може грунтуватися на цифрових сертифікатах у форматі X. 509 або паролях. Для шифрування трафіку між SOCKS - клієнтом і SOCKS- сервером можуть бути використані протоколи, орієнтовані на сеансовий або нижчі рівні моделі OSI. Окрім аутентифікації користувачів, трансляції IP- адрес і криптозахисту трафіку, SOCKS-сервер може виконувати також такі функції, як:

- розмежування доступу до ресурсів внутрішньої мережі;
- розмежування доступу до ресурсів зовнішньої мережі;
- фільтрація потоку повідомлень, наприклад, динамічний пошук вірусів;
- реєстрація подій і реагування на події, що задаються;
- кешування даних, що просяться із зовнішньої мережі.

Протокол SOCKS здійснює вбудовану підтримку популярних Web-навігаторів Netscape Navigator і Netscape Communicator компанії Netscape, а також Internet Explorer компанії Microsoft.

Спеціальні програми, звані соксифікаторами, доповнюють клієнтські застосування підтримкою протоколу SOCKS. До таких програм відноситься, наприклад, NEC SocksCap та ін. При установці соксифікатор впроваджується між призначеними для користувача застосуваннями і стеком комунікаційних протоколів. Далі в процесі роботи він перехоплює комунікаційні виклики, що формуються застосуваннями, і перенаправляє їх у разі потреби на SOCKS- сервер. За відсутності порушень встановлених правил безпеки робота SOCKS- клієнта абсолютно прозора для клієнтських застосувань і користувачів.

Таким чином, для формування захищених віртуальних мереж по протоколу SOCKS в точці сполучення кожної локальної мережі з Інтернетом на комп'ютері-шлюзі встановлюється SOCKS- сервер, а на робочих станціях в локальних мережах і на комп'ютерах видалених користувачів встановлюються SOCKS- клієнти. По

суті, SOCKS- сервер можна розглядати як МЕ, підтримувальний протокол SOCKS (Рис. 11.7).

Віддалені користувачі можуть підключатися до Інтернету будь-яким способом — по комутованій або виділеній лінії. При спробі користувача захищеної віртуальної мережі встановити з'єднання з яким-небудь прикладним сервером SOCKS- клієнт починає взаємодіяти з SOCKS- сервером. Після закінчення першого етапу взаємодії користувач буде аутентифікований, а перевірка правил доступу покаже, чи має він право з'єднатися з конкретним серверним застосуванням, що функціонує на комп'ютері з вказаною адресою. Подальша взаємодія може відбуватися по криптографічний захищеному каналу [45].

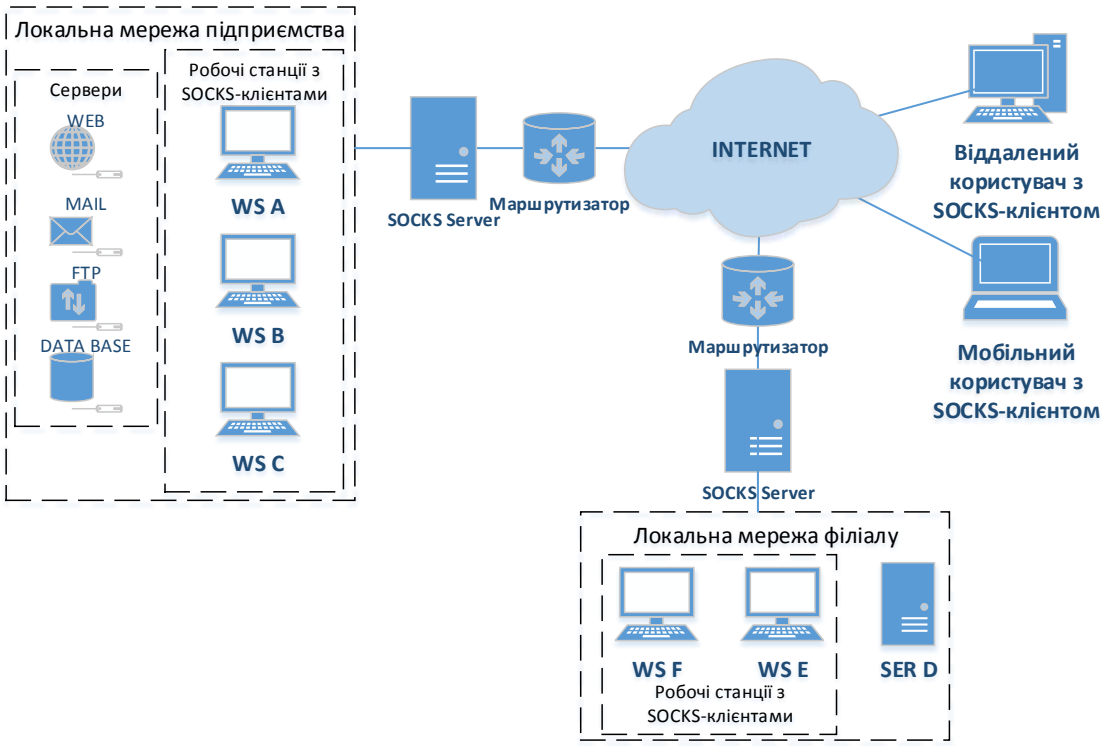

Рис. 11.7. Схема взаємодії по протоколу SOCKS

Окрім захисту локальної мережі від НСД, на SOCKS- сервер може покладатися контроль доступу користувачів цієї локальної мережі до відкритих ресурсів Інтернету (Telnet, WWW, SMTP, POP та ін.). Доступ є повністю авторизованим, оскільки ідентифікуються і аутентифікуються конкретні користувачі, а не комп'ютери, з яких вони входять в мережу. Правила доступу можуть забороняти або дозволяти з'єднання з конкретними ресурсами Інтернету залежно від повноважень конкретного співробітника. Дія правил доступу може залежати і від інших параметрів, наприклад від методу аутентифікації або часу доби.

На додаток до функцій розмежування доступу може виконуватися реєстрація подій і реагування на події, що задаються. Для досягнення більш високої міри безпеки мережевої взаємодії сервери локальної мережі, до яких дозволений доступ з боку Інтернету, мають бути виділені в окремий під'єднуваний до SOCKS- серверу сегмент, що утворює відкриту підмережу, що захищається.

11.3. Захист безпровідних мереж

Безпровідні мережі починають використовуватися практично у всьому світі. Це обумовлено їх зручністю, гнучкістю і порівняно невисокою вартістю. Безпровідні технології повинні задовольняти ряду вимог до якості, швидкості, радіусу прийому і захищеності, причому захищеність часто є найважливішим чинником.

Складність забезпечення безпеки безпровідної мережі очевидна. Якщо в дротяних мережах зловмисник повинен спочатку отримати фізичний доступ до кабельної системи або крайових пристроїв, то у безпровідних мережах ця умова відпадає само собою: оскільки дані передаються «по повітрю», для діставання доступу досить звичайного приймача, встановленого в радіусі дії мережі (див. розд. 2.2.3).

Проте, незважаючи на відмінності в реалізації, підхід до безпеки безпровідних мереж і їх дротяних аналогів ідентичний: тут є присутніми аналогічні вимоги до забезпечення конфіденційності і цілісності передаваних даних і, звичайно ж, до перевірки достовірності як безпровідних клієнтів, так і точок доступу.

Загальні відомості

Як і усі стандарти IEEE 802, базовий стандарт організації безпровідних локальних мереж IEEE 802.11 працює на нижніх двох рівнях моделі ISO/OSI — фізичному і канальному. Мережеве застосування, мережева ОС або протокол (наприклад, TCP/IP) так само добре працюватимуть в мережі 802.11, як і в мережі Ethernet.

Основна архітектура, особливості і служби визначаються у базовому стандарті 802.11 (див. розд. 4.2), який визначає два режими роботи безпровідної мережі — режим клієнт/сервер (чи режим інфраструктури) і режим «точка-точка» (Ad — hoc).

У режимі клієнт/сервер безпровідна мережа складається як мінімум з однієї точки доступу AP (Access point), підключеною до дротяної мережі, і деякого набору безпровідних крайових станцій. Така конфігурація носить назву базового набору служб BSS (Basic Service Set). Два або більше BSS, що утворюють єдину підмережу, формують розширений набір служб ESS (Extended Service Set). Оскільки більшості безпровідних станцій вимагається діставати доступ до файлових серверів, принтерів, Інтернету, доступних в дротяній локальній мережі, вони працюватимуть в режимі клієнт/сервер.

Режим «точка-точка» — це проста мережа, в якій зв'язок між численними станціями встановлюється безпосередньо, без використання спеціальної точки доступу. Такий режим корисний у тому випадку, якщо інфраструктура безпровідної мережі не сформована (наприклад, в готелі, виставковому залі, аеропорту).

На фізичному рівні стандарту 802.11 визначені 2 широкосмугових радіочастотних методу передачі і 1 — в інфрачервоному діапазоні. Радіочастотні методи працюють в ISM діапазоні 2,4 ГГц і зазвичай використовують смугу 83 Мгц від 2,400 ГГц до 2,483 ГГц. Технології широкосмугового сигналу, використовувані в радіочастотних методах, збільшують надійність, пропускну спроможність,

дозволяють багатьом незв'язаним один з одним пристроям розділяти одну смугу частот з мінімальними перешкодами один для одного.

Основне доповнення, внесене стандартом 802.11b в основний стандарт, — це підтримка двох нових швидкостей передачі даних — 5,5 і 11 Mbps. Для досягнення цих швидкостей був вибраний метод прямої послідовності DSSS (Direct Sequence Spread Spectrum).

Канальний (Data1ink) рівень стандарту 802.11 складається з двох підрівнів: управління логічним зв'язком LLC (Logical1ink Control) і управління доступом до носія MAC (Media Access Control).

Забезпечення безпеки безпровідних мереж

Система захисту безпровідних мереж WLAN, заснована на протоколі WEP (Wired Equivalent Privacy) первинного стандарту 802.11, має істотні недоліки. Проте з'явилися ефективніші технології забезпечення інформаційної безпеки WLAN, які описані в стандарті WPA (Wi – Fi Protected Access) організації WiFi Alliance і стандарті 802.11i інституту IEEE і покликані усунути недоліки стандарту 802.11. Оскільки процес розробки стандарту 802.11i занадто затягнувся, організація WiFi Alliance була вимушена запропонувати в 2002 р. власну технологію забезпечення інформаційної безпеки WLAN — стандарт WPA.

Стандарт WPA дуже привабливий тим, що відносно простий в реалізації і дозволяє захистити нині чинні WLAN. Стандарти WPA і 802.11i сумісні один з одним, тому використання підтримувальних WPA продуктів можна вважати початковим етапом переходу до системи захисту на базі стандарту 802.1n (див. розд. 4.2).

Між технологіями стандартів 802.11i і WPA багато спільного. Так, в них визначена ідентична архітектура системи безпеки з поліпшеними механізмами аутентифікації користувачів і протоколами поширення і оновлення ключів. Але є і істотні відмінності. Наприклад, технологія WPA базується на протоколі динамічних ключів TKIP (Temporal Key Integrity Protocol), підтримку якого у більшості облаштувань WLAN можна реалізувати шляхом оновлення їх ПЗ, а у більше функціональній концепції стандарту 802.11 і передбачено використання нового стандарту шифрування AES (Advanced Encryption Standard), з яким сумісно лише новітнє устаткування для WLAN.

У стандарті WPA передбачено використання захисних протоколів 802.lx, EAP, TKIP і RADIUS.

Механізм аутентифікації користувачів заснований на протоколі контролю доступу 802.1x (розроблений для дротяних мереж) і протоколі розширеної аутентифікації EAP (Extensible Authentication Protocol). Останній дозволяє мережевому адміністраторові задіяти алгоритми аутентифікації користувачів за допомогою сервера RADIUS (див. л. 13).

Функції забезпечення конфіденційності і цілісності даних базуються на протоколі TKIP, який на відміну від протоколу WEP використовує ефективніший механізм управління ключами, але той же самий алгоритм RC4 для шифрування даних. Згідно з протоколом TKIP, мережеві пристрої працюють з 48-бітовим вектором ініціалізації (на відміну від 24-бітового вектору ініціалізації протоколу WEP) і реалізують правила зміни послідовності його бітів, що виключає повторне використання ключів і здійснення гер1ау-атак.

У протоколі TKIP передбачені генерація нового ключа для кожного передаваного пакету і поліпшений контроль цілісності повідомлень за допомогою криптографічної контрольної суми MIC (Message Integrity Code), що перешкоджає хакерові змінювати вміст передаваних пакетів.

Система мережевої безпеки стандарту WPA працює в двох режимах: PSK (Pre - Shared Key) і Enterprise (корпоративний). Для розгортання системи, працюючої в режимі PSK, потрібний пароль, що розділяється. Таку систему нескладно встановлювати, але вона захищає WLAN не так надійно, як це робить система, що функціонує в режимі Enterprise з ієрархією динамічних ключів. Хоча протокол TKIP працює з тим же самим блоковим шифром RC4, який передбачений специфікацією протоколу WEP, технологія WPA захищає дані надійніше за останній.

Щоб точки доступу WLAN стали сумісними із стандартом WPA, досить модернізувати їх ПЗ. Для перекладу ж мережевої інфраструктури на стандарт 802.1 I знадобиться нове устаткування, що підтримує алгоритм шифрування AES, оскільки AES- шифрування створює велике навантаження на центральний процесор безпровідного клієнтського пристрою.

Щоб корпоративні точки доступу працювали в системі мережевої безпеки стандарту WPA або 802.11i, вони повинні підтримувати аутентифікацію користувачів по протоколу RADIUS і реалізовувати передбачений стандартом метод шифрування — TKIP або AES, що зажадає модернізації їх ПЗ. І ще одна вимога — швидко здійснювати повторну аутентифікацію користувачів після розриву з'єднання з мережею. Це особливо важливо для нормального функціонування застосувань, працюючих в реальному масштабі часу.

Якщо сервер RADIUS, вживаний для контролю доступу користувачів дротяної мережі, підтримує потрібні методи аутентифікації EAP, то його можна задіяти і для аутентифікації користувачів WLAN. Інакше слід встановити сервер WLAN RADIUS. Цей сервер працює таким чином: спочатку він перевіряє аутентифікуючу інформацію користувача (на відповідність вмісту своєї БД про їх ідентифікатори і паролі) або його цифровий сертифікат, а потім активізує динамічну генерацію ключів шифрування точкою доступу і клієнтською системою для кожного сеансу зв'язку.

Для роботи технології WPA потрібно механізм EAP - TLS (Transport Layer Security), тоді як в стандарті IEEE 802.11i застосування конкретних методів аутентифікації EAP не обмовляється. Вибір методу аутентифікації EAP визначається специфікою роботи клієнтських застосувань і архітектурою мережі. Щоб ноутбуки і кишенькові ПК працювали в системі мережевої безпеки стандарту WPA або 802.11, вони мають бути оснащені клієнтськими програмами, що підтримують стандарт 802.1 x.

Найпростішим, з точки зору розгортання, варіантом системи мережевої безпеки стандарту WPA є система, працююча в режимі PSK. Вона призначена для невеликих і домашніх офісів і не потребує сервера RADIUS, а для шифрування пакетів і розрахунку криптографічної контрольної суми MIC в ній використовується пароль PSK. Забезпечуваний нею рівень інформаційної безпеки мережі цілком достатній для більшості вищезгаданих офісів. З метою підвищення ефективності захисту даних слід застосовувати паролі, що містять не менше 20 символів.

Підприємствам доцільно впроваджувати у себе системи мережевої безпеки стандарту WPA з серверами RADIUS. Більшість компаній віддають перевагу саме таким системам, оскільки працюючі в режимі PSK рішення складніше адмініструвати і вони більше уразливі для хакерських атак.

До тих пір, поки засоби стандарту 802.11i не стануть доступними на ринку, WPA залишатиметься самим відповідним стандартом для захисту WLAN.

Стандарти WPA і 802.1 П достатньою мірою надійні і забезпечують високий рівень захищеності безпровідних мереж. Проте одного протоколу захисту недостатньо — слід також приділяти увагу правильній побудові і налаштуванню мережі.

Фізичний захист. При розгортанні Wi - Fi- мережі необхідно фізично обмежити доступ до безпровідних точок.

Правильне налаштування. Парадокс сучасних безпровідних мереж полягає в тому, що користувачі не завжди включають і використовують вбудовані механізми аутентифікації і шифрування.

Захист призначених для користувача пристроїв. Не слід повністю покладатися на вбудовані механізми захисту мережі. Найбільш оптимальним є метод ешелонованої оборони, перша лінія якої — засоби захисту, встановлені на стаціонарному ПК, ноутбуку або КПК.

Традиційні заходи. Ефективна робота комп'ютера в мережі немислима без класичних заходів зашиті — своєчасної установки оновлень, використання захисних механізмів, вбудованих в ОС і застосування, а також антивірусів. Проте цих заходів на сьогодні недостатньо, оскільки вони орієнтовані на захист від вже відомих загроз.

Моніторинг мережі. Слабка ланка в корпоративній мережі — самовільно встановлені точки доступу. Актуальним є завдання локалізації несанкціонованих точок доступу. Спеціальні засоби локалізації точок доступу дозволяють графічно відображати місце розташування «чужого» терміналу на карті поверху або будівлі. Якщо класичні методи не рятують від вторгнення, слід застосовувати системи виявлення атак.

VPN- агенти. Багато точок доступу працюють у відкритому режимі, тому необхідно використати методи захисту передаваних даних. На комп'ютері, що захищається, має бути встановлений VPN- клієнт, який візьме на себе рішення цієї задачі. Практично усі сучасні ОС (наприклад, Windows XP) містять у своєму складі такі програмні компоненти.

Лекція 12 ЗАХИСТ НА МЕРЕЖЕВОМУ РІВНІ — ПРОТОКОЛ IPSEC

Радикальне усунення уразливостей комп'ютерних мереж можливо при створенні системи захисту не для окремих класів застосувань, а для мережі в цілому. Стосовно IP-мереж це означає, що системи захисту повинні діяти на мережевому рівні моделі OSI. Перевага такого вибору полягає в тому очевидному факті, що в IP- мережах саме мережевий рівень відрізняється найбільшою гомогенністю: незалежно від вищерозміщених протоколів, фізичного середовища передачі і технології канального рівня транспортування даних по мережі не може бути проведене в обхід протоколу IP. Тому реалізація захисту мережі на третьому рівні автоматично гарантує як мінімум таку ж міру захисту усіх мережевих застосувань, причому без якої-небудь модифікації останніх.

При формуванні захищених віртуальних каналів на мережевому рівні моделі OSI досягається оптимальне співвідношення між прозорістю і якістю захисту. Розміщення засобів захисту на мережевому рівні робить їх прозорими для застосувань, оскільки між мережевим рівнем і застосуванням функціонує реалізація протоколу транспортного рівня. Для користувачів процедури захисту виявляються такими ж прозорими, як і сам протокол IP. На мережевому рівні існує можливість досить повної реалізації функцій захисту трафіку і управління ключами, оскільки саме на мережевому рівні виконується маршрутизація пакетів повідомлень.

Стек протоколів IPSec використовується для аутентифікації учасників обміну, тунелювання трафіку і шифрування IP— пакетів. Основне призначення протоколу IPSec (Internet Protocol Security) — забезпечення безпечної передачі даних по мережах IP. Оскільки архітектура IPSec сумісна з протоколом IPv4, її підтримку досить забезпечити на обох кінцях, з'єднання; проміжні мережеві вузли можуть взагалі нічого «не знати» про IPSec. Протокол IPSec може захищати трафік як поточної версії протоколу IPv4, вживаної сьогодні в Internet, так і трафік нової версії IPv6, яка поступово впроваджується в Internet.

12.1. Архітектура засобів безпеки IPSec

Основне призначення протоколів IPSec — забезпечення безпечної передачі даних по мережах IP. Застосування IPSec гарантує:

- цілісність передаваних даних (тобто дані при передачі не спотворені, не втрачені і не продубльовані);
- автентичність відправника (тобто дані передані саме тим відправником, який довів, що він той, за кого себе видає);
- конфіденційність передаваних даних (тобто дані передаються у формі, що запобігає їх несанкціонованому перегляду).

Слід зазначити, що зазвичай в поняття безпеки даних включають ще одну вимогу — доступність даних, що в даному контексті можна інтерпретувати як гарантію їх доставки. Протоколи IPSec не вирішують цю задачу, залишаючи її протоколу транспортного рівня TCP. Стек протоколів IPSec забезпечує захист інформації на мережевому рівні, що робить цей захист невидимим для працюючих застосувань.

Фундаментальною одиницею комунікації в IP- мережах являється IP-пакет. IP- пакет містить S- адреса джерела і D- адресу одержувача повідомлення, транспортний заголовок, інформацію про тип даних, які передаються в цьому пакеті, і самі дані (Рис. 12.1).

Рис. 12.1. Структура IP-пакета

Користувач сприймає мережу як надійно захищене середовище тільки у тому випадку, якщо він упевнений, що його партнер по обміну — саме той, за кого він себе видає (аутентифікація сторін), що передавані пакети не видимі сторонніми особами (конфіденційність зв'язку) і що отримувані дані не піддалися зміні в процесі передачі (цілісність даних).

Для того, щоб забезпечити аутентифікацію, конфіденційність і цілісність передаваних даних стек протоколів IPSec побудований на базі стандартизованих криптографічних технологій:

- обміну ключами згідно з алгоритмом Діффі-Хеллмана для розподілу секретних ключів між користувачами у відкритій мережі;
- криптографії відкритих ключів для підписки обмінів Діффі- Хеллмана, щоб гарантувати достовірність двох сторін і уникнути атак типу «man — in — the — middle»;
- цифрових сертифікатів для підтвердження достовірності відкритих ключів;
- блокових симетричних алгоритмів шифрування даних;
- алгоритмів аутентифікації повідомлень на базі функцій хешування.

Протокол IPSec визначає стандартні способи захисту інформаційного обміну на мережевому рівні моделі OSI для IP— мережі, що є основним видом відкритих мереж. Цей протокол входить до складу нової версії протоколу IP (IPv6) і застосований також до його по точної версії (IPv4). Для протоколу IPv4 підтримка IPSec є бажаною, а для IPv6 — обов'язковою. Протокол IPSec є системою відкритих стандартів, яка має чітко обкреслене ядро, і в той же час дозволяє доповнювати її новими протоколами, алгоритмами і функціями. Стандартизованими функціями IPSec— захисту можуть користуватися протоколи більш високих рівнів, зокрема, протоколи, що управляють, протоколи конфігурації, а також протоколи маршрутизації.

Основними завданнями встановлення і підтримки захищеного каналу є наступні:

- аутентифікація користувачів або комп'ютерів при ініціації захищеного каналу;
- шифрування і аутентифікація передаваних даних між кінцевими точками захищеного каналу;
- забезпечення кінцевих точок каналу секретними ключами, необхідними для роботи протоколів аутентифікації і шифрування даних.

Для вирішення перерахованих завдань система IPSec використовує комплекс засобів безпеки інформаційного обміну.

Більшість реалізацій протоколу IPSec мають наступні компоненти.

Основний протокол IPSec. Цей компонент реалізує протоколи ESP і AH. Він обробляє заголовки, взаємодіє з БД SPD і SAD для визначення політики безпеки, що застосовується до пакету.

Протокол управління обміном ключової інформації IKE (Internet Key Exchange). IKE зазвичай представляється як процес призначеного для користувача рівня, за винятком реалізацій, вбудованих в ОС.

База даних політик безпеки SPD (Security Policy Database). Це один з найважливіших компонентів, оскільки він визначає політику безпеки, що застосовується до пакету. SPD використовується основним протоколом IPSec при обробці пакетів, що входять і витікаючих.

База цих безпечних асоціацій SAD (Security Association Database). БД SAD зберігає список безпечних асоціацій SA (Security Association) для обробки інформації, що входить і витікаючої. Вихідні SA використовуються для захисту витікаючих пакетів, а SA, що входять, використовуються для обробки пакетів із заголовками IPSec. БД SAD заповнюється SA вручну або за допомогою протоколу управління ключами IKE.

Управління політикою безпеки і безпечними асоціаціями SA. Це — застосування, які управляють політикою безпеки і SA [9].

Основний протокол IPSec (реалізовуючий ESP і AH) тісно взаємодіє з транспортним і мережевим рівнем стека протоколів TCP/IP. Фактично протокол IPSec є частиною мережевого рівня. Основний модуль протоколу IPSec забезпечує два інтерфейси: вхідний і вихідний. Вхідний інтерфейс використовується пакетами, що входять, а вихідний — вихідними. Реалізація IPSec не повинна залежати від інтерфейсу між транспортним і мережевим рівнем стека протоколів TCP/IP.

БД SPD і SAD істотно впливають на ефективність роботи IPSec. Вибір структури даних для зберігання SPD і SAD є критичним моментом, від якого залежить продуктивність IPSec. Особливості реалізації SPD і SAD залежать від вимог продуктивності і сумісності системи.

Усі протоколи, що входять в IPSec, можна розділити на дві групи:

1) протоколи, що безпосередньо здійснюють обробку передаваних даних (для забезпечення їх захисту);

2) протоколи, що дозволяють автоматично погоджувати параметри захищених з'єднань, необхідні для протоколів 1-ої групи.

Архітектура засобів безпеки IPSec представлена на Рис. 12.2.

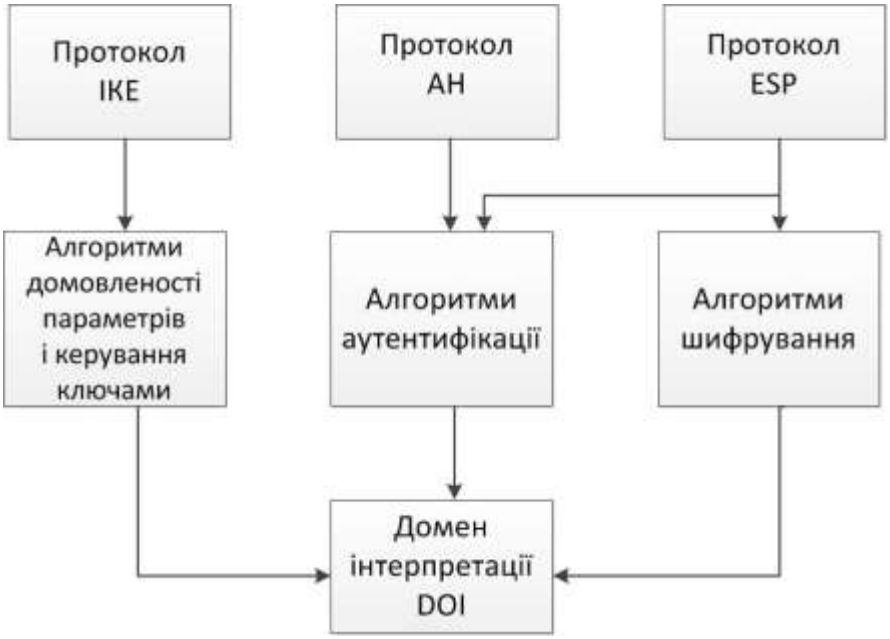

Рис. 12.2. Архітектура стека протоколів IPSec

На верхньому рівні розташовані 3 протоколи, що становлять ядро IPSec:

- протокол узгодження параметрів віртуального каналу і управління ключами IKE (Internet Key Exchange), визначальний спосіб ініціалізації захищеного каналу, включаючи узгодження використовуваних алгоритмів криптозахисту, а також процедури обміну і управління секретними ключами у рамках захищеного з'єднання;
- протокол аутентифікуючого заголовка AH (Authentication header), що забезпечує аутентифікацію джерела даних, перевірку їх цілісності і достовірності після прийому, а також захист від нав'язування повторних повідомлень;
- протокол інкапсулюючого захисту вмісту ESP (Encapsulating Security Payload), що забезпечує криптографічне закриття, аутентифікацію і цілісність передаваних даних, а також захист від нав'язування повторних повідомлень.

Розділення функцій захисту між двома протоколами AH і ESP обумовлене вживаною у багатьох країнах практикою обмеження експорту і/або імпорту засобів, що забезпечують конфіденційність даних шляхом шифрування. Кожен з протоколів AH і ESP може використовуватися як самостійно, так і спільно з іншим. З короткого переліку функцій протоколів AH і ESP видно, що можливості цих протоколів частково перекриваються.

Протокол AH відповідає тільки за забезпечення цілісності і аутентифікації даних, тоді як протокол ESP є потужнішим, оскільки може шифрувати дані, а крім того, виконувати функції протоколу AH (хоча, як побачимо пізніше, аутентифікація і цілісність забезпечуються ним в дещо урізаному вигляді).

Протокол ESP може підтримувати функції шифрування і аутентифікації/цілісності у будь-яких комбінаціях, тобто або і ту і іншу групу функцій, або тільки аутентифікацію/цілісність, або тільки шифрування.

Середній рівень архітектури IPSec утворюють алгоритми узгодження параметрів і управління ключами, вживані в протоколі IKE, а також алгоритми аутентифікації і шифрування, використовувані в протоколах аутентифікуючого заголовка AH і інкапсулюючого захисту вмісту ESP.

Слід зазначити, що протоколи захисту віртуального каналу верхнього рівня архітектура IPSec (AH і ESP) не залежить від конкретних криптографічних алгоритмів. За рахунок можливості використання великого числа різноманітних алгоритмів аутентифікації і шифрування IPSec забезпечує високу міру гнучкості організації захисту мережі. Гнучкість IPSec полягає в тому, що для кожного завдання пропонується декілька способів її рішення. Вибрані методи для одного завдання зазвичай не залежать від методів реалізації інших завдань. Наприклад, вибір для шифрування алгоритму AES не впливає на вибір функції обчислення дайджеста, використовуваного для аутентифікації даних.

Нижній рівень архітектури IPSec утворює так званий домен інтерпретації DOI (Domain of Interpretation). Необхідність застосування домена інтерпретації DOI обумовлена наступними причинами. Протоколи AH і ESP мають модульну структуру, допускаючи застосування користувачами по їх погодженому вибору різних криптографічних алгоритмів шифрування і аутентифікації. Тому потрібний модуль, який міг би забезпечити спільну роботу усіх вживаних і знову таких, що включаються протоколів і алгоритмів. Саме такі функції покладені на домен інтерпретації DOI. Домен інтерпретації DOI в якості БД зберігає відомості про використовуваних в IPSec протоколах і алгоритмах, їх параметрах, протокольних ідентифікаторах і т. п. По суті, він виконує роль фундаменту в архітектурі IPSec. Для того, щоб використати алгоритми, що відповідають національним стандартам в якості алгоритмів аутентифікації і шифрування в протоколах AH і ESP, необхідно зареєструвати ці алгоритми в домені інтерпретації DOI [9].

12.2. Захист передаваних даних за допомогою протоколів AH і ESP

Протокол аутентифікуючого заголовка AH і протокол інкапсулюючого захисту вмісту ESP можуть працювати в тунельному або транспортному режимах. Для виконання своїх завдань по забезпеченню безпечної передачі даних протоколи AH і ESP включають в оброблювані ними пакети додаткову службову інформацію, оформляючи її у вигляді заголовків.

12.2.1. Протокол аутентифікуючого заголовка AH

Протокол аутентифікуючого заголовка AH (Authentication Header) забезпечує перевірку автентичності і цілісності IP- пакетів, а також захист від відтворення раніше посланих IP-пакетів.

Протокол AH дозволяє приймальній стороні переконатися, що:

- пакет був відправлений саме тією стороною, з якою встановлена ця асоціація;
- вміст пакету не піддався спотворенням в процесі передачі його по мережі;
- пакет не є дублікатом деякого пакету, отриманого раніше.

Протокол AH повністю захищає від підробки і спотворення вміст IP— пакетів, включаючи дані протоколів більш високих рівнів. Повнота захисту полів IP— заголовків залежить від використовуваного режиму роботи — тунельного або транспортного. Проте протокол AH не забезпечує конфіденційність передаваних даних, тобто не призначений для їх шифрування. Дані можуть бути прочитані проміжними вузлами, але не можуть бути змінені. Цілісність і автентичність даних

забезпечуються додаванням аутентифікуючого заголовка (AH) перед заголовком IP і заголовком транспортного рівня (TCP/UDP). Формат заголовка AH показаний на Рис. 12.3.

Рис. 12.3. Формат заголовка AH

Заголовок AH включає поля:

- наступний заголовок (Next Header) — однобайтове поле, що містить код протоколу наступного заголовка, вкладеного в IPSec— пакет, наприклад код протоколу TCP або ESP, чий заголовок йде за AH;
- довжина (Payload Leri) — вказує довжину заголовка AH в 32-бітових словах;
- індекс параметрів захисту SPI (Security Parameters Index) — є 32-розрядною міткою безпечної асоціації SA (Security Association), що містить усі параметри тунеля IPSec, включаючи типи криптографічних алгоритмів і ключі шифрування. На підставі індексу SPI пакет буде правильно віднесений до однієї з існуючих асоціацій в приймальному шлюзі (чи хості). Якщо ж активної асоціації, на яку вказує мітка SPI, не існує, то пакет просто відкидається;
- порядковий номер SN (Sequence Number) — беззнакове 32-бітове число, що збільшується на одиницю після передачі кожного захищеного по протоколу AH IP— пакету. Забезпечує захист від неправдивого відтворення раніше посланих IP— пакетів. При формуванні кожного захищеного сеансу інформаційного обміну у рамках тунеля IPSec взаємодіючі сторони роблять свої лічильники нульовими, а потім погодженим чином збільшують їх. Одержувач перевіряє це поле з метою упевнитися, що пакету з таким номером прийнято ще не було. Якщо ж такий пакет вже був, він не приймається;
- аутентифікаційні дані (Authentication Data) — поле змінної довжини, що містить інформацію, що використовувану для аутентифікації пакету і називається MAC-кодом (Message Authentication Code). Це поле називають також цифровим підписом, дайджестом або кодом перевірки цілісності — ICV (Integrity Check Value) пакету. Вміст поля Authentication Data обчислюється за допомогою одного з двох обов'язково підтримуваних протоколом AH алгоритмів HMAC — MD5 і HMAC — SHA1, заснованих на застосуванні односторонніх хеш-функций з секретними ключами. Довжина дайджеста залежить від вибраного алгоритму, тому

це поле має в загальному випадку змінний розмір. Найчастіше використовуваний алгоритм HMAC — MD5 породжує 16-байтный дайджест.

Протокол АН захищає увесь IP- пакет за винятком деяких полів в IP-заголовку, таких як час життя (TTL) і тип служби (Type of Service), які можуть мінятися в процесі передачі пакету в мережі. Помітимо, що протокол АН забезпечує захист від змін IP- адрес в заголовку пакету. Протокол аутентифікації АН створює своєрідний конверт, що забезпечує аутентифікацію джерела даних, їх цілісність і захист від нав'язування повторних повідомлень.

Місце розташування заголовка АН в пакеті залежить від того, в якому режимі — транспортному або тунельному — конфігурований захищений канал. На Рис. 12.4 показано розташування АН— заголовка відносно IP— заголовка в обох режимах.

У транспортному режимі заголовок початкового IP- пакету стає зовнішнім заголовком, за ним йде заголовок АН, а потім усі дані пакету (тобто пакет протоколу верхнього рівня), що захищається.

Рис. 12.4. IP- пакет після застосування протоколу АН в транспортному і тунельному режимах

Протокол АН захищає увесь отриманий таким чином пакет, включаючи заголовок IP і власне сам заголовок АН. Таким чином, будь-яка зміна даних в пакеті або заголовків буде виявлена. Слід також помітити, що в цьому режимі дані пакету відсилаються відкритими, тобто дані пакету захищені від змін, але не захищені від перегляду. Зокрема, не вдається приховати IP- адреси джерела і призначення від можливого перегляду сторонніми особами, оскільки ці поля завжди присутні у незашифрованому вигляді і відповідають дійсним адресам хостів.

У тунельному режимі в якості заголовка зовнішнього IP-пакета створюється новий заголовок IP. IP- адреси що посилає і приймає сторін можуть відрізнятися від адрес в заголовку початкового IP- пакету. У захищеному IP- пакеті внутрішній (первинний) IP- заголовок містить цільову адресу пакету, а зовнішній IP- заголовок містить адресу кінця тунеля. За новим заголовком зовнішнього IP- пакету йде

заголовок АН, а потім увесь початковий пакет (заголовок IP і самі дані). Як і у разі транспортного режиму, протокол АН захищає увесь створений пакет (два заголовки IP, заголовок АН і дані), що також дозволяє виявити будь-які зміни в пакеті. Як і в транспортному режимі, сам пакет не захищений від перегляду.

Незалежно від режиму роботи, протокол АН надає заходи захисту від атак, спрямованих на порушення цілісності і достовірності пакетів повідомлень. За допомогою цього протоколу аутентифікується кожен пакет, що робить програми, що намагаються перехопити управління сеансом, неефективними. Протокол АН забезпечує аутентифікацію не лише вмісту, але і заголовків IP- пакетів. Проте слід мати на увазі, що аутентифікація по протоколу АН не допускає маніпулювання основними полями IP- заголовка під час проходження пакету. З цієї причини цей протокол не можна застосовувати в середовищі, де використовується механізм трансляції мережевих адрес NAT (Network Address Translation), оскільки для його роботи потрібне маніпулювання IP- заголовками.

Протокол АН може застосовуватися як окремо, так і в комбінації з протоколом ESP або навіть з пакетом, який вже містить АН- заголовок (вкладене застосування).

12.2.2. Протокол інкапсулюючого захисту ESP

Протокол інкапсулюючого захисту вмісту ESP (Encapsulating Security Payload) забезпечує конфіденційність, автентичність, цілісність і захист від повторів для пакетів даних. Слід зазначити, що конфіденційність даних протокол ESP забезпечує завжди, а цілісність і автентичність є для нього опціональними вимогами. Конфіденційність даних забезпечується шляхом шифрування вмісту окремих пакетів. Цілісність і автентичність даних забезпечуються на основі обчислення дайджеста.

З приведеного переліку функцій по захисту інформаційного обміну видно, що функціональність протоколу ESP ширша, ніж у протоколу АН. Протокол ESP підтримує усі функції протоколу АН по захисту зашифрованих потоків даних від підробки, відтворення і випадкового спотворення, а також забезпечує конфіденційність даних.

У протоколі ESP функції аутентифікації і криптографічного закриття можуть бути задіяні або разом, або окремо один від одного. При виконанні шифрування без аутентифікації з'являється можливість використання механізму трансляції мережевих адрес NAT (Network Address Translation), оскільки в цьому випадку адреси в заголовках IP- пакетів можна модифікувати [9].

Для вирішення своїх завдань протокол ESP використовує заголовок формату, приведеного на Рис. 12.5.

Рис. 12.5. Формат заголовка ESP

Заголовок ESP містить наступні поля:

- індекс параметрів захисту SPJ (Security Parameters Index) — використовується спільно з адресою одержувача і протоколом захисту (AH або ESP). Вказує відповідна угода SA. Одержувач використовує це значення для визначення угоди про захист, з якою ідентифікується цей пакет;
- порядковий номер SN (Sequence Number) — забезпечує захист від повторів для SA. Є 32-бітовим числом, спочатку рівним 1 і що збільшується з кроком 1. Воно не повторюється циклічно і вказує номер пакету, що посилається за цією угодою. Одержувач перевіряє це поле з метою упевнитися, що пакету з таким номером прийнято ще не було. Якщо ж такий пакет вже був, він не приймається;
- дані (Payload Data)
- заповнювач (Padding) — дописується від 0 до 255 байт для 32-бітового вирівнювання з розміром блоку шифру;
- довжина заповнювача (Padding Length) — вказує довжину поля заповнювача у байтах;
- наступний заголовок (Next Header) — вказує природу передаваних даних (наприклад, TCP або UDP);
- аутентифікаційні дані (Authentication Data) — містять код перевірки цілісності ICV (Integrity Check Value) і код автентичності повідомлення, використовувані для перевірки достовірності відправника і цілісності повідомлення. Значення ICV обчислюється для заголовка ESP, передаваних даних і кінцевої мітки ESP. Полі Authentication Data поміщається в заголовок ESP тільки при включеній аутентифікації.

Неважко помітити, що деякі поля заголовка ESP аналогічні полям заголовка AH: Next Header, SPI, SN, Authentication Data. Але є і два додаткові поля — заповнювач (Padding) і довжина заповнювача (Pad Length). Заповнювач може знадобитися в трьох випадках. По-перше, для нормальної роботи деяких

алгоритмів шифрування необхідно, щоб шифрований текст містив кратне число блоків певного розміру. По-друге, формат заголовка ESP вимагає, щоб поле даних закінчувалося на межі чотирьох байтів. По-третє, заповнювач можна використати для приховання дійсного розміру пакету в цілях забезпечення так званої часткової конфіденційності трафіку, хоча протокол ESP обмежує можливості маскування 255 байтами заповнювача; це зроблено для того, щоб не занадто знижувалася корисна пропускна спроможність каналу зв'язку із-за великого об'єму надмірних даних.

Як видно з Рис. 12.5, заголовок ділиться на дві частини, що розділяються полемо даних (корисне навантаження — Payload Data). Перша частина, яка далі позначатиметься як заголовок ESP, утворюється двома полями — SPI і SN — і розміщується перед полем даних. Інші службові поля протоколу ESP розташовані у кінці пакету. Безпосередньо за полем даних йде так званий трейлер, в який входять заповнювач (Padding), довжина заповнювача (Pad Length), а також покажчик на протокол наступного рівня (Next Header). Завершує пакет поле контролю цілісності (Authentication Data). У тому випадку, коли при встановленні безпечної асоціації прийнято рішення не використати можливості ESP по забезпеченню цілісності, це поле відсутнє.

ПЗ перерахованих протоколів (утиліти шифрування, цифровому підпису і ін.) може функціонувати на серверах або комп'ютерах кінцевих користувачів. Проте частіше його встановлюють на маршрутизаторах або спеціальних пристроях, які в архітектурі IPSec іменуються шлюзами безпеки (security gateway).

Протокол ESP також використовують в двох режимах — транспортному і тунельному. На Рис. 12.6 показано розташування ESP заголовка в тунельному і транспортному режимах [62].

У транспортному режимі зашифровані дані транспортуються безпосередньо між хостами. У транспортному режимі протоколу ESP заголовок початкового IP-пакету залишається зовнішнім. Заголовок ESP поміщається в передаваний пакет між заголовками протоколів третього (IP) і четвертого (наприклад, TCP) рівнів. Слід зауважити, що поля протоколу ESP слідують після стандартного IP- заголовка, а це означає, що такий пакет може маршрутизуватися в мережі за допомогою звичайного устаткування, підтримувального IP.

Рис. 12.6. IP- пакет після застосування протоколу ESP в транспортному і тунельному режимах

Шифруванню піддаються тільки дані початкового IP- пакету (пакет верхнього рівня) і завершальна частина ESP заголовка (ESP trailer). У цьому режимі ESP не шифрує заголовок IP- пакету, інакше маршрутизатор не зможе прочитати поля заголовка і коректно здійснити просування пакету між мережами. У число шифрованих полів не потрапили також поля SPI і SN, які повинні передаватися у відкритому виді, для того, щоб прибулий пакет можна було віднести до певної асоціації SA і захиститися від неправдивого відтворення пакету.

На відміну від протоколу AH, контроль цілісності і автентичності даних в протоколі ESP не поширюється на заголовок початкового пакету, і з цієї причини має сенс застосовувати обидва протоколи спільно — ESP для шифрування, а AH для контролю цілісності.

Таким чином, адресна інформація (IP- адреси що посилає і приймає сторін) видно при пересилці пакету по мережі, і несанкціонована зміна цих IP- адрес не буде помічена.

У тунельному режимі основна роль відводиться шлюзам безпеки, оскільки передбачається, що клієнтські станції (чи сервери) можуть не підтримувати IPSec і відправляють в мережу звичайний IP- трафік. Перш ніж досягти каналів глобальної мережі, кожен початковий IP- пакет спочатку потрапляє в шлюз, який поміщає цей пакет цілком в «оболонку» IPSec, зашифровувавши його вміст разом з початковим IP- заголовком. Щоб забезпечити можливість маршрутизації пакету, що вийшов, шлюз забезпечує його новим IP- заголовком і тільки після цього відправляє в мережу. Шлюз, що знаходиться на протилежному кінці з'єднання, розшифровує цей пакет і передає його на крайовий пристрій в первинному виді. Описана процедура називається тунелюванням.

З Рис. 12.6 видно, що в тунельному режимі в якості зовнішнього заголовка створюється новий заголовок IP. Увесь початковий IP- пакет (і дані і заголовок IP) і завершальна частина заголовка ESP (трейлер ESP) шифруються. Тому адресна інформація початкового IP- пакету не доступна для перегляду. Заголовок зовнішнього IP- пакету протоколом ESP не захищається.

Тунелювання дозволяє розповсюдити дію засобів захисту на мережевий рівень моделі OSI і, зокрема, приховати істинні адреси джерела і одержувача. При цьому зменшується ризик атак, заснованих на детальному аналізі трафіку.

Порівнюючи протоколи ESP і AH можна помітити, що вони дублюють функціональність один одного в області забезпечення аутентифікації даних. Головною відмінністю протоколу AH від ESP в цьому питанні являється те, що протокол AH забезпечує аутентифікацію усього пакету (і IP заголовка і самих даних), тоді як протокол ESP аутентифікує тільки дані з пакету (див. Рис. 12.6). При шифруванні в протоколі ESP використовується симетричний секретний ключ, тобто передавані дані зашифровуються і розшифровуються за допомогою одного і того ж ключа. Для протоколу ESP також визначений перелік обов'язкових алгоритмів шифрування — DES, MD5 і SHA — 1.

При аутентифікації даних протокол ESP використовує ті ж алгоритми HMAC, що і протокол AH (використовуючі MD5 або SHA - 1 в якості функції хешування). Проте способи застосування розрізняються (див. Рис. 12.6).

У транспортному режимі:

- протокол ESP аутентифікує тільки дані з пакету, не зачіпаючи IP-заголовка;

- протокол АН захищає і дані і обидва заголовки.

У тунельному режимі:

- аутентифікація в ESP протоколі застосовується до даних пакету і початкового IP- заголовка, але не зачіпає новий IP- заголовок;
- протокол АН аутентифікує дані, АН- заголовок і обоє IP- заголовка.

Протокол ESP може застосовуватися окремо або спільно з протоколом АН. При спільному використанні протоколи АН і ESP можуть комбінуватися різними способами. Якщо використовується транспортний режим, то аналогічно тому, як у рамках ESP аутентифікація йде слідом за шифруванням, протокол АН повинен застосовуватися після протоколу ESP. У тунельному режимі протоколи АН і ESP застосовуються до різних вкладених пакетів і, крім того, допускається багатократна вкладеність тунелів з різними початковими і/або кінцевими точками.

12.2.3. Алгоритми аутентифікації і шифрування в IPSec

Стек протоколів IPSec є погодженим набором відкритих стандартів, що має цілком певне ядро, і в той же час він може бути досить просто доповнений новими протоколами, алгоритмами і функціями. Завдяки модульній структурі протоколи АН і ESP допускають застосування користувачами по їх погодженому вибору різних криптографічних алгоритмів аутентифікації і шифрування. Для шифрування даних в IPSec (протокол ESP) може бути застосований практично будь-який симетричний алгоритм шифрування, що використовує секретні ключі.

Для забезпечення цілісності і аутентифікації даних (протоколи АН і ESP) використовується один з прийомів шифрування — шифрування за допомогою односторонньої функції (one — way function), що називається також хеш-функцією (hash function) або дайджест-функцією (digest function) [45, 72]. Ця функція, застосована до шифрованих даних, дає в результаті значення-дайджест, що складається з фіксованого невеликого числа байт. Дайджест передається в IP— пакеті разом з початковим повідомленням. Одержувач, знаючи, яка одностороння функція шифрування була застосована для складання дайджеста, наново обчислює його, використовуючи початкове повідомлення. Якщо значення отриманого і вичисленого дайджестів співпадають, це означає, що вміст пакету під час передачі не був підданий ніяким змінам. Знання дайджеста не дає можливості відновити початкове повідомлення і тому не може бути використане для захисту конфіденційності, але воно дозволяє перевірити цілісність даних.

Дайджест є свого роду контрольною сумою для початкового повідомлення. На відміну від традиційної контрольної суми при обчисленні дайджеста використовується секретний ключ. Якщо для отримання дайджеста застосовувалася одностороння функція з параметром (яким виступає секретний ключ), відомим тільки відправнику і одержувачеві, будь-яка модифікація початкового повідомлення буде негайно виявлена.

В цілях забезпечення сумісності продуктів різних виробників робоча група IETF визначила базовий набір підтримуваних функцій і алгоритмів, який має бути однотипно реалізований в усіх продуктах, підтримувальних IPSec. На сьогодні визначені 2 алгоритми аутентифікації і 7 алгоритмів шифрування.

Зараз для протоколів АН і ESP зареєстроване 2 алгоритми аутентифікації — HMAC — MD5 і HMAC— SHA1. Алгоритм HMAC (Keyed — Hashing for Message

Authentication Code) визначається стандартом RFC 2104. Функції MD5 (Message Digest version 5, стандарт RFC 1321) і SHA1 (Secure Hash Algorithm version 1, стандарт FIPS 180-1) є функціями хешування. Алгоритми HMAC — MD5 і HMAC — SHA1 є алгоритмами аутентифікації із загальним секретним ключем. Секретний ключ має довжину 128 біт у разі MD5 і 160 біт у разі SHA1 [9].

Якщо секретний ключ відомий тільки передавальною і приймаючою сторонам, це забезпечить аутентифікацію джерела даних, а також цілісність пакетів, що пересилаються між двома сторонами. Ключі для HMAC генеруються за допомогою процедури ISAKMP/Oakley. Для забезпечення сумісності устаткування і ПЗ на початковій стадії реалізації протоколу

IPSec один із зареєстрованих алгоритмів аутентифікації прийнято використати за умовчанням. В якості такого алгоритму визначений алгоритм HMAC - MD5.

Структура алгоритму HMAC показана на Рис. 12.7. Принцип дії алгоритму HMAC полягає в двократній обробці пакету функцією хешування, керованої ключем аутентифікації (наприклад, функцією хешування MD5). Як видно з малюнка, обидва рази в оброблювані дані включається секретний ключ, який забезпечує аутентифікацію передаваної інформації. Отримана контрольна сума поміщається в заголовок АН протоколу. Перевірка аутентифікації на іншій стороні здійснюється шляхом повторного обчислення контрольної суми для пакету, що прийшов, з використанням такого ж ключа і порівняння отриманого результату з присланим.

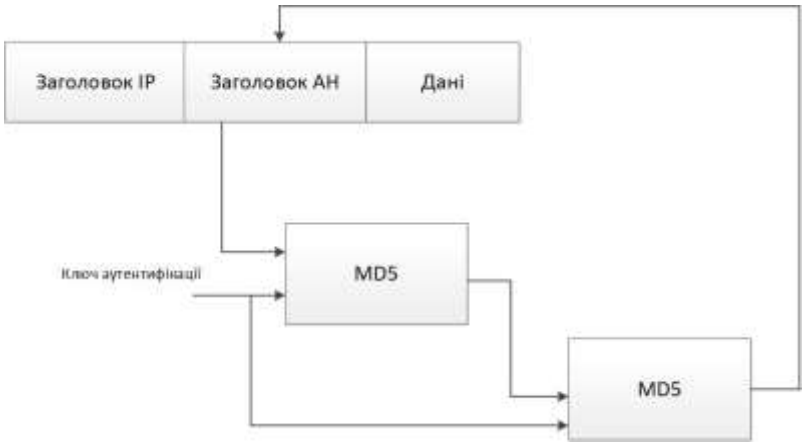

Рис. 12.7. Структура HMAC алгоритму

Алгоритм HMAC реалізує симетричну схему аутентифікації, використовуючи параметр перевірки цілісності пакету ICV (Integrity Check Value). По суті, він є цифровим підписом, що поміщається в поле аутентифікації і дозволяє відправнику підписати результат попереднього хешування змістовної частини пакету ESP.

Аналіз утримуваного цього поля дає можливість одержувачеві ідентифікувати джерело даних і переконатися в тому, що вони не були змінені в процесі передачі. Якщо для протоколу ESP функції аутентифікації є факультативними, то для протоколу АН процес аутентифікації обов'язковий.

Для протоколу ESP зареєстровані декілька алгоритмів шифрування. Найчастіше в якості алгоритмів шифрування для ESP застосовуються DES (Data

Encryption Standard), 3DES (потрійний DES) і новий стандарт шифрування AES (Advanced Encryption Standard). Для забезпечення ГРБес-сумісності за умовчанням в якості алгоритму шифрування стандартом передбачений симетричний метод DES - CBC (Cipher Block Chaining) з явно заданим вектором ініціалізації IV і з 56-розрядним ключем. Алгоритм AES всюди вбудовується в стандарт IPSec як альтернатива DES і 3DES.

Вибір алгоритму шифрування цілком залежить від розробника. Можливість вибору алгоритму шифрування надає користувачеві додаткову перевагу: зловмисник повинен не лише розкрити шифр, але і визначити, який саме шифр йому потрібно розкривати, а разом з необхідністю підбору ключів, це ще більше зменшує його шанси своєчасно розшифрувати дані користувача.

IPSec може працювати спільно з протоколами L2TP або L2F, які виконують тільки тунелювання, але не забезпечують шифрування і аутентифікацію даних. Ці протоколи створюють через Internet тунель для пакетів будь-яких протоколів, упаковувавши їх в пакети IP. Коли трафік за допомогою L2F або L2TP виявляється упакованим в пакети IP, то далі для його захисту можна використати IPSec. В результаті комбінування IPSec з протоколами тунелювання типу L2F/L2TP дозволяє вирішити завдання захисту даних для протоколів, відмінних від IP.

Алгоритмічна незалежність протоколів AH і ESP вимагає попереднього узгодження взаємодіючими сторонами набору вживаних алгоритмів і їх параметрів.

12.3. Протокол управління криптоключами IKE

Протоколи ESP і AH дозволяють реалізувати найважливіші атрибути захищеної передачі — конфіденційність зв'язку, аутентифікацію сторін і цілісність даних. Проте їх функції втрачають всяку цінність у відсутність потужної підтримувальної інфраструктури, яка забезпечувала б розподіл ключів і узгодження протоколів між учасниками обміну.

Роль такої інфраструктури в IPSec виконує група протоколів IKE (Internet Key Exchange). Ця назва прийшла в 1998 р. на зміну більше ранньому — ISAKMP/Oakley, яке безпосередньо вказувало на походження засобів управління ключами у складі IPSec.

Протокол ISAKMP (Internet Security Association and Key Management Protocol), описаний в документі RFC 2408, дозволяє погоджувати алгоритми і математичні структури (так звані мультиплікативні групи, визначені на кінцевому полі) для процедури обміну ключами Діффі-Хеллмана, а також процесів аутентифікації [98, 102]. Протокол Oakley, описаний в RFC 2412, заснований на алгоритмі Діффі-Хеллмана і служить для організації безпосереднього обміну ключами.

Протоколи IKE вирішують три задачі:

- здійснюють аутентифікацію взаємодіючих сторін, погоджують алгоритми шифрування і характеристики ключів, які використовуватимуться в захищеному сеансі обміну інформацією;
- забезпечують створення, управління ключової інформації з'єднання, безпосередній обмін ключами (у тому числі можливість їх частої зміни);

• управляють параметрами з'єднання і захистом від деяких типів атак, контролюють виконання усіх досягнутих угод.

Розробники IPSec розпочали свою діяльність з рішення останньою з перерахованих завдань. В результаті на світ з'явилася концепція захищених віртуальних з'єднань або безпечних асоціацій SA (Security Associations).

12.3.1. Встановлення безпечної асоціації SA

Основою функціонування IPSec є захищені віртуальні з'єднання або безпечні асоціації SA (Security Associations). Для того, щоб протоколи AH і ESP могли виконувати свою роботу по захисту передаваних даних, між двома кінцевими точками має бути сформована асоціація SA — угода про захист обміну даними між двома взаємодіючими партнерами.

Встановлення SA повинне розпочинатися зі взаємної аутентифікації сторін, тому що заходи безпеки втрачають всякий сенс, якщо дані передаються або приймаються неавторизованими користувачами. Процедури встановлення SA виправдані лише у тому випадку, якщо у кожної із сторін є повна упевненість в тому, що її партнер — саме той, за кого він себе видає.

Для виконання аутентифікації сторін в IKE застосовуються два основні способи.

Перший спосіб заснований на використанні секрету, що розділяється. Перед ініціалізацією IPSec - пристроїв, що утворюють безпечні асоціації, в їх БД поміщається заздалегідь розподілений секрет, що розділяється. Цифровий підпис на основі односторонньої функції, наприклад, MD5, що використовує як аргумент цей заздалегідь розподілений секрет, доводить автентичність протилежної сторони.

Другий спосіб заснований на використанні технології цифрового підпису і цифрових сертифікатів стандарту X. 509. Кожна із сторін підписує свій цифровий сертифікат своїм закритим ключем і передає ці дані протилежній стороні. Якщо підписаний сертифікат розшифровується відкритим ключем відправника, то це засвідчує той факт, що відправник, що надав дані, дійсно має частину у відповідь цього відкритого ключа — відповідний закритий ключ.

Проте слід зазначити, що для посвідчення автентичності сторони треба ще переконатися в автентичності самого сертифікату, і для цього сертифікат має бути підписаний не лише його власником, але і деякою третьою стороною, що видала сертифікат і викликала довіру. У архітектурі IPSec ця третя сторона іменується органом сертифікації CA (Certification Authority). Цей орган покликаний засвідчити достовірність обох сторін і повинен користуватися повною довірою сторін, а її відкритий ключ — відомий усім вузлам, що використовують його сертифікати для засвідчення осіб один одного.

Після проведення взаємної аутентифікації взаємодіючі сторони можуть безпосередньо перейти до узгодження параметрів захищеного каналу. Вибирані параметри SA визначають: протокол, використовуваний для забезпечення безпеки передачі даних; алгоритм аутентифікації протоколу AH і його ключі; алгоритм шифрування, використовуваний протоколом ESP, і його ключі; наявність або відсутність криптографічної синхронізації; способи захисту сеансу обміну; частоту зміни ключів і ряд інших параметрів. Важливим параметром SA є так званий криптографічний матеріал, тобто секретні ключі, використовувані в роботі

протоколів AH і ESP. Сервіси безпеки, пропоновані IPSec, використовують для формування криптографічних ключів секрети, що розділяються.

Параметри SA повинні влаштовувати обидві кінцеві точки захищеного каналу. Тому при використанні автоматичної процедури встановлення SA протоколи IKE, працюючі по різні сторони каналу, вибирають параметри в ході переговорного процесу. Для кожного завдання, що вирішується протоколами AH і ESP, пропонується декілька схем аутентифікації і шифрування — це робить IPSec дуже гнучким засобом. Безпечна асоціація SA є в IPSec однонапрямленим логічним з'єднанням, тому при двосторонньому обміні даними необхідно встановити дві асоціації SA. У рамках однієї асоціації SA може працювати тільки один з протоколів захисту даних — або AH, або ESP, але не обоє разом.

Для ідентифікації кожної SA призначений індекс параметрів безпеки SPI (Security Parameters Index). Цей індекс включається в заголовки захищених IPSec-пакетів, щоб приймаюча сторона змогла правильно їх розшифрувати і аутентифікувати, скориставшись вказаною безпечною асоціацією.

Система IPSec допускає застосування ручного і автоматичного способу встановлення SA. При ручному способі адміністратор конфігурує кожен кінцевий вузол так, щоб вони підтримували погоджені параметри асоціації, включаючи і секретні ключі.

Для автоматичного встановлення асоціації потрібний відповідний протокол, в якості якого в стандартах IPSec визначений протокол IKE. Він є комбінацією протоколів ISAKMP, Oakley і SKEME. Протокол узгодження параметрів віртуального каналу і управління ключами ISAKMP (Internet Security Association Key Management Protocol) описує базову технологію аутентифікації, обміну ключами і узгодження інших параметрів IPSec- тунеля при створенні SA, проте самі протоколи аутентифікації сторін і обміну ключами в нім детально не визначені. Тому при розробці протоколу IKE загальні правила і процедури протоколу ISAKMP доповнені процедурами аутентифікації і обміну ключами, узятими з протоколів Oakley і SKEME. Оскільки протокол IKE використовує для управління асоціаціями алгоритми і формати протоколу ISAKMP, назви цих протоколів іноді використовують як синоніми.

На підставі протоколу ISAKMP узгодження параметрів захищеної взаємодії потрібне як при формуванні IPSec- тунеля, так і при формуванні в його рамках кожного захищеного однонапрямленого з'єднання. Параметри IPSec- тунеля узгоджуються по протоколу ISAKMP/Oakley. Параметри кожного захищеного однонапрямленого з'єднання узгоджуються у рамках сформованого IPSec- тунеля і утворюють SA.

Криптографічні ключі для кожного захищеного одного-спрямованого з'єднання генеруються на основі ключів, вироблених у рамках IPSec- тунеля. При цьому враховуються алгоритми аутентифікації і шифрування, використовувані в протоколах аутентифікуючого заголовка (AH) і інкапсулюючого захисту (ESP).

Стандарти IPSec дозволяють шлюзам використати як одну асоціацію SA для передачі трафіку що усіх, що взаємодіють через Internet хостів, так і створювати для цієї мети довільне число асоціацій SA, наприклад по одній на кожне з'єднання TCP.

12.3.2. Бази даних SAD і SPD

IPSec пропонує різні методи захисту трафіку.

У кожному вузлі, підтримувальному IPSec, використовуються БД двох типів:

- база цих безпечних асоціацій SAD (Security Associations Database);
- база даних політики безпеки SPD (Security Policy Database).

При встановленні SA дві вступаючі в обмін сторони приймають ряд угод, що регламентують процес передачі потоку даних між ними. Угоди представляються у вигляді набору параметрів. Для SA такими параметрами є, зокрема, тип і режим роботи протоколу захисту (AH або ESP), методи шифрування, секретні ключі, значення поточного номера пакету в асоціації і інша інформація.

Об'єднання службової інформації у рамках SA надає користувачеві можливість сформувати різні класи захисту, призначені, наприклад, для електронного спілкування з різними «співрозмовниками». Іншими словами, застосування структур SA відкриває шлях до побудови безлічі віртуальних приватних мереж, що розрізняються своїми параметрами.

Набори поточних параметрів, що визначають усі активні асоціації, зберігаються на обох крайніх вузлах захищеного каналу у вигляді SAD. Кожен вузол IPSec підтримує дві бази SAD — одну для вихідних, іншу — для вхідних асоціацій.

SPD задає відповідність між IP- пакетами і встановленими для них правилами обробки. При обробці пакетів БД SPD використовуються спільно з БД SAD. SPD є впорядкованим набором правив, кожне з яких включає сукупність селекторів і допустимих політик безпеки. Селектори служать для відбору пакетів, а політики безпеки задають необхідну обробку. Така БД формується і підтримується на кожному вузлі, де встановлене ПЗ IPSec.

12.4. Особливості реалізації засобів IPSec

Вище було розглянуто, що протоколи AH або ESP можуть захищати передавані дані в двох режимах: тунельному, при якому IP- пакети захищаються цілком, включаючи їх заголовки, і транспортному, що забезпечує захист тільки утримуваного IP- пакетів.

Основним режимом є тунельний. У тунельному режимі початковий пакет поміщається в новий IP- пакет і передача даних по мережі виконується на підставі заголовка нового IP- пакету. При роботі в цьому режимі кожен звичайний 1P-пакет поміщається цілком в криптозахищеному виді в конверт IPSec, а той у свою чергу інкапсулюється в інший захищений IP- пакет. Тунельний режим зазвичай реалізують на спеціально виділених шлюзах безпеки, в ролі яких можуть виступати маршрутизатори або МЭ. Між такими шлюзами і формуються захищені тунелі IPSec.

Після прийому на іншій стороні тунеля захищені IP- пакети «розпаковуються» і отримані початкові IP- пакети передаються комп'ютерам приймальної локальної мережі за стандартними правилами. Тунелювання IP-пакетів повністю прозоро для звичайних комп'ютерів в локальних мережах, що є утримувачами тунелів. На крайових системах тунельний режим може використовуватися для підтримки видалених і мобільних користувачів. В цьому

випадку на комп'ютерах цих користувачів повинно бути встановлено ПЗ, що реалізовує тунельний режим IPSec.

У транспортному режимі передача IP- пакету через мережу виконується за допомогою початкового заголовка цього пакету. У конверт IPSec в криптозахищеному виді поміщається тільки утримуване початкового IP- пакету і до отриманого конверта додається початковий IP- заголовок. Транспортний режим швидше тунельного і розроблений для застосування на крайових системах. Цей режим може використовуватися для підтримки видалених і мобільних користувачів, а також захисту інформаційних потоків усередині локальних мереж. Слід зазначити, що робота в транспортному режимі відбивається на тих, що усіх, що входять до групи захищеної взаємодії системах, і у більшості випадків потрібно перепрограмування мережевих застосувань.

12.4.1. Основні схеми застосування IPSec

Застосування тунельного або транспортного режиму залежить від вимог, що пред'являються до захисту даних, а також від ролі вузла, в якому працює IPSec. Вузлом, що завершує захищений канал, може бути хост (кінцевий вузол) або шлюз (проміжний вузол) [48]. Відповідно розрізняють три основні схеми застосування IPSec:

1) хост-хост;
2) шлюз-шлюз;
3) хост-шлюз.

У схемі 1 захищений канал, або, що у даному контексті одне і те ж, SA, встановлюється між двома кінцевими вузлами мережі, тобто хостами H1 і H2 (Рис. 12.8). Протокол IPSec в цьому випадку працює на кінцевому вузлі і захищає дані, що поступають на нього. Для хостів, підтримувальних IPSec, дозволяється використати як транспортний режим, так і тунельний.

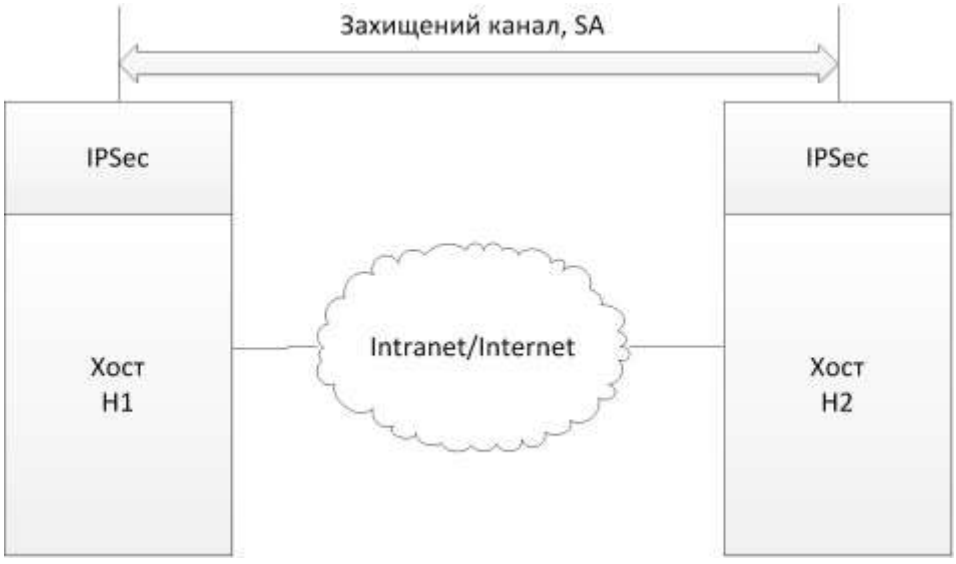

Рис. 12.8 Схема хост-хост

Відповідно до схеми 2 захищений канал встановлюється між двома проміжними вузлами, що називаються шлюзами безпеки SG1 і SG2 (Security Gateway), на кожному з яких працює протокол IPSec (Рис. 12.9).

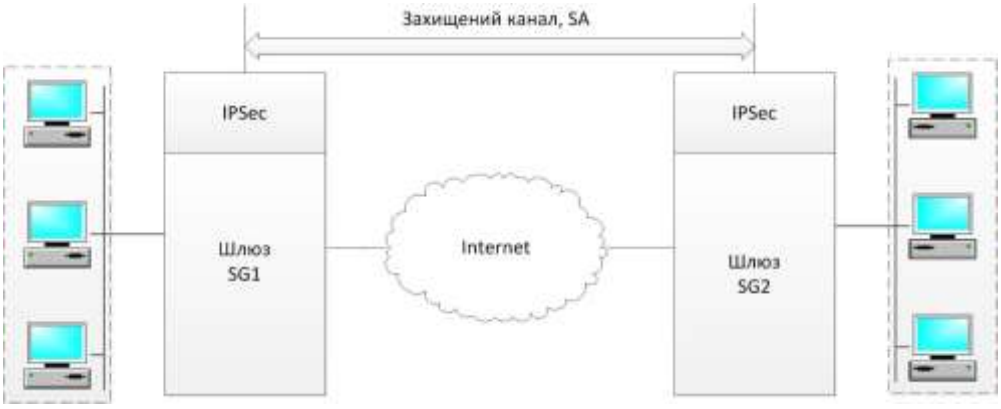

Рис. 12.9. Схема шлюз-шлюз

Захищений обмін даними може відбуватися між будь-якими двома кінцевими вузлами, підключеними до мереж, які розташовані позаду шлюзів безпеки. Від кінцевих вузлів підтримку протоколу IPSec не потрібно, вони передають свій трафік в незахищеному виді через заслуговуючі довіру мережі Intranet підприємства. Трафік, що направляється в загальнодоступну мережу, проходить через шлюз безпеки, який і забезпечує його захист за допомогою IPSec, діючи від свого імені. Шлюзам дозволяється використати тільки тунельний режим роботи, хоча вони могли б підтримувати і транспортний режим, але він в цьому випадку малоефективний.

При захищеному видаленому доступі часто застосовується схема 3 хост-шлюз (Рис. 12.10).

Тут захищений канал організовується між видаленим хостом H1, на якому працює IPSec, і шлюзом SG, що захищає трафік для усіх хостів, що входять в мережу Intranet підприємства. Видалений хост може використати при відправці пакетів шлюзу як транспортний, так і тунельний режим, шлюз же відправляє пакети хосту тільки в тунельному режимі.

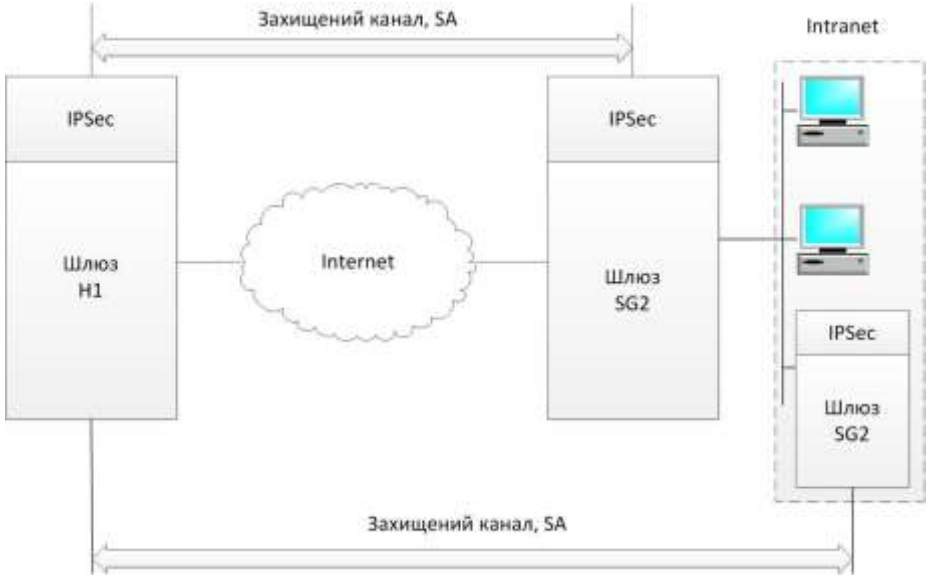

Рис. 12.10. Схема хост-шлюз, доповнена каналом хост-хост

Цю схему можна модифікувати, створивши паралельно ще один захищений канал — між видаленим хостом H1 і яким-небудь хостом H2, що належить

внутрішній мережі, що захищається шлюзом. Таке комбіноване використання двох SA дозволяє надійно захистити трафік і у внутрішній мережі.

Розглянуті схеми побудови захищених каналів на базі IPSec широко застосовуються при створенні різноманітних віртуальних захищених мереж VPN. Їх спектр варіюється від провайдерських мереж, що дозволяють управляти обслуговуванням клієнтів безпосередньо на їх площах, до корпоративних мереж VPN, що розгортаються і керованих самими компаніями. На базі IPSec успішно реалізуються віртуальні захищені мережі будь-якої архітектури, включаючи VPN з видаленим доступом (Remote Access VPN), внутрішньокорпоративні VPN (Intranet VPN) і міжкорпоративні VPN (Extranet VPN).

12.4.2. Переваги засобів безпеки IPSec

Система стандартів IPSec увібрала в себе прогресивні методики і досягнення в області мережевої безпеки, завоювала визнання фахівців як надійна і легко інтегрована система безпеки для IP- мереж. Система IPSec міцно займає сьогодні лідируючі позиції в наборі стандартів для створення VPN. Цьому сприяє її відкрита побудова, здатна включати усі нові досягнення в області криптографії. IPsec дозволяє захистити мережу від більшості мережевих атак, «скидаючи» чужі пакети ще до того, як вони досягнуть рівня IP на приймаючому комп'ютері. У комп'ютер, що захищається, або мережу можуть увійти тільки пакети від зареєстрованих партнерів по взаємодії.

IPsec забезпечує:

- аутентифікацію — доказ відправки пакетів вашим партнером по взаємодії, тобто володарем секрету, що розділяється;
- цілісність — неможливість зміни даних в пакеті;
- конфіденційність — неможливість розкриття передаваних даних;
- надійне управління ключами — протокол IKE обчислює секрет, що розділяється, відомий тільки одержувачеві і відправнику пакету;
- тунелювання — повне маскування топології локальної мережі підприємства.

Робота у рамках стандартів IPSec забезпечує повний захист інформаційного потоку даних від відправника до одержувача, закриваючи трафік для спостерігачів на проміжних вузлах мережі. VPN- рішення на основі стека протоколів IPSec забезпечують побудову віртуальних захищених мереж, їх безпечну експлуатацію і інтеграцію з відкритими комунікаційними системами.

Лекція 13 ІНФРАСТРУКТУРА ЗАХИСТУ НА ПРИКЛАДНОМУ РІВНІ

Розвиток IT дозволяє підвищити ефективність діяльності компаній, а також відкриває нові можливості для взаємодії з потенційними клієнтами на базі загальнодоступних мереж, у тому числі Інтернету. Створення Web— сайту — своєрідного представництва підприємства в Інтернеті — є лише першим кроком на цьому шляху. Активне ведення комерційних операцій в Мережі припускає масовий доступ споживачів електронних послуг (чи Web— клієнтів) до Internet— застосуванням і проведення електронних транзакцій мільйонами користувачів Мережі. Розміщення Internet— застосувань усередині корпоративної мережі може завдати збитку безпеки IT-інфраструктури, оскільки відкриття доступу через МЕ неминуче створює потенційну можливість для несанкціонованого проникнення зловмисників в мережу підприємства.

Забезпечення інформаційної безпеки повинне включати рішення таких завдань, як безпечний доступ до Web - серверів і Web- застосувань, аутентифікація і авторизація користувачів, забезпечення цілісності і конфіденційності даних, реалізація електронного цифрового підпису та ін.

Організації потребують надійних, гнучких і безпечних методів і засобів для отримання і використання відкритої і конфіденційної інформації численними групами людей — своїми співробітниками, партнерами, клієнтами і постачальниками. Проблема полягає в забезпеченні доступу до такої інформації тільки авторизованим користувачам. Доцільно використати інтегровану систему управління доступом користувачів до чутливої інформації в широкому діапазоні точок доступу і застосувань. Така система вирішує багато проблем контролю доступу, з якими стикаються організації, забезпечуючи при цьому зручний доступ і високу безпеку.

13.1. Управління ідентифікацією і доступом

Для реалізації зростаючих потреб електронного бізнесу необхідно побудувати надійне з точки зору безпеки середовище для здійснення електронного бізнесу в режимі online. Технології, які дають можливість здійснювати електронний бізнес, виконують чотири основні функції:

- аутентифікацію, або перевірку достовірності користувача;
- управління доступом, що дозволяє авторизованим користувачам діставати доступ до необхідних ресурсів;
- шифрування, що гарантує, що зв'язок між користувачем і базовою інфраструктурою захищений;
- невідмовність, що означає, що користувачі не можуть пізніше відмовитися від виконаної транзакції (Рис. 13.1).

Рис. 13.1. Технології, що забезпечують електронний бізнес

Тільки рішення, яке виконує усі ці чотири функції, може створити довірене середовище, здібну насправді забезпечити реалізацію електронного бізнесу.

Управління доступом є критичним компонентом загальної системи безпеки. Система управління доступом забезпечує авторизованим користувачам доступ до належних ресурсів. Проектування цієї інфраструктури вимагає тонкого балансу між наданням доступу до критичних ресурсів тільки авторизованим користувачам і забезпеченням необхідної безпеки цих ресурсів, відомих великому числу користувачів.

13.1.1. Особливості управління доступом

У розподіленій корпоративній мережі зазвичай застосовуються два методи управління доступом:

- управління мережевим доступом (регулює доступ до ресурсів внутрішньої мережі організації);
- управління Web- доступом (регулює доступ до Web - серверам і їх вмісту).

Усі запити на доступ до ресурсів проходять через один або більше за списки контролю доступу ACL (Access Control List). ACL є набором правил доступу, які задають для набору ресурсів, що захищаються. Ресурси з низьким ризиком матимуть менш суворі правила доступу, тоді як висококритичні ресурси повинні мати суворіші правила доступу. ACL, по суті, визначають політику безпеки.

Доступ до мережевих ресурсів організації можна регулювати шляхом створення списків контролю доступу Login ACL, які дозволяють точно визначити конкретні дозволи і умови для дістування доступу до ресурсів внутрішньої мережі.

Засоби контролю і управління Web- доступом дозволяють створювати і виконувати політики Web- доступу. Створюючи конкретні списки контролю Web доступу Web ACL, адміністратори безпеки визначають, які користувачі можуть отримати доступ до Web- серверам організації і їх вмісту і за яких заздалегідь встановлених умов.

Управління доступом спрощується при застосуванні єдиної централізованої інфраструктури контролю і управління доступом, яка може дозволити користувачам «самообслуговування», доручаючи їм такі завдання управління, як реєстрація, редагування профілю, відновлення пароля і управління підпискою. Вона може також забезпечити делегування адміністрування, передачу функцій управління користувачами, людям, найбільш обізнаним про конкретну групу користувачів як усередині, — у бізнес-підрозділах організації, так і поза нею — у клієнтів і в підрозділах бізнес-партнерів. Щоб полегшити підтримку системи безпеки масштабу підприємства, засоби управління доступом можуть отримувати дані користувачів і політик, даних, що вже зберігаються в таких існуючих сховищах, як каталоги LDAP і реляційні БД.

13.1.2. Функціонування системи управління доступом

Централізовані системи управління доступом випускаються рядом компаній, зокрема Secure Computing, RSA Security Inc., Baltimore та ін.

Розглянемо функціонування системи управління доступом на прикладі системи PremierAccess компанії Secure Computing. Ця система здійснює управління Web і мережевим доступом усіх користувачів, включаючи внутрішніх користувачів, віддалених співробітників, клієнтів, постачальників і бізнес-партнерів. Вона базується на політиці безпеки, яка дозволяє персоналізувати права доступу користувачів. Користувачі дістають доступ тільки до тих ресурсів, на які було дано дозвіл відповідно до їх прав доступу, через Web— доступ, VPN— доступ або віддалений доступ з використанням серверів RADIUS. У системі реалізовані засновані на застосуванні процесів аутентифікації, авторизації і адміністрування дій користувачів. Система підтримує різні типи аутентифікаторів — від багаторазових паролів до біометричних засобів аутентифікації. Перевага віддається методам і засобам строгої аутентифікації.

Засоби управління користувачами дозволяють управляти великим числом користувачів. Сервер реєстрації дає можливість самим користувачам реєструватися в мережі, використовуючи стандартні Web- браузери. В процесі реєстрації користувачам призначаються ролі. Ролі є ярликами, що ідентифікують групи користувачів, які розділяють однакові права доступу. Інакше кажучи, ролі визначають набори правил доступу, застосовувані до конкретних груп користувачів. Категорування користувачів по ролях можна виконати на основі їх функціональних обов'язків.

Засоби управління мережевим доступом

У системі управління доступом використовуються так звані агенти. Агент системи — це програмний модуль, інстальований на відповідний сервер у рамках корпоративної мережі (Рис. 13.2).

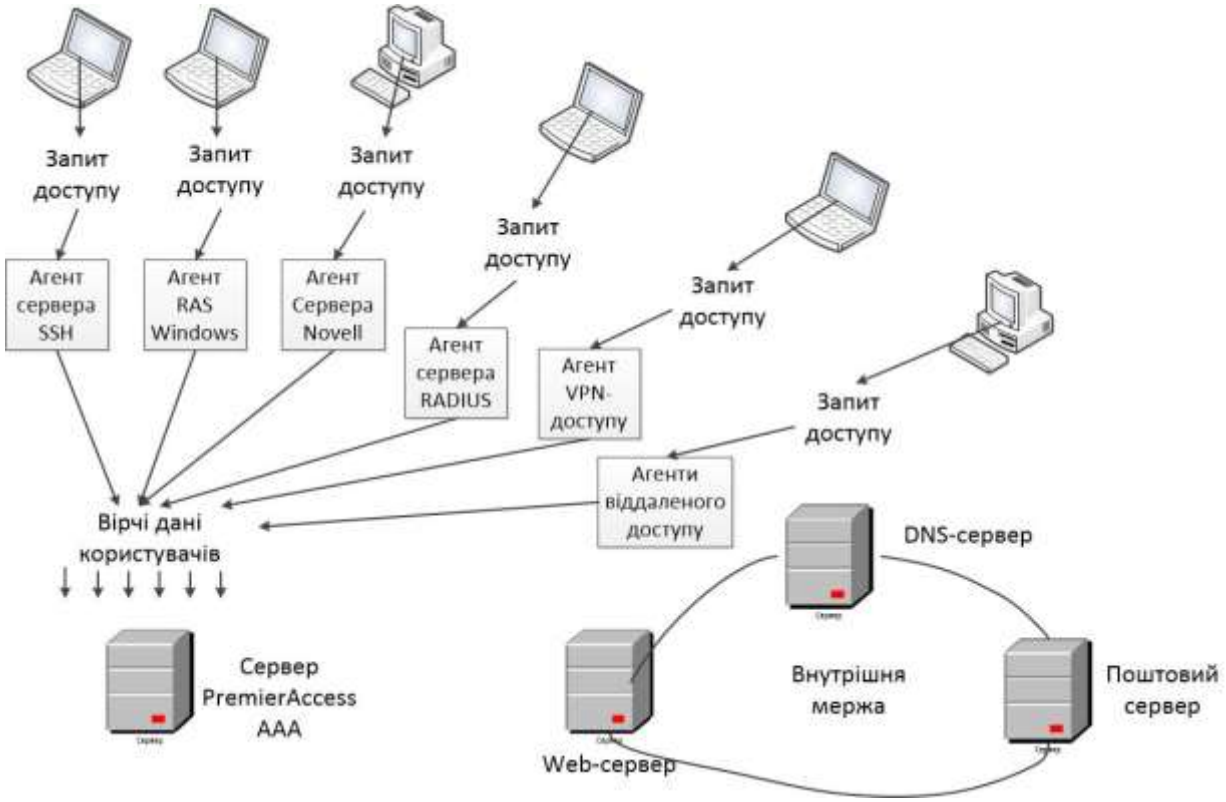

Рис. 13.2. Схема управління доступом до мережі

Такими агентами виступають агенти віддаленого доступу, агенти VPN-доступу, агенти серверів RADIUS, Novel RAS, Citrix та ін. При спробі користувача підключитися до внутрішньої мережі, агенти системи перехоплюють запит користувача на вхід в мережу.

Агенти діють як точки аутентифікації користувачів UAPs (User Authentication Points) на лініях комунікації з сервером PremierAccess. У відповідь на запит користувача агент просить у користувача його вірчі дані — ідентифікатор користувача і аутентификатор. Відповідаючи на запит агента, користувач вводить свої дані. Ці вірчі дані передаються AAA— серверу (AAA — Authentication, Authorization, Accounting).

AAA- сервер порівнює ідентифікатор ID користувача або сертифікат з даними, що зберігаються в каталозі LDAP, з метою перевірки їх тотожності. Якщо ідентифікатор ID користувача співпадає з тим, що зберігається, запис користувача у БД перевіряється по ролі (чи ролям) і ресурсам, до яких вони авторизуються. Для аутентифікації можуть застосовуватися фіксований пароль, апаратний або програмний аутентифікатори. Якщо користувач успішно проходить усі кроки підтвердження своєї достовірності, він дістає доступ до ресурсу мережі.

Засоби управління Web- доступом

Система PremierAccess використовує універсальний Web- агент UWA (Universal Web Agent), який инсталируется на хост-машині кожного Web- сервера, що захищається. У даному прикладі користувачем виступає бізнес-партнер, який просить доступ до Web, що захищається, - ресурсу компанії (Рис. 13.3).

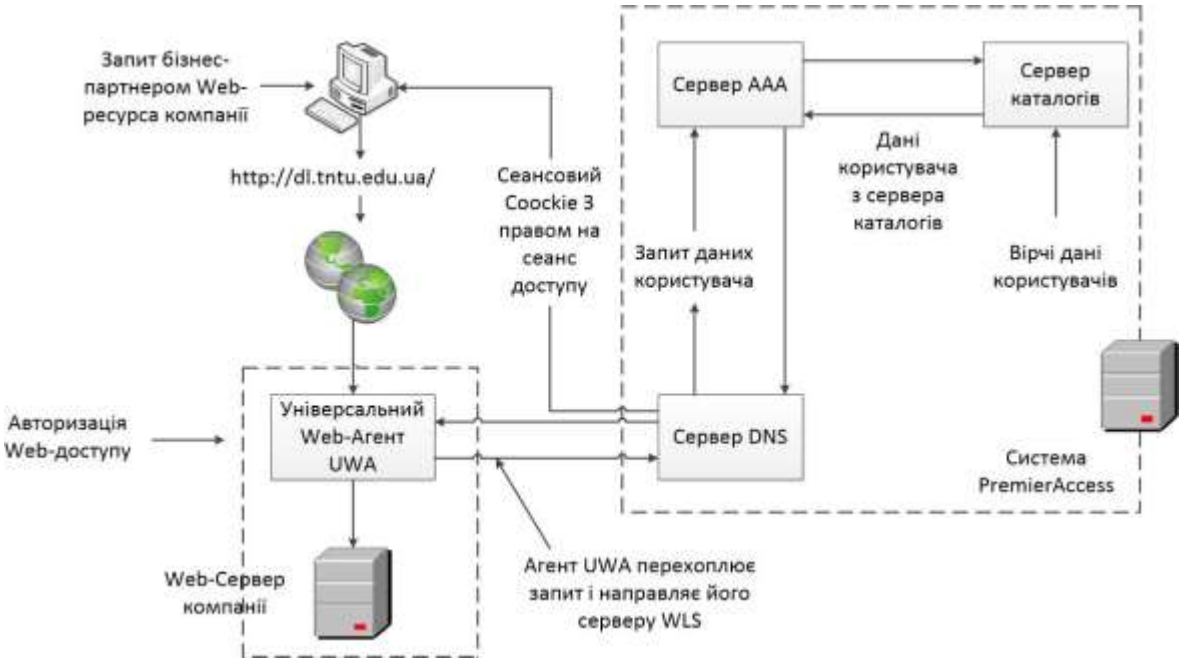

Рис. 13.3. Схема управління Web- доступом

Управління Web- доступом реалізується у вигляді процесу, що складається з двох етапів.

1. Користувач намагається увійти до системи, використовуючи сервер WLS (Web Login Server). Запит користувача на доступ до захищеному Web - ресурсу компанії перехоплюється агентом UWA, який для обробки цього запиту звертається до сервера WLS. Сервер WLS просить результат аутентифікації у

сервера AAA. У разі успішної аутентифікації сервер WLS генерує сеансовий cookie, який містить сеансовий ідентифікатор користувача.

2. Користувач намагається отримати доступ до Web - ресурсу. Сервер WLS використовує сеансовий ідентифікатор в cookie для запиту у AAA- сервера даних сеансу користувача. Щоб виконати запит на доступ, сервер WLS передає користувачеві сеансовий cookie з правами на сеанс. Агент UWA отримує сеансовий ID, потім отримує від AAA- сервера дані сеансу. Грунтуючись на ролях користувача і політиці доступу, він приймає рішення, давати або заборонити користувачеві доступ до Web - ресурсу.

При побудові систем управління доступом важливе значення мають:

- засоби і протоколи аутентифікації віддалених користувачів;
- засоби управління доступом за схемою одноразового входу з авторизацією Single Sign - On;
- інфраструктури управління відкритими ключами PKI.

Перераховані засоби і системи розглядаються в подальших розділах цієї глави.

13.2. Організація захищеного віддаленого доступу

Віддалений доступ до комп'ютерних ресурсів став нині таким же актуальним і значимим, як і доступ в режимі безпосереднього підключення. Віддалений доступ до корпоративної мережі здійснюється з незахищеного зовнішнього оточення через відкриті мережі. Тому засоби побудови захищеної корпоративної мережі повинні забезпечити безпеку мережевої взаємодії при підключенні до мережі віддалених комп'ютерів.

Віддалений доступ до корпоративної мережі можливий через глобальну комп'ютерну мережу або через середовище передачі інформації, утворене ланцюжком з телефонної і глобальної комп'ютерної мереж. Доступ через глобальну мережу Internet являється досить ефективним способом, причому для підключення віддаленого користувача до Internet може використовуватися канал телефонного зв'язку. Основні достоїнства віддаленого доступу до корпоративної мережі через Internet:

- забезпечення масштабованої підтримки віддаленого доступу, що дозволяє мобільним користувачам зв'язуватися з Internet- провайдером і потім через Internet входити у свою корпоративну мережу;
- скорочення витрат на інформаційний обмін через відкрите зовнішнє середовище (віддалені користувачі, підключившись до Internet, зв'язуються з мережею своєї організації з мінімальними витратами);
- управління трафіком віддаленого доступу здійснюється так само, як будь-яким іншим трафіком Internet.

У корпоративній мережі для взаємодії з віддаленими користувачами виділяється сервер віддаленого доступу, який служить:

- для установки з'єднання з видаленим комп'ютером;
- аутентифікації віддаленого користувача;
- управління видаленим з'єднанням;
- посередництва при обміні даними між видаленим комп'ютером і корпоративною мережею.

Серед протоколів віддаленого доступу до локальної мережі найбільше поширення отримав протокол «точка-точка» PPP (Point — to — Point Protocol), який є відкритим стандартом Internet. Протокол PPP призначений для встановлення віддаленого з'єднання і обміну інформацією по встановленому каналу пакетами мережевого рівня, інкапсульованими в PPP-кадри. Використовуваний в протоколі PPP метод формування кадрів забезпечує одночасну роботу через канал віддаленого зв'язку декількох протоколів мережевого рівня.

Протокол PPP підтримує наступні важливі функції:

- аутентифікації віддаленого користувача і сервера віддаленого доступу;
- компресії і шифрування передаваних даних;
- виявлення і корекції помилок;
- конфігурації і перевірки якості каналу зв'язку;
- динамічного привласнення адрес IP і управління цими адресами.

На основі протоколу PPP побудовані часто використовувані при видаленому доступі протоколи PPTP, L2F і L2TP. Ці протоколи дозволяють створювати захищені канали для обміну даними між віддаленими комп'ютерами і локальними мережами, що функціонують по різних протоколах мережевого рівня, — IP, IPX або NetBEUI. Для передачі по телефонних каналах зв'язку пакети цих протоколів інкапсулюються в PPP-кадри. При необхідності передачі через Internet захищені PPP-кадри інкапсулюються в IP— пакети мережі Internet. Криптозахист трафіку можливий як в каналах Internet, так і упродовж усього шляху між комп'ютером віддаленого користувача і сервером віддаленого доступу локальної мережі.

13.2.1. Протоколи аутентифікації віддалених користувачів

Контроль доступу користувачів до ресурсів корпоративної мережі повинен здійснюватися відповідно до політики безпеки організації, якій належить ця мережа. Ефективне розмежування доступу до мережевих ресурсів може бути забезпечене тільки при надійній аутентифікації користувачів. Вимоги до надійності аутентифікації віддалених користувачів мають бути особливо високими, оскільки при взаємодії з фізично віддаленими користувачами значно складніше забезпечити доступ до мережевих ресурсів. На відміну від локальних користувачів віддалені користувачі не проходять процедуру фізичного контролю при допуску на територію організації.

При віддаленій взаємодії важлива аутентифікація не лише користувачів, але і устаткування, оскільки підміни користувача або маршрутизатора призводить до одних і тих же наслідків — дані з корпоративної мережі передаються не тим особам, яким вони призначені.

Для забезпечення надійної аутентифікації віддалених користувачів потрібне виконання наступних вимог:

- проведення аутентифікації обох взаємодіючих сторін — як віддаленого користувача, так і сервера віддаленого доступу — для виключення маскування зловмисників;
- оперативне узгодження використовуваних протоколів аутентифікації;
- здійснення динамічної аутентифікації взаємодіючих сторін в процесі роботи віддаленого з'єднання;

- застосування криптозахисту передаваних секретних паролів або механізму одноразових паролів для виключення перехоплення і несанкціонованого використання аутентифицирующей інформації.

Протокол PPP має вбудовані засоби, які можуть бути використані для організації аутентифікації при віддаленій взаємодії. У стандарті RFC 1334 визначені два протоколи аутентифікації:

- по паролю — PAP (Password Authentication Protocol);
- по рукостисканню — CHAP (Challenge Handshake Authentication Protocol).

В процесі встановлення віддаленого з'єднання кожна зі взаємодіючих сторін може запропонувати для застосування один із стандартних протоколів аутентифікації — PAP або CHAP [9].

Іноді компанії створюють власні протоколи аутентифікації віддаленого доступу, працюючі разом з протоколом PPP. Ці фірмові протоколи зазвичай є модифікаціями протоколів PAP і CHAP.

Широке застосування для аутентифікації по одноразових паролях отримав протокол S/Key. У програмних продуктах, що забезпечують зв'язок по протоколу PPP, протоколи PAP і CHAP, як правило, підтримуються в першу чергу.

Протокол PAP

Суть роботи протоколу PAP досить проста. В процесі аутентифікації беруть участь дві сторони — що перевіряється і перевіряюча. Протокол PAP використовує для аутентифікації передачу ідентифікатора і пароля, що перевіряється, у вигляді відкритого тексту. Якщо перевіряюча сторона виявляє збіг ідентифікатора і пароля із записом, наявним у нього у БД легальних користувачів, то процес аутентифікації вважається успішно завершеним, стороні посилається відповідне повідомлення. В якості сторони, чия достовірність перевіряється, як правило, виступає віддалений користувач, а в якості перевіряючої сторони — сервер віддаленого доступу.

Для ініціалізації процесу аутентифікації на базі протоколу PAP сервер віддаленого доступу після встановлення сеансу зв'язку висилає видаленому комп'ютеру пакет LCP (Link Control Protocol) — протокол управління каналом, що вказує на необхідність застосування протоколу PAP. Далі здійснюється обмін пакетами PAP. Віддалений комп'ютер передає по каналу зв'язку перевіряючій стороні ідентифікатор і пароль, введені видаленим користувачем. Сервер віддаленого доступу по отриманому ідентифікатору користувача вибирає еталонний пароль з БД системи захисту і порівнює його з отриманим паролем. Якщо вони співпадають, то аутентифікація вважається успішною, що повідомляється видаленому користувачеві.

Слід особливо відмітити, що протокол аутентифікації PAP, згідно з яким ідентифікатори і паролі передаються по лінії зв'язку в незашифрованому виді, доцільно застосовувати тільки спільно з протоколом, орієнтованим на аутентифікацію по одноразових паролях, наприклад спільно з протоколом S/Key. Інакше пароль, що передається по каналу зв'язку, може бути перехоплений зловмисником і використаний повторно в цілях маскування під санкціонованого віддаленого користувача.

Протокол CHAP

У протоколі CHAP використовується секретний статичний пароль. На відміну від протоколу PAP, в протоколі CHAP пароль кожного користувача для

передачі по лінії зв'язку шифрується на основі випадкового числа отриманого від сервера. Така технологія забезпечує не лише захист пароля від розкрадання, але і захист від повторного використання зловмисником перехоплених пакетів із зашифрованим паролем. Протокол CHAP застосовується в сучасних мережах набагато частіше, ніж PAP, оскільки він використовує передачу пароля по мережі в захищеній формі, і, отже, набагато безпечніше [9].

Шифрування пароля відповідно до протоколу CHAP виконується за допомогою криптографічного алгоритму хешування і тому є безповоротним. У стандарті RFC 1334 для протоколу CHAP в якості хеш-функції визначений алгоритм MD5, що виробляє з вхідної послідовності будь-якої довжини 16-байтове значення. Хоча мінімальною довжиною секрету є 1 байт, для підвищення криптостійкості рекомендується використати секрет завдовжки не менше 16 байт. Специфікація CHAP не унеможливлює використання інших алгоритмів обчислення хеш-функцій.

Для ініціалізації процесу аутентифікації по протоколу CHAP сервер віддаленого доступу після встановлення сеансу зв'язку повинен вислати видаленому комп'ютеру пакет LCP, що вказує на необхідність застосування протоколу CHAP, а також необхідного алгоритму хешування. Якщо віддалений комп'ютер підтримує запропонований алгоритм хешування, то він повинен відповісти пакетом LCP про згоду із запропонованими параметрами. Інакше виконується обмін пакетами LCP для узгодження алгоритму хешування.

Після цього починається аутентифікація на основі обміну пакетами протоколу CHAP.

У протоколі CHAP визначені пакети чотирьох типів:

- Виклик (Challenge);
- Відгук (Response);
- Підтвердження (Success);
- Відмова (Failure).

Протокол CHAP використовує для аутентифікації віддаленого користувача результат шифрування довільного слова виклику за допомогою унікального секрету. Цей секрет є як у перевіряючої, так і у сторони яку перевіряють. Процедура аутентифікації розпочинається з відправки сервером віддаленого доступу пакету Виклик (Рис. 13.4).

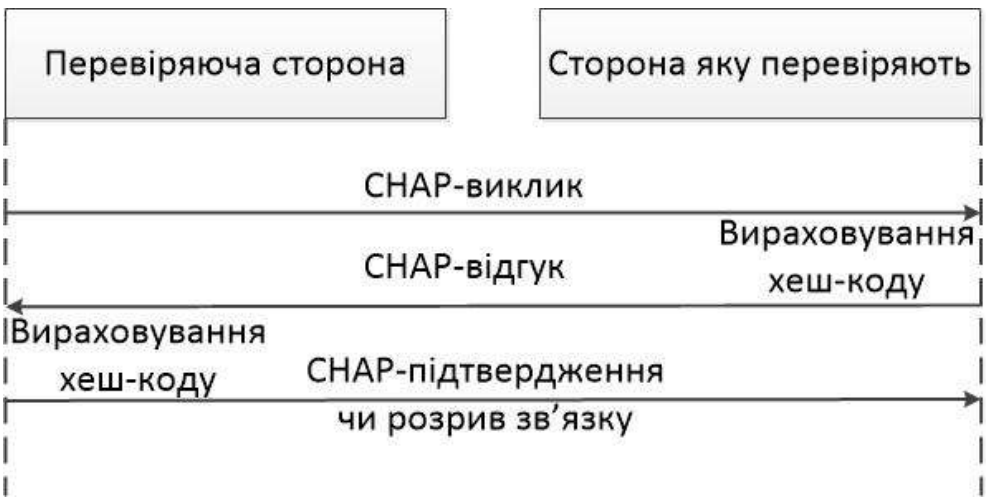

Рис. 13.4. Кроки процесу аутентифікації по протоколу CHAP

Віддалений комп'ютер, отримавши пакет Виклик, зашифровує його за допомогою односторонньої функції і відомого йому секрету, отримуючи в результаті дайджест. Дайджест повертається перевіряючій стороні у вигляді пакету Відгук.

Оскільки використовується одностороння хеш-функция, то по перехоплених пакетах Виклик і Відгук вичислити пароль віддаленого користувача практично неможливо.

Отримавши пакет Відгук, сервер віддаленого доступу порівнює вміст результату з отриманого пакету Відгук з результатом, вичисленим самостійно. Якщо ці результати співпадають, то аутентифікація вважається успішною і сервер висилає видаленому комп'ютеру пакет Підтвердження.

Інакше сервер віддаленого доступу висилає пакет Відмова і розриває сеанс зв'язку.

Пакет Виклик має бути відправлений сервером повторно, якщо у відповідь на нього не був отриманий пакет Відгук. Крім того, пакет Виклик може вирушати періодично впродовж сеансу віддаленого зв'язку для проведення динамічної аутентифікації, щоб переконатися, що протилежна сторона не була підмінена. Відповідно пакет Відгук повинен вирушати стороною, що перевіряється, у відповідь на кожен прийнятий пакет Виклик.

Протокол S/Key

Одним з найбільш поширених протоколів аутентифікації на основі одноразових паролів є стандартизованный в Інтернеті протокол S/Key (RFC 1760) [9, 32]. Цей протокол реалізований у багатьох системах, що вимагають перевірки достовірності віддалених користувачів, зокрема в системі TACACS+ компанії Cisco.

Перехоплення одноразового пароля, що передається по мережі в процесі аутентифікації, не надає зловмисникові можливості повторно використати цей пароль, оскільки при наступній перевірці достовірності необхідно пред'являти вже інший пароль. Тому схема аутентифікації на основі одноразових паролів, зокрема S/Key, дозволяє передавати по мережі одноразовий пароль у відкритому виді і, таким чином, компенсує основний недолік протоколу аутентифікації PAP.

Проте слід зазначити, що протокол S/Key не виключає необхідність завдання секретного пароля для кожного користувача. Цей секретний пароль використовується тільки для генерації одноразових паролів. Для того, щоб зловмисник не зміг по перехопленому одноразовому паролю вичислити секретний початковий пароль, генерація одноразових паролів виконується за допомогою односторонньої, тобто безповоротною, функції. В якості такої односторонньої функції в специфікації протоколу S/Key визначений алгоритм хешування MD4 (Message Digest Algorithm 4). Деякі реалізації протоколу S/Key в якості односторонньої функції використовують алгоритм хешування MD5 (Message Digest Algorithm 5).

Пояснимо основну ідею протоколу S/Key на наступному прикладі.

Нехай видаленому користувачеві (стороні, що перевіряється) для регулярного проходження аутентифікації потрібний набір з 100 одноразових паролів.

Стороні, що перевіряється, заздалегідь призначається генерований випадковий ключ К в якості її секретного постійного пароля. Потім перевіряюча сторона виконує процедуру ініціалізації списку одноразових N = 100 паролів. В ході цієї процедури перевіряюча сторона за допомогою односторонньої функції h обчислює по ключу К перевірочне значення w_{101} для 1-го одноразового пароля. Для обчислення значення w_{101} ключ К підставляють в якості аргументу функції h і ця функція рекурсивно виконується 101 раз:

$$w_1 = h(K),\ w_2 = h(h(K)),\ w_3 = h(h(h(K))),\ \ldots,$$
$$w_{101} = h(h(h(\ldots h(K)\ldots))) = h^{101}(K).$$

Ідентифікатор користувача і що відповідає цьому користувачеві секретний ключ К, а також несекретні числа N і w_{101} зберігаються у БД перевіряючої сторони. Число N є номером одноразового пароля для чергової аутентифікації зі списку одноразових паролів. Слід зазначити, що після використання кожного такого одноразового пароля номер N зменшується на одиницю.

В процесі чергової аутентифікації, що проводиться після ініціалізації, сторона, що перевіряється, надає перевіряючій стороні свій ідентифікатор, а та повертає те, що відповідає цьому ідентифікатору число N. У нашому прикладі N= 100. Сторона, що потім перевіряється, обчислює по своєму секретному ключу К одноразовий пароль

$$w'_{100} = h(h(h(\ldots h(K))\ldots))) = h^{100}(K)$$

і посилає його перевіряючій стороні.

Отримавши значення w'_{100} перевіряюча сторона виконує над ним 1 раз односторонню функцію $w'_{101} = h(w'_{100})$. Далі перевіряюча сторона порівнює отримане значення w'_{101}, зі значенням w_{101} з БД. Якщо вони співпадають, то це означає, що і $w'_{100} = w_{100}$ і, отже, аутентифікація є успішною.

У разі успішної аутентифікації перевіряюча сторона замінює у БД для сторони, що перевіряється, число w_{101} на отримане від неї число w'_{100}, а число N на N=N-1. З урахуванням того, що при успішній аутентифікації номер одноразового пароля N для чергової аутентифікації зменшився на 1, у БД перевіряючої сторони спільно з ідентифікатором і секретним ключем К сторони, що перевіряється, зберігатимуться числа (N - 1) і w_{100} - Тут під w_{100} розуміється отриманий від сторони, що перевіряється, при успішній аутентифікації останній одноразовий пароль. Після використання чергового списку одноразових паролів процедура ініціалізації повинна виконуватися знову.

Іноді бажано, щоб користувач мав можливість сам призначати секретний постійний пароль. Для здійснення такої можливості специфікація S/Key передбачає режим обчислення одноразових паролів не лише на основі секретного пароля, але і на основі генерованого перевіряючою стороною випадкового числа. Таким чином, відповідно до протоколу S/Key за кожним користувачем закріплюється ідентифікатор і секретний постійний пароль.

Перш ніж проходити аутентифікацію, кожен користувач повинен спочатку пройти процедуру ініціалізації чергового списку одноразових паролів, тобто фазу

парольної ініціалізації. Ця фаза виконується за запитом користувача на сервері віддаленого доступу.

Для прискорення процедури аутентифікації певне число одноразових паролів, наприклад декілька десятків, може бути вичислене заздалегідь і зберігатися на видаленому комп'ютері в зашифрованому виді.

Протокол аутентифікації на основі одноразових паролів S/Key застосовують, зокрема, для поліпшення характеристик протоколів централізованого контролю доступу до мережі віддалених користувачів TACACS і RADIUS.

13.2.2. Централізований контроль віддаленого доступу

Для управління віддаленими з'єднаннями невеликої локальної мережі цілком достатньо одного сервера віддаленого доступу. Проте якщо локальна мережа об'єднує відносно великі сегменти і число віддалених користувачів істотно зростає, то одного сервера віддаленого доступу недостатньо.

При використанні в одній локальній мережі декількох серверів віддаленого доступу потрібно централізований контроль доступу до комп'ютерних ресурсів.

Розглянемо, як вирішується завдання контролю доступу до мережі віддалених користувачів відповідно до звичайної схеми, коли віддалені користувачі намагаються отримати доступ до мережевих ресурсів, які знаходяться під управлінням декількох різних ОС. Користувач додзвонюється до свого сервера віддаленого доступу, і RAS виконує для нього процедуру аутентифікації, наприклад по протоколу CHAP. Користувач логічно входить в мережу і звертається до потрібного сервера, де знову проходить аутентифікацію і авторизацію, внаслідок чого отримує або не отримує дозвіл на виконання запрошеної операції.

Неважко помітити, що така схема незручна користувачеві, оскільки йому доводиться кілька разів виконувати аутентифікацію — при вході в мережу на сервері віддаленого доступу, а потім ще кожного разу при зверненні до кожного ресурсного сервера мережі. Користувач вимушений запам'ятовувати декілька різних паролів. Крім того, він повинен знати порядок проходження різних процедур аутентифікації в різних ОС. Виникають також труднощі з адмініструванням такої мережі. Адміністратор повинен заводити облікову інформацію про кожного користувача на кожному сервері. Ці розрізнені БД важко підтримувати в коректному стані. При звільненні співробітника складно виключити його з усіх списків. Виникають проблеми при призначенні паролів, істотно утруднюється аудит.

Відмічені труднощі долаються при установці в мережі централізованої служби аутентифікації і авторизації. Для централізованого контролю доступу виділяється окремий сервер, що називається сервером аутентифікації. Цей сервер служить для перевірки достовірності віддалених користувачів, визначення їх повноважень, а також фіксації і накопичення реєстраційної інформації, пов'язаної з видаленим доступом. Надійність захисту підвищується, якщо сервер віддаленого доступу просить необхідну для аутентифікації інформацію безпосередньо у сервера, на якому зберігається загальна БД системи захисту комп'ютерної мережі.

Проте у більшості випадків сервери віддаленого доступу потребують посередника для взаємодії з центральною БД системи захисту, наприклад із службою каталогів.

Більшість мережевих ОС і служб каталогів зберігають еталонні паролі користувачів з використанням одностороннього хешування, що не дозволяє серверам віддаленого доступу, що стандартно реалізовує протоколи PAP і CHAP, витягнути відкритий еталонний пароль для перевірки відповіді.

Роль посередника у взаємодії між серверами віддаленого доступу і центральної БД системи захисту може бути покладена на сервер аутентифікації. Централізований контроль віддаленого доступу до комп'ютерних ресурсів за допомогою сервера аутентифікації виконується на основі спеціалізованих протоколів. Ці протоколи дозволяють об'єднувати використовувані сервери віддаленого доступу і сервер аутентифікації в одну підсистему, що виконує усі функції контролю віддалених з'єднань на основі взаємодії з центральною БД системи захисту. Сервер аутентифікації створює єдину точку спостереження і перевірки усіх віддалених користувачів і контролює доступ до комп'ютерних ресурсів відповідно до встановлених правил.

До найбільш популярних протоколів централізованого контролю доступу до мережі віддалених користувачів відносяться протоколи TACACS (Terminal Access Controller Access Control System) і RADIUS (Remote Authentication Dial - In User Service). Вони призначені в першу чергу для організацій, в центральній мережі яких використовується декілька серверів віддаленого доступу. У цих системах адміністратор може управляти БД ідентифікаторів і паролів користувачів, надавати їм привілеї доступу і вести облік звернень до системних ресурсів [9].

Протоколи TACACS і RADIUS вимагають застосування окремого сервера аутентифікації, який для перевірки достовірності користувачів і визначення їх повноважень може використати не лише власну БД, але і взаємодіяти із з тимчасовими службами каталогів, наприклад з NDS (Novell Directory Services) і Microsoft Windows NT Directory Service. Сервери TACACS і RADIUS виступають посередниками між серверами віддаленого доступу, що отримали дзвінки від користувачів, з одного боку, і мережевими ресурсними серверами — з іншою. Реалізації TACACS і RADIUS можуть також служити посередниками для зовнішніх систем аутентифікації.

Розглянемо особливості централізованого контролю віддаленого доступу на прикладі протоколу TACACS (Рис. 13.5).

Система TACACS виконана в архітектурі клієнт-сервер [32]. У комп'ютерній мережі, що включає декілька серверів віддаленого доступу, встановлюється один сервер аутентифікації, який називають сервером TACACS (звичайно це програма, працююча в середовищі універсальної ОС, частіше усього Unix).

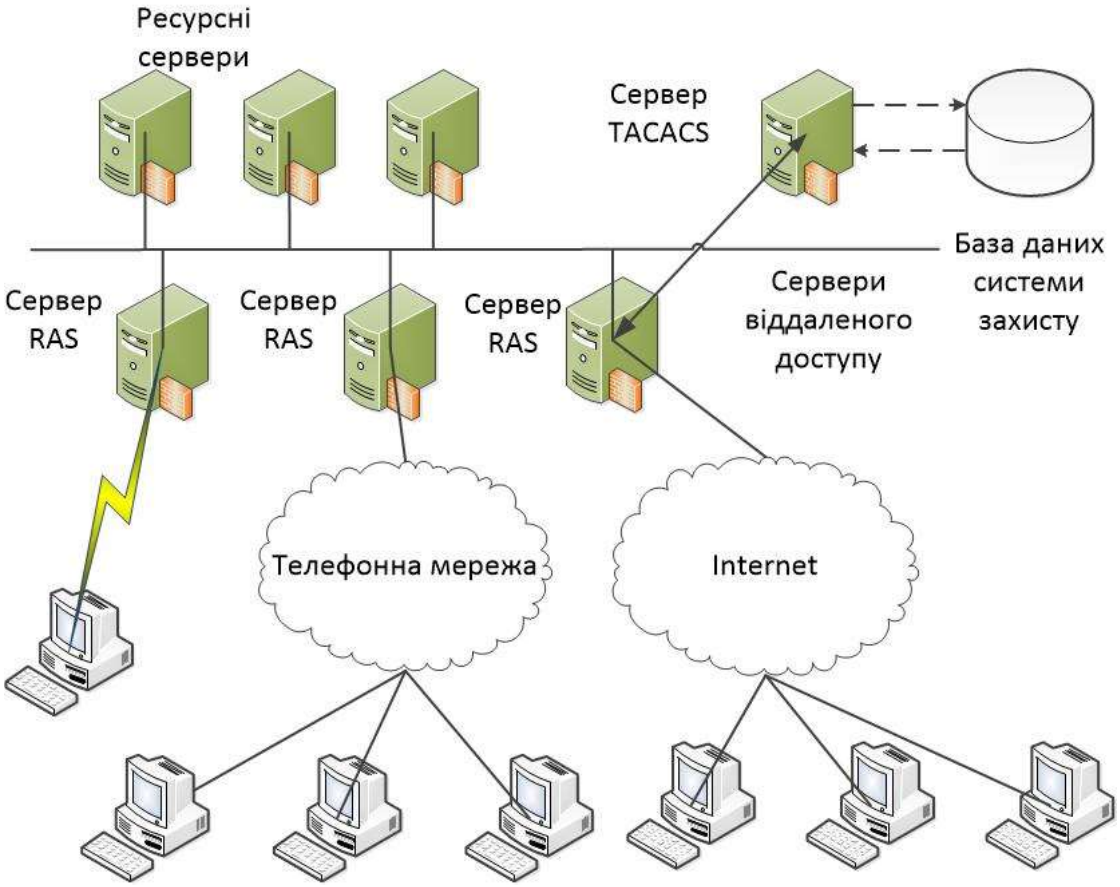

Рис. 13.5. Схема централізованого контролю віддаленого доступу

На сервері TACACS формується центральна база облікової інформації про віддалених користувачів, що включає їх імена, паролі і повноваження. У повноваженнях кожного користувача задаються підмережі, комп'ютери і сервіси, з якими він може працювати, а також різні види обмежень, наприклад тимчасові обмеження. На цьому сервері ведеться БД аудиту, в якій накопичується реєстраційна інформація про кожен логічний вхід, тривалість сесії, а також часу використання ресурсів мережі.

Клієнтами сервера TACACS є сервери віддаленого доступу, приймаючі запити на доступ до ресурсів мережі від віддалених користувачів. У кожен такий сервер вбудовано ПЗ, що реалізовує стандартний протокол, по якому вони взаємодіють з сервером TACACS. Цей протокол також називається TACACS.

Протокол TACACS стандартизує схему взаємодії серверів віддаленого доступу з сервером TACACS на основі завдання можливих типів запитів, відповідей і з'єднань. Визначені запити, з якими клієнти можуть звертатися до сервера TACACS. Сервер на кожен запит повинен відповісти відповідним повідомленням. Протокол задає декілька типів з'єднань, кожне з яких визначається як послідовність пар запит-відповідь, орієнтована на рішення окремої задачі.

Визначений три типи з'єднань:

- AUTH — виконується тільки аутентифікація;
- LOGIN — виконується аутентифікація і фіксується логічне з'єднання з користувачем;
- SLIP — виконується аутентифікація, фіксується логічне з'єднання, підтверджується IP— адреса клієнта.

За допомогою з'єднання AUTH сервери віддаленого доступу перенаправляють серверу TACACS потік запитів на логічне підключення користувачів до мережі в цілому. З'єднання LOGIN служить для перенаправлення запитів серверу TACACS на логічне підключення користувачів до окремих комп'ютерів локальної мережі.

При з'єднанні AUTH сервер віддаленого доступу посилає на сервер TACACS тільки одне повідомлення — пакет AUTH, на який сервер TACACS відповідає повідомленням REPLY.

Сервер TACACS на підставі наявних у нього даних перевіряє пароль і повертає відповідь у вигляді пакету REPLY, де повідомляє про успіх або неуспіх аутентифікації. Відповідно до протоколу TACACS пароль передається між сервером віддаленого доступу і сервером аутентифікації у відкритому виді. Тому протокол TACACS необхідно застосовувати спільно з протоколом аутентифікації по одноразових паролях, наприклад з протоколом S/Key.

На підставі отриманих від сервера TACACS вказівок сервер віддаленого доступу виконує процедуру аутентифікації і дозволяє або не дозволяє видаленому користувачеві логічно увійти до мережі.

Сервер TACACS може виконувати аутентифікацію і авторизацію віддалених користувачів різними способами:

- використати вбудований механізм аутентифікації тієї ОС, під управлінням якої працює сервер;
- використати централізовані довідкові системи ОС;
- використати системи аутентифікації, засновані на одноразових паролях, наприклад систему SecurlD;
- передавати запити іншим системам аутентифікації, наприклад, системі Kerberos.

Слід зазначити, що недоліки протоколу TACACS, пов'язані з відкритою передачею пароля по мережі, усунені компанією Cisco у версії, названою TACACS+. Відповідно до протоколу TACACS+ пароль для передачі по мережі шифрується за допомогою алгоритму MD5. TACACS+ передбачає роздільне зберігання БД аутентифікаційної, авторизаційної і облікової інформації, у тому числі і на різних серверах. Поліпшена взаємодія з системою Kerberos.

Іншою поширеною системою централізованої аутентифікації при видаленому доступі є система RADIUS. По своїх функціональних можливостях протоколи TACACS і RADIUS практично еквівалентні і є відкритими стандартами, проте протокол RADIUS став популярніший серед виробників систем централізованого контролю віддаленого доступу. Це пов'язано з тим, що засноване на нім серверне ПЗ поширюється безкоштовно. Крім того, протокол RADIUS менш складений в реалізації.

13.3. Управління доступом за схемою одноразового входу з авторизацією Single Sign - On (SSO)

Більшість користувачів інформаційних засобів і систем використовують комп'ютери для доступу до ряду сервісів, будь це декілька локальних застосувань або складні застосування, які включають одну або більше віддалених систем, до яких машина користувача під'єднується через мережу. В цілях забезпечення

безпеки багато застосувань вимагають проведення аутентифікації користувача, перш ніж йому дадуть доступ до сервісів і даних, що надаються застосуванням.

Кінцеві користувачі зазвичай сприймають такі вимоги системи безпеки як додаткове навантаження, яке примушує підтримувати і пам'ятати численні вхідні ідентифікатори і паролі і використати їх щодня по кілька разів, щоб мати можливість виконувати свою звичайну роботу. Досить звичайна ситуація, коли один користувач має 5 і більше за таких призначених для користувача accounts, все на різних платформах, з різними правилами для довжин паролів, а також з різною частотою їх заміни. Користувач повинен або заучувати їх, або записувати, піддаючи тим самим безпеку серйозному ризику, оскільки їх і можуть знайти неавторизовані користувачі.

Зі збільшенням числа паролів, що вимагають запам'ятовування, зростає вірогідність того, що ці паролі забуватимуться, а це зажадає від адміністраторів додаткових зусиль із їх відновлення. Цю проблему часто називають «проблемою багатьох входів». Її дозволяє вирішити схема одноразового входу з авторизацією SSO (Single Sign - On).

Управління доступом за схемою SSO дає можливість користувачам корпоративної мережі при їх вході в мережу пройти одну аутентифікацію, пред'явивши тільки один раз пароль (чи інший необхідний аутентификатор), і потім без додаткової аутентифікації отримати доступ до усіх авторизованих мережевих ресурсів, які потрібні для виконання їх роботи. Такими мережевими ресурсами можуть бути принтери, застосування, файли і інші дані, що розміщуються по усьому підприємству на серверах різних типів, працюючих на базі різних ОС. Управління доступом за схемою SSO дозволяє підвищити продуктивність праці користувачів мережі, зменшити вартість мережевих операцій і поліпшити мережеву безпеку.

З функціонуванням схеми SSO безпосередньо пов'язані процеси аутентифікації і авторизації. За допомогою аутентифікації система перевіряє достовірність користувача, тоді як авторизація визначає, що саме дозволяється робити користувачеві (зазвичай грунтуючись на його ролі в організації). Більшість підходів SSO централізований здійснює аутентифікацію користувача. Авторизацію зазвичай виконують на ресурсах цільових об'єктів, хоча деякі просунуті SSO-рішення централізованого здійснюють і авторизацію, при цьому використовуються продукти централізованого адміністрування безпеки, які здійснюють адміністрування повноважень користувачів.

Схему SSO підтримують такі засоби, як протокол LDAP (Lightweight Directory Access Protocol), протокол SSL (Secure Sockets Layer), система Kerberos і інфраструктура управління відкритими ключами PKI (Public Key Infrastructure), а також засоби інтеграції сервісів каталогів і безпеки. Ці засоби і технології утворюють разом фундамент для застосування схеми SSO при обробці даних системами, що використовують різні комбінації клієнтів, серверів, сервісів і застосувань.

Існуючі рішення схеми SSO тягнуться від простих засобів до SSO- сервісів на базі мережевих ОС NOS (Network Operating System), багатофункціональних застосувань і SSO рівня підприємства [9].

Прості засоби SSO включають кеш паролів Windows і кеш паролів, вбудований в продукти, подібні Internet Explorer і інші пакети.

NOS - based SSO- сервіси дають можливість користувачеві входити в такі мережеві ОС, як Windows NT/2000/XP, NetWare або Solaris, і таким чином діставати доступ багатьом або до усіх застосувань, працюючих на базі NOS.

Продукти SSO рівня підприємства, такі як IBM's Global Sign - On та ін., зазвичай застосовують комбіновані підходи до sign - on, засновані на використанні клієнтів і proxy, технології і стандарти кратної аутентифікації, включаючи введення ID користувача і пароля.

13.3.1. Проста система одноразового входу SSO

Просте SSO- рішення полягає в тому, щоб просто автоматизувати процес пред'явлення пароля. Для багатьох з продуктів SSO інформація входу і будь-які необхідні записи зберігаються в спеціальному сервері аутентифікації. Використовуючи клієнтське ПЗ, користувач пред'являє серверу аутентифікації пароль, і цей сервер повідомляє клієнтському ПЗ, до яких ресурсів може отримати доступ користувач (Рис. 13.6). Клієнтське ПЗ представляє користувачеві допустимі опції. Коли користувач вибере ресурс, клієнтське ПЗ використовує мандат входу і scripts, надані сервером аутентифікації, щоб встановити від імені користувача з'єднання з відповідним ресурсом цільового об'єкту (сервера, хоста, домена або застосування).

Рис. 13.6. Просте SSO— рішення — автоматизація входу

При автоматизації процедури входу виконуються наступні кроки.

1. Користувач пред'являє серверу аутентифікації пароль, використовуючи спеціальне клієнтське ПЗ на своєму персональному комп'ютері.
2. Сервер аутентифікації перевіряє, до яких ресурсів може отримати доступ цей користувач і відправляє цю інформацію назад на клієнтське SSO-застосування спільно з необхідним мандатом входу і scripts для з'єднання з кожним дозволеним ресурсом.
3. Клієнтське SSO- застосування представляє користувачеві доступні ресурси і входить від імені користувача у вибрані застосування.

Автоматизація процедури входу дозволяє отримати просту схему SSO, але при цьому ще більше децентралізовується адміністрування безпекою. Ряд постачальників пропонує додаткові кошти централізованого адміністрування безпекою. Ці засоби використовують агентів в цільових системах і забезпечують засноване на ролях (role — based) централізоване адміністрування облікових записів користувачів і інформації про їх повноваження. В деяких випадках ці засоби адміністрування повністю відокремлені від схеми SSO; у інших — інтегровані з SSO.

Первинною метою SSO було скорочення числа використовуваних багаторазових паролів для отримання користувачами доступу до мережевих ресурсів. При формуванні сучасного рішення SSO застосовуються також такі засоби аутентифікації користувача, як токени, цифрові сертифікати PKI, смарт-карти і біометричні пристрої. Досконаліший підхід до аутентифікації зазвичай заснований на використанні токенів. Найбільш відомою системою аутентифікації є Kerberos.

Просунуті SSO- рішення надають більше контролю над повноваженнями користувача, підтримуваними зазвичай на прикладному рівні. У продуктах SSO можуть бути також підтримані нетокенные механізми аутентифікації, засновані на сертифікатах PKI (зокрема, RSA ClearTrust підтримує PKI).

13.3.2. SSO- продукти рівня підприємства

SSO- продукти рівня підприємства проектуються для великих компаній з гетерогенним розподіленим комп'ютерним середовищем, що складається з багатьох систем і застосувань.

Характерним представником SSO- продуктів рівня підприємства являється продукт IBM Global Sign - On for Multiplatforms (далі званий GSO). Продукт GSO представляє безпечне, просте рішення, що дозволяє діставати доступ до мережевих комп'ютерних ресурсів, використовуючи одноразовий вхід в систему. GSO звільняє користувача від необхідності вводити різні ідентифікатори і паролі для усіх його цільових об'єктів, які включають ОС, програмні засоби колективного користування, БД або застосування іншого виду [9].

Було б ідеально, якби GSO міг діяти як універсальний безпечний, надійний механізм аутентифікації для будь-якого цільового об'єкту. На жаль, таке рішення уніфікованої аутентифікації створити неможливе, тому що більшість продуктів, яким потрібно сервіс аутентифікації, виконують процедуру аутентифікації різними способами. Щоб зробити реальністю такий ідеальний підхід, постачальники повинні модифікувати свої продукти так, щоб забезпечити виконання вимог загального стандарту X/Open Single Sign - On (XSSO).

Тому GSO дотримується реального підходу, заснованого на тому факті, що продукти постачальників не підтримують довірену зовнішню аутентифікацію. Для аутентифікації ці продукти найчастіше вимагають ідентифікатор ID і пароль кожного користувача. GSO здійснює безпечне зберігання призначених для користувача ідентифікаторів IDs і паролів, а також забезпечення ними цільових об'єктів, коли користувачеві треба пред'явити пароль при вході. Це звільняє користувача від необхідності пам'ятати і вводити IDs і пароль щодня для кожного цільового об'єкту.

Осередок GSO містить, принаймні, сервер GSO і одну робочу станцію користувача, що називається також клієнтом GSO. У осередку GSO може бути більший за один сервер GSO і безліч клієнтів (Рис. 13.7).

Рис. 13.7. Базові компоненти GSO

Користувач взаємодіє зі своєю робочою станцією і деякими цільовими об'єктами (застосуваннями), які можуть виконуватися на цій робочій станції або на якому-небудь іншому комп'ютері, наприклад сервері департаменту або серверах застосувань.

Перш ніж почати роботу, користувач повинен увійти до своєї робочої станції. Він пред'являє пароль саме GSO, а не застосуванню або іншим серверам. GSO виконує аутентифікацію, засновану на ідентифікаторі ID і паролі користувача (іноді підтримуваних смарт-картою або считывателем відбитків пальців). Сервер GSO включається в процес аутентифікації, для того, щоб перевірити пароль користувача і витягнути його мандат (credentials).

Потім GSO вводить користувача в цільові об'єкти (застосування або сервери), з якими цей користувач повинен працювати. GSO використовує для входу користувача методи, що надаються цільовими об'єктами. У більшості випадків GSO імітує вхід користувача, передаючи цільовому об'єкту ID і пароль користувача, неначе вводить їх сам користувач. Важлива відмінність, очевидно, полягає в тому, що тепер користувачеві не треба запам'ятовувати ці ідентифікатори ID і паролі, оскільки турботу про них переймає на себе GSO.

GSO являється клієнт/серверним застосуванням. На додаток до сервера GSO існує програма клієнта (сегмент програмного коду), що виконується на робочій станції користувача, яка взаємодіє з сервером GSO [9].

SSO- продукти рівня підприємства мають наступні достоїнства:

- допускають використання багатьох цільових платформ зі своїми власними механізмами аутентифікації;
- безпечно зберігають у БД облікову інформацію користувачів (таку як ідентифікатор ID, пароль і деяку додаткову інформацію) на кожну цільову платформу і кожного користувача;
- радикально зменшують долю паролів, що забуваються, оскільки паролі користувачів зберігаються безпечно і надійно;

• використовують методи і засоби безпечної аутентифікації і комунікації; чутлива призначена для користувача інформація зберігається і передається по мережі тільки в зашифрованому виді.

Недоліками SSO- продуктів рівня підприємства є їх відносно велика вартість і високі вимоги до кваліфікації обслуговуючого персоналу.

13.4. Протокол Kerberos

Протокол Kerberos використовується в системах клієнт-сервер для аутентифікації і обміну ключовою інформацією, призначеною для встановлення захищеного каналу зв'язку між абонентами, працюючими як в локальній мережі, так і глобальних мережах. Цей протокол вбудований в якості основного протоколу аутентифікації в Microsoft Windows 2000 і в UNIX BSD.

Kerberos забезпечує аутентифікацію у відкритих мережах, тобто при роботі Kerberos мається на увазі, що зловмисники можуть виконувати наступні дії:

• видавати себе за одну з легітимних сторін мережевого зєднання;

• мати фізичний доступ до одного з комп'ютерів, що беруть участь в з'єднанні;

• перехоплювати будь-які пакети, модифікувати їх і (чи) передавати повторно.

Відповідно, забезпечення безпеки в Kerberos побудоване так, щоб нейтралізувати будь-які потенційні проблеми, які можуть виникнути через вказані дії зловмисників.

Kerberos розроблений для мереж TCP/IP і побудований на основі довіри учасників протоколу до третьої (довіреної) сторони. Служба Kerberos, працююча в мережі, діє як довірений посередник, забезпечуючи надійну аутентифікацію в мережі з подальшою авторизацією доступу клієнта (клієнтського застосування) до ресурсів мережі. Захищеність встановлених у рамках сесії Kerberos з'єднань обумовлюється застосуванням симетричних алгоритмів шифрування. Служба Kerberos розділяє окремий секретний ключ з кожним суб'єктом мережі, і знання такого секретного ключа рівносильне доказу достовірності суб'єкта мережі.

Основу Kerberos складає протокол аутентифікації і розподілу ключів Нидхема — Шредера з третьою довіреною стороною [9]. Розглянемо цю версію протоколу. У протоколі Kerberos (версія 5) беруть участь дві взаємодіючі сторони і довірений сервер KS, що виконує роль Центру розподілів ключів.

Зухвалий (початковий) об'єкт позначається через A, а що викликається (об'єкт призначення) — через B. Учасники сеансу A і

У мають унікальні ідентифікатори. Сторони A і B, кожна окремо, розділяють свій секретний ключ з сервером KS.

Нехай сторона A хоче отримати сеансовий ключ для інформаційного обміну із стороною B.

Сторона A ініціює фазу розподілу ключів, посилаючи по мережі серверу KS ідентифікатори Id_A і Id_B:

$$A \rightarrow \text{KS: } Id_A, Id_B \quad (1)$$

Сервер KS генерує сполучення з тимчасовою відміткою T, терміном дії L, випадковим сеансовим ключем K і ідентифікатором Id_A Він шифрує це повідомлення секретним ключем, який розділяє із стороною B.

Потім сервер KS бере тимчасову відмітку T, термін дії L, сеансовий ключ K, ідентифікатор Id_B сторони B і шифрує усе це секретним ключем, який розділяє із стороною A. Обоє ці зашифровані повідомлення він відправляє стороні A:

$$KS \rightarrow A: E_A(T, L, K, Id_B), E_B(T, L, K, Id_A) \quad (2)$$

Сторона A розшифровує повідомлення своїм секретним ключем, перевіряє відмітку часу T, щоб переконатися, що це повідомлення не є повторенням попередньої процедури розподілу ключів. Потім сторона A генерує сполучення зі своїм ідентифікатором Id_A і відміткою часу T, шифрує його сеансовим ключем K і відправляє стороні B. Крім того, A відправляє для B повідомлення від KS, зашифроване ключем сторони B:

$$A \rightarrow B: E_K(Id_A, T), E_B(T, L, K, Id_A) \quad (3)$$

Тільки сторона B може розшифрувати повідомлення (3). Сторона B отримує відмітку часу T, термін дії L, сеансовий ключ K і ідентифікатор Id_A Потім сторона B розшифровує сеансовим ключем K другу частину повідомлення (3). Збіг значень T і Id_A в двох частинах повідомлення підтверджують достовірність A по відношенню до B.

Для взаємного підтвердження достовірності сторона B створює повідомлення, що складається з відмітки часу T плюс 1, шифрує його ключем K і відправляє стороні A:

$$B \rightarrow A: E_K(T+1) \quad (4)$$

Якщо після расшифровування повідомлення (4) сторона A отримує очікуваний результат, вона знає, що на іншому кінці лінії зв'язку знаходиться дійсно B.

Цей протокол успішно працює за умови, що годинник кожного учасника синхронізований з годинником сервера KS. Слід зазначити, що в цьому протоколі потрібний обмін з KS для отримання сеансового ключа кожного разу, коли A бажає встановити зв'язок з B. Протокол забезпечує надійне з'єднання об'єктів A і B за умови, що жоден з ключів не скомпрометований і сервер KS захищений.

Система Kerberos має структуру типу клієнт-сервер і складається з клієнтських частин З, встановлених на усіх робочих станціях користувачів і серверах мережі, і сервера Kerberos KS, розташованого на якому-небудь (не обов'язково виділеному) комп'ютері (див. Рис. 13.8). Клієнтами можуть бути користувачі, а також незалежні програми, виконуючі такі дії, як завантаження віддалених файлів, відправка повідомлень, доступ до БД, доступ до принтерів, отримання привілеїв у адміністратора і т. п.

Сервер Kerberos KS, можна розділити на дві частини: сервер аутентифікації AS (Authentication Server) і сервер служби видачі мандатів TGS (Ticket Granting

Service). Фізично ці сервери можуть бути поєднані. Інформаційними ресурсами, необхідними клієнтам З, управляє сервер інформаційних ресурсів RS. Передбачається, що сервери служби Kerberos надійно захищені від фізичного доступу зловмисників.

Мережеві служби, що вимагають перевірки достовірності, і клієнти, які хочуть використати ці служби, реєструють в Kerberos свої секретні ключі. Kerberos зберігає БД про клієнтів і їх секретні ключі. Наявність в цій БД секретних ключів кожного користувача і ресурсів мережі, що підтримують цей протокол, дозволяє створювати зашифровані повідомлення, що направляються клієнтові або серверу; успішне расшифрование цих повідомлень і є гарантією проходження аутентифікації усіма учасниками протоколу.

Kerberos також створює сеансові ключі (session key), які видаються клієнтові і серверу (чи двом клієнтам) і нікому більше. Сеансовий ключ використовується для шифрування повідомлень, якими обмінюються дві сторони, і знищується після закінчення сеансу.

Зона дії системи Kerberos поширюється на ту ділянку мережі, усі користувачі якої зареєстровані під своїми іменами і паролями у БД сервера Kerberos.

Укрупнено процес ідентифікації і аутентифікації користувача в системі Kerberos версії 5 можна описати таким чином (Рис. 13.8).

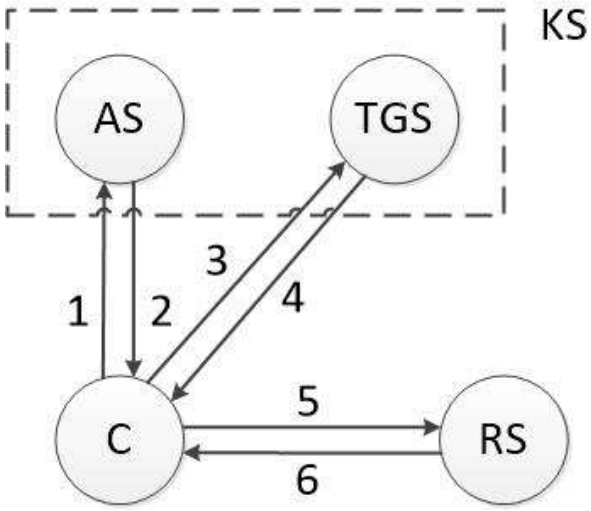

Рис. 13.8. Схема роботи протоколу Kerberos
KS — сервер системи Kerberos
AS — сервер аутентифікації
TGS — сервер служби виділення мандатів
RS — сервер інформаційних ресурсів
C — клієнт системи

Клієнт С, бажаючи отримати доступ до ресурсу мережі, направляє запит серверу аутентифікації AS. Сервер AS ідентифікує користувача за допомогою його імені і пароля і висилає клієнтові мандат (ticket) на доступ до сервера служби виділення мандатів TGS (Ticket - Granting Service).

Для використання конкретного цільового сервера інформаційних ресурсів RS клієнт С просить у TGS мандат на звернення до цільового сервера RS. Якщо все

гаразд, TGS дозволяє використання необхідних ресурсів мережі і посилає відповідний мандат клієнтові С.

Основні кроки роботи системи Kerberos (див. Рис. 13.10):

1. С -> AS — запит клієнта С до сервера AS дозволити звернутися до служби TGS.
2. AS -> С — дозвіл (мандат) від сервера AS клієнтові Із звернутися до служби TGS.
3. С -> TGS — запит клієнта С до служби TGS на отримання допуску (мандату) до сервера ресурсів RS.
4. TGS -> С — дозвіл (мандат) від служби TGS клієнтові С для звернення до сервера ресурсів RS.
5. З -> RS — запит інформаційного ресурсу (послуги) у сервера RS.
6. RS -> З — підтвердження достовірності сервера RS і надання інформаційного ресурсу (послуги) клієнтові С.

Ця модель взаємодії клієнта з серверами може функціонувати тільки за умови забезпечення конфіденційності і цілісності передаваної і керуючої інформації. Без строгого забезпечення інформаційної безпеки клієнт С не може відправляти серверам AS, TGS і RS свої запити і отримувати дозволи на доступ до обслуговування в мережі.

Щоб уникнути можливості перехоплення і несанкціонованого використання інформації, Kerberos застосовує при передачі будь-якої інформації, що управляє, в мережі систему багатократного шифрування з використанням комплексу секретних ключів (секретний ключ клієнта, секретний ключ сервера, секретні сеансові ключі пари клієнт-сервер). Kerberos може використати різні симетричні алгоритми шифрування і хеш-функції.

На сьогодні протокол Kerberos є широко поширеним засобом аутентифікації. Kerberos може використовуватися у поєднанні з різними криптографічними схемами, включаючи шифрування з відкритим ключем.

13.5. Інфраструктура управління відкритими ключами PKI

Історично в завдання будь-якого центру управління інформаційною безпекою завжди входив набір завдань по управлінню ключами, використовуваними різними засобами захисту інформації (ЗЗІ). У цей набір входять видача, оновлення, відміна і поширення ключів.

У разі використання симетричної криптографії завдання поширення секретних ключів представляло найбільш важку проблему, оскільки:

- для N користувачів необхідно розповсюдити в захищеному режимі N/2 ключів, що обтяжливо при N близько декількох сотень;
- система поширення ключів складна (багато ключів і закритий канал поширення), що призводить до появи вразливих місць.

Асиметрична криптографія дозволяє обійти цю проблему, запропонувавши до використання тільки N секретних ключів. При цьому у кожного користувача тільки один секретний ключ

і один відкритий, отриманий по спеціальному алгоритму з секретного.

З відкритого ключа практично неможливо отримати секретний, тому відкритий ключ можна поширювати відкритим способом усім учасникам взаємодії.

На підставі свого закритого ключа і відкритого ключа свого партнера по взаємодії будь-який учасник може виконувати будь-які криптографічні операції: електронно-цифровий підпис, розрахунок секрету, що розділяється, захист конфіденційності і цілісності повідомлення.

В результаті вирішуються дві головні проблеми симетричної криптографії:

- перевантаженість кількістю ключів — їх тепер усього N;
- складність поширення — їх можна поширювати відкрито.

Проте у цієї технології є один недолік — схильність атаці man — in — the — middle (человек-в-середине), коли атакуючий зловмисник розташований між учасниками взаємодії. В цьому випадку з'являється ризик підміни передаваних відкритих ключів.

Інфраструктура управління відкритими ключами PKI (Public Key Infrastructure) дозволяє здолати цей недолік і забезпечити ефективний захист від атаки man - in - the - middle.

13.5.1. Принципи функціонування PKI

Інфраструктура відкритих ключів PKI призначена для надійного функціонування КИЦЬ і дозволяє як внутрішнім, так і зовнішнім користувачам безпечно обмінюватися інформацією за допомогою ланцюжка довірчих стосунків. Інфраструктура відкритих ключів грунтується на цифрових сертифікатах, які діють подібно до електронних паспортів, що зв'язують індивідуальний секретний ключ користувача з його відкритим ключем.

Захист від атаки man - in - the - middle

При здійсненні атаки man - in - the - middle той, що атакує може непомітно замінити передавані по відкритому каналу відкриті ключі законних учасників взаємодії на свій відкритий ключ, створити секрети, що розділяються, з кожним із законних учасників і потім перехоплювати і розшифровувати усі їх повідомлення.

Пояснимо на прикладі (Рис. 13.9) дії того, що атакує і спосіб захисту від цієї атаки. Припустимо, що користувач 1 і користувач 2 вирішили встановити захищене з'єднання, розрахувавши загальний для них секрет, що розділяється, за схемою Діффі — Хеллмана. Проте у момент передачі по відкритому каналу відкритих ключів K_1^0 і K_2^0 користувачів 1 і 2 зловмисник @ перехопив ці ключі, не давши їм дійти до адресатів. Створивши свої закритий і відкритий ключі, зловмисник @ передає свій відкритий ключ $K_@^0$ користувачів 1 і 2, непомітно підмінивши своїм ключем $K_@^0$ їх справжні відкриті ключі до, K_1^0 і K_2^0. В результаті користувачі 1 і 2 створять секрети, що розділяються, не між собою, а між 1 <-> @ і 2 <-> @, оскільки вони використовуватимуть свої закриті ключі і і відкритий ключ К зловмисника @.

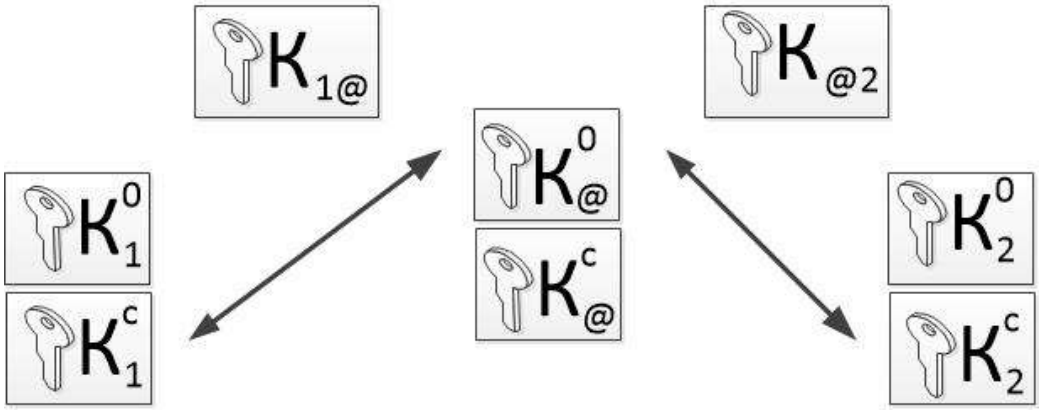

Рис. 13.9. Здійснення атаки man - in - the - middle

Коли користувач 1 відправлятиме користувачеві 2 зашифровану інформацію, зловмисник @ може її перехопити і розшифрувати (у нього з користувачем 1 свій секрет $K_{@1}$ що розділяється,,). Потім зловмисник @ зашифрує інформацію (можливо, змінену) наново, використовуючи другий секрет $K_{@2}$, що розділяється, розрахований ним і користувачем 2. В результаті користувач 2 отримуватиме, розшифровуватиме і використає інформацію, відправлену зловмисником @, вважаючи, що він має захищений канал з користувачем 1.

Ця проста, але результативна атака є розплатою за гарне рішення завдання розподілу ключів, запропоноване асиметричною криптографією.

Проблема підміни відкритих ключів успішно вирішується шляхом використання сертифікатів відкритих ключів.

Сертифікати відкритих ключів

Сертифікати відкритих ключів відіграють важливу роль в криптографії відкритих ключів. Їх основне призначення — зробити доступним і достовірним відкритий ключ користувача.

У основу формування сертифікатів відкритих ключів покладені принципи строгої аутентифікації, що рекомендовані стандартом X. 509 і базуються на властивостях криптосистем з відкритим ключем.

Криптосистеми з відкритим ключем припускають наявність у користувача парних ключів — секретного і відкритого (загальнодоступного). Кожен користувач ідентифікується за допомогою свого секретного ключа. За допомогою парного відкритого ключа будь-який інший користувач має можливість визначити, чи являється його партнер по зв'язку справжнім власником секретного ключа.

Процедура, що дозволяє кожному користувачеві встановлювати однозначну і достовірну відповідність між відкритим ключем і його власником, забезпечується за допомогою механізму сертифікації відкритих ключів.

Міра достовірності факту встановлення достовірності (аутентифікації) користувача залежить від надійності зберігання секретного ключа і надійності джерела постачання відкритих ключів користувачів. Щоб користувач міг довіряти процесу аутентифікації, він повинен витягати відкритий ключ іншого користувача з надійного джерела, якому він довіряє. Таким джерелом згідно із стандартом X. 509 є Центр сертифікації CA (Certification Authority).

Центр сертифікації CA є довіреною третьою стороною, що забезпечує аутентифікацію відкритих ключів, що містяться в сертифікатах. CA має власну

пару ключів (відкритий/секретний), де секретний ключ СА використовується для підписки сертифікатів, а відкритий ключ СА публікується і використовується користувачами для перевірки достовірності відкритого ключа, що міститься в сертифікаті.

Сертифікація відкритого ключа — це підтвердження достовірності відкритого ключа і що зберігається спільно з ним службовою інформацією, зокрема про приналежність ключа. Сертифікація ключа виконується шляхом обчислення ЕЦП ключа, що сертифікується, і службової інформації за допомогою спеціального секретного ключа-сертифікату, доступного тільки СА. Іншими словами, сертифікація відкритого ключа — ця підписка відкритого ключа електронним підписом, вичисленим на секретному ключі СА.

Відкритий ключ спільно з тією, що сертифікує його ЕЦП часто називають сертифікатом відкритого ключа або просто сертифікатом.

СА формує сертифікат відкритого ключа користувача шляхом завірення цифровим підписом СА певного набору даних.

Відповідно до формату X. 509 в цей набір даних включаються:

- період дії відкритого ключа, що складається з двох дат: почала і кінця періоду;
- номер і серія ключа;
- унікальне ім'я користувача;
- інформація про відкритий ключ користувача: ідентифікатор алгоритму, для якого призначений цей ключ, і власне відкритий ключ;
- ЕЦП і інформація, використовувана при проведенні процедури перевірки ЕЦП (наприклад, ідентифікатор алгоритму генерації ЕЦП);
- унікальне ім'я сертифікаційного центру.

Таким чином, цифровий сертифікат містить три головні складові:

- інформацію про користувача — власника сертифікату;
- відкритий ключ користувача;
- сертифікуючу ЕЦП двох попередніх складових, вичислену на секретному ключі СА.

Сертифікат відкритого ключа має наступні властивості:

- кожен користувач, що має доступ до відкритого ключа СА, може витягнути відкритий ключ, включений в сертифікат;
- жодна сторона, окрім СА, не може змінити сертифікат так, щоб це не було виявлено (сертифікати не можна підробити).

Оскільки сертифікати не можуть бути підроблені, то їх можна опублікувати, помістивши в загальнодоступний довідник не роблячи спеціальних зусиль із захисту цих сертифікатів.

Створення сертифікату відкритого ключа розпочинається із створення пари ключів (відкритий/секретний).

Процедура генерації ключів може здійснюватися двома способами.

1. СА створює пару ключів. Відкритий ключ заноситься в сертифікат, а парний йому секретний ключ передається користувачеві із забезпеченням аутентифікації користувача і конфіденційності передачі ключа.
2. Користувач сам створює пару ключів. Секретний ключ зберігається у користувача, а відкритий ключ передається по захищеному каналу в СА.

Кожен користувач може бути власником одного або декількох сертифікатів, сформованих сертифікаційним центром СА користувача. Користувач може володіти сертифікатами, отриманими з декількох різних сертифікаційних центрів.

На практиці часто виникає потреба аутентифицировать користувача, який отримує сертифікати в іншому сертифікаційному центрі. Принципи розподіленого адміністрування розглядаються нижче.

Базові моделі сертифікації

Концепція інфраструктури відкритих ключів PKI має на увазі, що усі сертифікати конкретної PKI (своя PKI може бути у будь-якої організації або організаційної одиниці) організовані в певну структуру.

У PKI розрізняють чотири типи сертифікатів.

1. Сертифікат кінцевого користувача (описаний вище).
2. Сертифікат СА. Має бути доступний для перевірки ЕЦП сертифікату кінцевого користувача і підписаний секретним ключем СА верхнього рівня, причому ця ЕЦП також повинна перевірятися, для чого має бути доступний сертифікат СА верхнього рівня, і т. д.
3. Самопідписаний сертифікат. Є кореневим для усієї PKI і довіреним за визначенням — в результаті перевірки ланцюжка сертифікатів СА з'ясується, що один з них підписаний кореневим секретним ключем, після чого процес перевірки ЕЦП сертифікатів закінчується.
4. Крос-сертифікат. Дозволяє розширити дію конкретної PKI шляхом взаємнопідписання кореневих сертифікатів двох різних PKI.

Існують три базові моделі сертифікації:

- ієрархічна модель, заснована на ієрархічному ланцюзі сертифікатів;
- модель кросс-сертификації (має на увазі взаємну сертифікацію);
- мережева (гібридна) модель, що включає елементи ієрархічної і взаємної сертифікації [9].

Узагальнені схеми ієрархічної і мережевої архітектури систем управління сертифікатами приведені на Рис. 13.10.

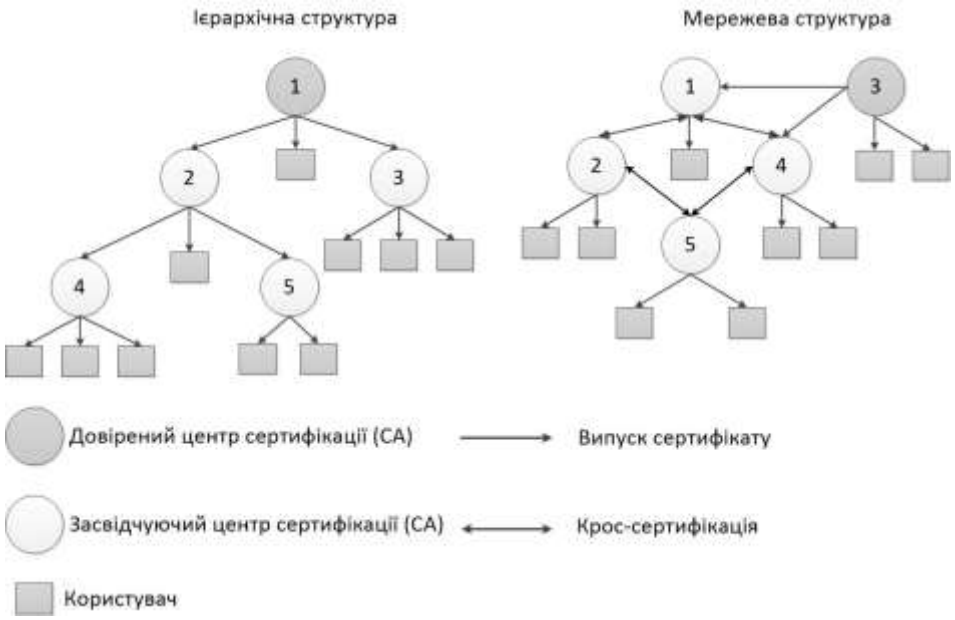

Рис. 13.10. Ієрархічна і мережева архітектура систем управління сертифікатами

У ієрархічній моделі СА розташовані в ієрархічному підпорядкуванні довіреному (кореневому) СА, що надає сертифікати іншим СА.

Достоїнства ієрархічної архітектури системи управління сертифікатами:

- аналогічна існуючим федеральним і відомчим структурам, що організаційно-управляють, і може будуватися з урахуванням цього;
- визначає простий алгоритм пошуку, побудови і верифікації ланцюжків сертифікатів для усіх взаємодіючих сторін;
- для забезпечення взаємодії двох користувачів одному з них досить надати іншому свій ланцюжок сертифікатів, що зменшує проблеми, пов'язані з їх взаємодією.

Недолік ієрархічної архітектури: для забезпечення взаємодії усіх кінцевих користувачів має бути тільки один кореневий довірений СА.

У моделі кросс-сертифікації незалежні СА, що не знаходяться на одній гілці ієрархії, взаємно сертифікують один одного в мережі СА. Крос-сертифікація є предметом двосторонньої угоди між СА. Слід зазначити, що модель кросс-сертифікації є часткою випадком мережевої архітектури системи управління сертифікатами.

Достоїнства мережевої архітектури системи управління сертифікатами:

- гнучкість, що сприяє встановленню безпосередніх довірених взаємовідносин, існуючих в сучасному бізнесі;
- стосунки довіри в системі: кінцевий користувач повинен довіряти, принаймні, тільки центру, що видав його сертифікат;
- можливість безпосередньої кросс-сертифікації різних засвідчуючих СА, користувачі яких часто взаємодіють між собою, що скорочує процес верифікації ланцюжків.

Недоліки мережевої архітектури управління сертифікатами:

- складність алгоритму пошуку і побудови ланцюжків сертифікатів для усіх взаємодіючих сторін;
- неможливість надання користувачем ланцюжка, який забезпечує перевірку його сертифікату усіма іншими користувачами.

Ймовірно, в недалекому майбутньому на найвищому рівні ієрархії сертифікації повинен виявитися державний нотаріус, який забезпечить зв'язок ланцюжків довіри різних організацій.

13.5.2. Логічна структура і компоненти PKI

Інфраструктура відкритих ключів PKI (Public Key Infrastructure) — це набір агентів і правил, призначених для управління ключами, політикою безпеки і власне обміном захищеними повідомленнями [9, 50].

Основні завдання PKI:

- підтримка життєвого циклу цифрових ключів і сертифікатів (тобто генерація ключів, створення і підпис сертифікатів, їх розподіл і ін.);
- реєстрація фактів компрометації і публікація «чорних» списків відкликаних сертифікатів;
- підтримка процесів ідентифікації і аутентифікації користувачів так, щоб скоротити, по можливості, час допуску кожного користувача в систему;

• реалізація механізму інтеграції (заснованого на PKI) існуючих застосувань і усіх компонентів підсистеми безпеки;

• надання можливості використання єдиного «токена» безпеці, однакового для усіх користувачів і застосувань, такого, що містить усі необхідні ключові компоненти і сертифікати.

Токен безпеки — цей індивідуальний засіб безпеки, що визначає усі права і оточення користувача в системі, наприклад смарт-карта.

Застосування, що вимагає систему управління ключами, повинне взаємодіяти з системою PKI у ряді точок (передача сертифікату на підпис, отримання сертифікату і «чорного» списку при встановленні взаємодії і т. п.). Очевидно, що ця взаємодія з чужою по відношенню до цього застосування системою може здійснюватися тільки за умови повної підтримки міжнародних стандартів, яким задовольняє більшість сучасних PKI- систем (наприклад, Baltimore, Entrust, Verisign).

Для надання віддаленого доступу мобільним користувачам центр управління повинен допускати підключення комп'ютерів, IP- адреса яких йому заздалегідь невідома. Учасники інформаційного обміну пізнаються по їх криптографічних сертифікатах. Оскільки криптографічний сертифікат користувача є електронним паспортом, він, як і будь-який паспорт, повинен відповідати певним стандартам. У криптографії це стандарт X. 509.

На Рис. 13.11 приведена логічна структура і основні компоненти інфраструктури управління відкритими ключами PKI.

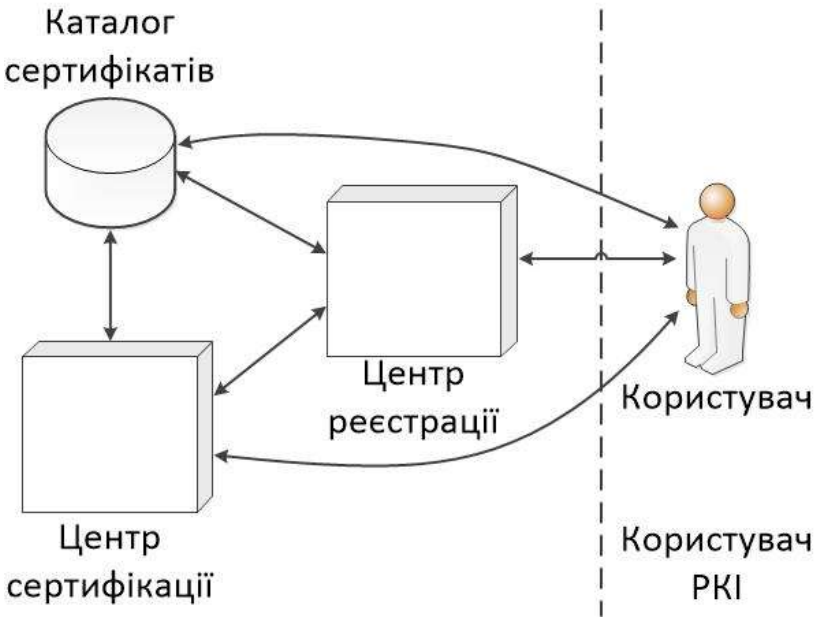

Рис. 13.11. Структура PKI

Компоненти цієї структури мають наступне призначення.

Каталог сертифікатів — загальнодоступне сховище сертифікатів користувачів. Доступ до сертифікатів проводиться зазвичай по стандартизованному протоколу доступу до каталогів LDAP (Lightweight Directory Access Protocol).

Центр реєстрації RA (Registration Authority) — організаційна одиниця, призначення якої — реєстрація користувачів системи.

Користувач — власник якого-небудь сертифікату (такий користувач підлягає реєстрації) або будь-який користувач, що просить сертифікат, що зберігається в каталозі сертифікатів.

Центр сертифікації CA (Certification Authority) — організаційна одиниця, призначення якої — сертифікація відкритих ключів користувачів (тут з відкритого ключа виходить сертифікат формату X. 509) і їх публікація в каталозі сертифікатів.

Загальна схема роботи CA виглядає таким чином:

- CA генерує власні ключі і формує сертифікати CA, призначені для перевірки сертифікатів користувачів;
- користувачі формують запити на сертифікацію і доставляють їх CA тим або іншим способом;
- CA на основі запитів користувачів формує сертифікати користувачів;
- CA формує і періодично оновлює списки скасованих сертифікатів CRL (Certificate Revocation List);
- сертифікати користувачів, сертифікати CA і списки відміни CRL публікуються CA (розсилаються користувачам або поміщаються в загальнодоступний довідник).

Інфраструктуру відкритих ключів PKI підтримує ряд ОС, застосувань і стандартів.

У свою чергу інфраструктура відкритих ключів PKI може інтегрувати перераховані функціональні області. В результаті можна створювати комплексну систему інформаційної безпеки шляхом інтеграції інфраструктури відкритих ключів в ІС компанії і використання єдиних стандартів і сертифікатів відкритих ключів.

Лекція 14 АНАЛІЗ ЗАХИЩЕНОСТІ І ВИЯВЛЕННЯ АТАК

Ряд провідних зарубіжних організацій, що займаються мережевою безпекою, розробили підходи, що дозволяють не лише розпізнавати існуючі уразливості і атаки, але і виявляти старі, що змінилися, або нові, що з'явилися, уразливості і протиставляти їм відповідні засоби захисту.

14.1. Концепція адаптивного управління безпекою

Атакою на КІС вважається будь-яка дія, що виконується порушником для реалізації загрози шляхом використання уразливостей КІС. Під уразливістю КІС розуміється будь-яка характеристика або елемент КІС, використання яких порушником може привести до реалізації загрози.

Архітектура КІС включає чотири рівні.

1. Рівень прикладного програмного забезпечення (ПЗ), що відповідає за взаємодію з користувачем. Прикладом елементів І З, працюючих на цьому рівні, можна назвати текстовий редактор WinWord, редактор електронних таблиць Excel, поштову програму Outlook і т. д.
2. Рівень системи управління базами даних (СУБД), що відповідає за зберігання і обробку даних ІС. Прикладом елементів ІС, працюючих на цьому рівні, можна назвати СУБД Oracle, MS SQL Server, Sybase і MS Access.
3. Рівень операційної системи (ОС), що відповідає за обслуговування СУБД і прикладного ПЗ. Прикладом елементів ІС, працюючих на цьому рівні, можна назвати ОС Microsoft Windows, Sun Solaris, Novell Netware.
4. Рівень мережі, що відповідає за взаємодію вузлів ІС. Прикладом елементів ІС, працюючих на цьому рівні, можна назвати стеки протоколів TCP/IP, IPS/SPX і SMB/NetBIOS.

Зловмисник має в розпорядженні широкий спектр можливостей для порушення безпеки КІС. Ці можливості можуть бути реалізовані на усіх чотирьох перелічених вище рівнях КІС. Наприклад, для отримання НСД до фінансової інформації в СУБД MS SQL Server зловмисник може реалізувати одну з наступних можливостей:

- перехопити передавані по мережі дані (рівень мережі);
- прочитати файли БД, звертаючись безпосередньо до файлової системи (рівень ОС);
- прочитати потрібні дані засобами самої СУБД (рівень СУБД);
- прочитати записи БД за допомогою SQL- запитів через програму MS Query, яка дозволяє діставати доступ до записів СУБД (рівень прикладного ПЗ).

При побудові більшості традиційних комп'ютерних засобів захисту використовувалися класичні моделі розмежування доступу, розроблені ще в 1970-80-і рр. недостатня ефективність таких традиційних механізмів захисту, як розмежування доступу, аутентифікація, фільтрація і інші, обумовлена тим, що при їх створенні не враховані багато аспектів, пов'язаних з сучасними атаками.

Розглянемо етапи здійснення атаки на КІС (Рис. 14.1) [40].

Перший, підготовчий, етап полягає в пошуку зловмисником передумов для здійснення тієї або іншої атаки. На цьому етапі зловмисник шукає уразливості в системі. На другому, основному етапі — реалізації атаки — здійснюється

використання знайдених вразливостей. На третьому, завершальному, етапі зловмисник завершує атаку і намагається приховати сліди вторгнення. В принципі перший і третій етапи самі по собі можуть бути атаками. Наприклад, пошук зловмисником вразливостей за допомогою сканерів безпеки сам по собі вважається атакою.

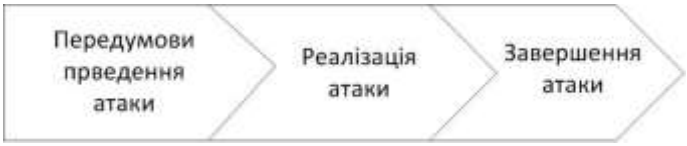

Рис. 14.1. Етапи здійснення атаки

Перший, підготовчий, етап полягає в пошуку зловмисником передумов для здійснення тієї або іншої атаки. На цьому етапі зловмисник шукає уразливості в системі. На другому, основному етапі — реалізації атаки — здійснюється використання знайдених вразливостей. На третьому, завершальному, етапі зловмисник завершує атаку і намагається приховати сліди вторгнення. В принципі перший і третій етапи самі по собі можуть бути атаками. Наприклад, пошук зловмисником вразливостей за допомогою сканерів безпеки сам по собі вважається атакою.

Слід зазначити, що існуючі механізми захисту, реалізовані в МЕ, серверах аутентифікації, системах розмежування доступу, працюють тільки на етапі реалізації атаки. По суті ці механізми захищають від атак, які знаходяться вже в процесі здійснення. Ефективнішим було б попередження атак, тобто запобігання самим передумовам реалізації вторгнення. Комплексна система забезпечення інформаційної безпеки повинна ефективно працювати на усіх трьох етапах здійснення атаки.

У організаціях часто не враховується той факт, що адміністратори і користувачі регулярно змінюють конфігурацію ІС. В результаті цих змін можуть з'являтися нові уразливості, пов'язані з ОС і застосуваннями. Крім того, дуже швидко змінюються інформаційні і мережеві технології, регулярно з'являється нове ПЗ. Безперервний розвиток мережевих технологій за відсутності аналізу їх безпеки, що постійно проводиться, і нестачі ресурсів для забезпечення захисту призводить до того, що з часом захищеність КІС падає, оскільки з'являються нові невраховані загрози і уразливості системи.

У більшості випадків для вирішення виникаючих проблем із захистом в організаціях використовуються часткові підходи. Ці підходи зазвичай обумовлені передусім поточним рівнем доступних ресурсів. Крім того, адміністратори безпеки мають тенденцію реагувати тільки на ті ризики безпеки, які їм зрозумілі. Фактично таких ризиків може бути істотно більший. Тільки строгий поточний контроль захищеності КІС і комплексний підхід, що забезпечує єдину політику безпеки, дозволяють істотно понизити риски безпеки.

Адаптивний підхід до безпеки дозволяє контролювати, виявляти і реагувати в реальному режимі часу на риски безпеки, використовуючи правильно спроектовані і добре керовані процеси і засоби.

Адаптивна безпека мережі складається з трьох основних елементів [40]:

- технології аналізу захищеності (security assessment);

- технології виявлення атак (intrusion detection);
- технології управління ризиками (risk management).

Оцінка ризику полягає у виявленні і ранжируванні вразливостей (по мірі серйозності збитку потенційних дій), підсистем мережі (по мірі критичності), загроз (виходячи з вірогідності їх реалізації) і т. д. Оскільки конфігурація мережі постійно змінюється, то і процес оцінки ризику повинен проводитися постійно. З оцінки ризиків повинна розпочинатися побудова системи захисту КІС.

Аналіз захищеності — це пошук вразливих місць в мережі. Мережа складається із з'єднань, вузлів, хостов, робочих станцій, застосувань і БД. Усі вони потребують як оцінки ефективності їх захисту, так і в пошуку невідомих вразливостей в них. Технології аналізу захищеності досліджують мережу і шукають «слабкі» місця в ній, узагальнюють ці відомості і друкують по них звіт. Якщо система, що реалізовує цю технологію, містить і адаптивний компонент, то усунення знайденої уразливості здійснюватиметься не вручну, а автоматично. Технологія аналізу захищеності є дієвим методом, що дозволяє реалізувати політику мережевої безпеки перш, ніж здійсниться спроба її порушення зовні або зсередини організації.

Перерахуємо деякі з проблем, що ідентифікуються технологією аналізу захищеності:

- «люки« в системах (back door) і програми типу »троянський кінь«;
- слабкі паролі;
- сприйнятливість до проникнення з незахищених систем і атак типу «відмова в обслуговуванні»;
- відсутність необхідних оновлень (patch, hotfix) ОС;
- неправильне налаштування МЕ, Web- серверів і БД;
- і багато інших.

Виявлення атак є процесом оцінки підозрілих дій, які відбуваються в корпоративній мережі. Виявлення атак реалізується за допомогою аналізу або журналів реєстрації ОС і застосування або мережевого трафіку в реальному часі. Компоненти виявлення атак, розміщені на вузлах або сегментах мережі, оцінюють різні події і дії, у тому числі і дії, використовуючі відомі уразливості (Рис. 14.2).

Рис. 14.2. Взаємодія систем аналізу захищеності і виявлення атак

Адаптивний компонент моделі адаптивного управління безпекою (ANS) відповідає за модифікацію процесу аналізу захищеності, надаючи йому саму останню інформацію про нові вразливості. Він також модифікує компонент виявлення атак, доповнюючи його останньою інформацією про атаки. Як приклад адаптивного компонента можна вказати механізм оновлення БД антивірусних програм для виявлення нових вірусів. Компонент, що управляє, має бути здатний

до генерації звітів і аналізу тенденцій, пов'язаних з формуванням системи захисту організації.

Адаптація даних може полягати в різних формах реагування, які можуть включати:

- відправлення повідомлень системам мережевого управління по протоколу SNMP, по електронній пошті або на пейджер адміністраторові;
- автоматичне завершення сесії з атакуючим вузлом або користувачем, реконфігурація МЕ або інших мережевих пристроїв (наприклад, маршрутизаторів);
- вироблення рекомендацій адміністраторові, що дозволяють своєчасно усунути виявлені уразливості в мережах, застосуваннях або інших компонентах ІС організації [40].

Використання моделі адаптивної безпеки мережі (Рис. 14.3) дозволяє контролювати практично усі загрози і своєчасно реагувати на них високоефективним способом, що дозволяє не лише усунути уразливості, які можуть привести до реалізації загрози, але і проаналізувати умови, що призводять до появи вразливостей.

Рис. 14.3. Модель адаптивної безпеки

Модель адаптивної безпеки мережі дозволяє також зменшити зловживання в мережі, підвищити обізнаність користувачів, адміністраторів і керівництва компанії про події безпеки в мережі. Слід зазначити, що ця модель не відкидає вже використовувані механізми захисту (розмежування доступу, аутентифікація і т. д.). Вона розширює їх функціональність за рахунок нових технологій.

Для того, щоб привести свою систему забезпечення інформаційної безпеки у відповідність сучасним вимогам, організаціям необхідно доповнити наявні рішення компонентами, що відповідають за аналіз захищеності, виявлення атак і управління рисками.

14.2. Технологія аналізу захищеності

У організації, що використовує КІС, доводиться регулярно перевіряти, наскільки реалізовані або використовувані механізми захисту інформації відповідає положенням прийнятої в організації політики безпеки. Таке завдання

періодично виникає при зміні і оновленні компонентів ІС, зміні конфігурації ОС і т. п. [9, 40].

Проте адміністратори мереж не мають досить часу на проведення такого роду перевірок для усіх вузлів корпоративної мережі. Тому фахівці відділів захисту інформації потребують засобів, що полегшують аналіз захищеності використовуваних механізмів забезпечення інформаційної безпеки. Цей процес допомагають автоматизувати засоби аналізу захищеності, що часто називаються сканерами безпеки (security scanners).

Використання засобів аналізу захищеності дозволяє визначити уразливості на вузлах корпоративної мережі і усунути їх до того, як ними скористаються зловмисники. По суті, дії системи аналізу захищеності аналогічні діям охоронця, що періодично обходить усі поверхи будівлі, що охороняється, у пошуках відкритих дверей, незакритих вікон і інших проблем. Тільки будівлею виступає корпоративна мережа, а в якості незакритих вікон і дверей — уразливості.

Засоби аналізу захищеності працюють на першому етапі здійснення атаки. Виявляючи і своєчасно усуваючи уразливості, вони тим самим запобігають саму можливість реалізації атаки, що дозволяє понизити витрати на експлуатацію засобів захисту.

Засоби аналізу захищеності можуть функціонувати на мережевому рівні, рівні ОС і рівні застосування. Вони можуть проводити пошук вразливостей, поступово нарощуючи число перевірок і «поглиблюючись» в ІС, досліджуючи усі її рівні.

Найбільше поширення отримали засоби аналізу захищеності мережевих сервісів і протоколів. Обумовлено це, в першу чергу, універсальністю використовуваних протоколів. Вивченість і повсюдне використання таких протоколів, як IP, TCP, HTTP, FTP, SMTP і т. п., дозволяють з високою мірою ефективності перевіряти захищеність ІС, працюючою в мережевому оточенні.

Другими за поширеністю є засоби аналізу захищеності ОС. Обумовлено це також універсальністю і поширеністю деяких ОС (наприклад, UNIX і Windows NT).

Засоби аналізу захищеності застосувань доки існують тільки для широко поширених прикладних систем типу Web- браузери і СУБД.

Застосування засобів аналізу захищеності дозволяє швидко визначити усі вузли корпоративної мережі, доступні у момент проведення тестування, виявити усі використовувані в мережі сервіси і протоколи, їх налаштування і можливості для несанкціонованої дії (як зсередини корпоративної мережі, так і зовні). За результатами сканування ці засоби виробляють рекомендації і покрокові заходи, що дозволяють усунути виявлені недоліки.

Цей метод контролю порушень політики безпеки не може замінити фахівця з інформаційної безпеки. Засоби аналізу захищеності можуть лише автоматизувати пошук деяких відомих вразливостей.

14.2.1. Засоби аналізу захищеності мережевих протоколів і сервісів

Взаємодія абонентів у будь-якій мережі базується на використанні мережевих протоколів і сервісів, що визначають процедуру обміну інформацією між двома і більше вузлами. При розробці мережевих протоколів і сервісів до них пред'являлися вимоги (зазвичай явно недостатні) по забезпеченню безпеки

оброблюваної інформації. Тому постійно з'являються повідомлення про виявлених в мережевих протоколах вразливості. В результаті виникає потреба в постійній перевірці усіх використовуваних в корпоративній мережі протоколів і сервісів.

Системи аналізу захищеності виконують серію тестів по виявленню вразливостей. Ці тести аналогічні вживаним зловмисниками при здійсненні атак на корпоративні мережі.

Сканування з метою виявлення вразливостей розпочинається з отримання попередньої інформації про систему, що перевіряється. Закінчується сканування спробами імітації проникнення, використовуючи широко відомі атаки, наприклад підбір пароля методом повного перебору (brute force — «груба сила»).

За допомогою засобів аналізу захищеності на рівні мережі можна тестувати не лише можливість НСД в корпоративну мережу з мережі Internet. Ці засоби можуть бути використані як для оцінки рівня безпеки організації, так і для контролю ефективності налаштування мережевого програмного і апаратного забезпечення.

Нині відомий більше десятка різних засобів, що автоматизують пошук вразливостей мережевих протоколів і сервісів. Серед комерційних систем аналізу захищеності можна назвати Internet Scanner компанії Internet Security Systems, Inc., NetSonar компанії Cisco, CyberCop Scanner компанії Network Associates і ряд інших.

Типова схема проведення аналізу захищеності (на прикладі системи Internet Scanner) приведена на Рис. 14.4.

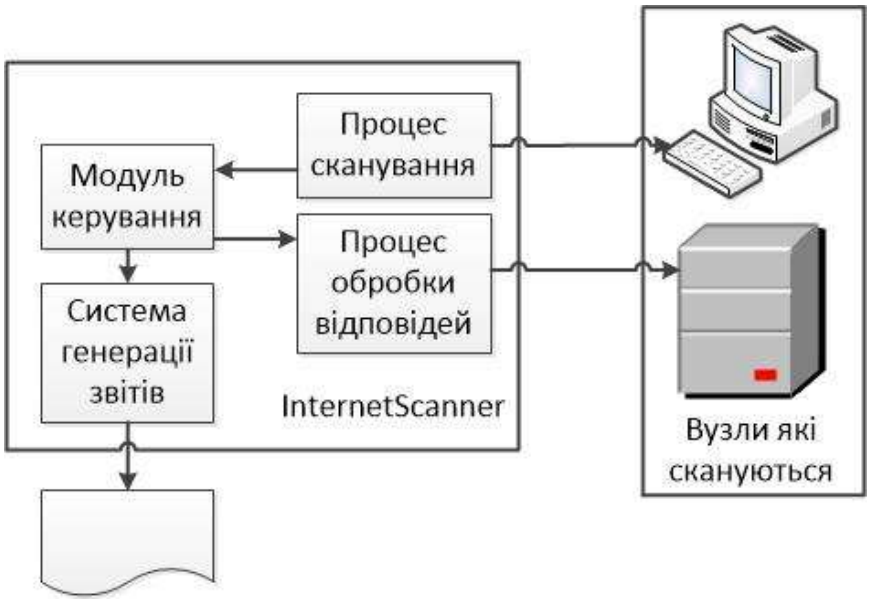

Рис. 14.4. Схема проведення аналізу захищеності (на прикладі системи Internet Scanner)

Засоби аналізу захищеності цього класу аналізують не лише уразливість мережевих сервісів і протоколів, але і системного і прикладного ПЗ, що відповідає за роботу з мережею. До такого забезпечення можна віднести Web-, FTP - і поштові сервери, МЕ, браузери і т. п.

14.2.2. Засоби аналізу захищеності ОС

Засоби цього класу призначені для перевірки налаштувань ОС, що впливають на її захищеність. До таких налаштувань можна віднести:

- облікові записи користувачів (account), наприклад довжину пароля і термін його дії;
- права користувачів на доступ до критичних системних файлів;
- уразливі системні файли;
- встановлені патчі (patch) і т. п.

Системи аналізу захищеності на рівні ОС можуть бути використані також для контролю конфігурації ОС.

На відміну від засобів аналізу захищеності мережевого рівня ці системи проводять сканування не зовні, а зсередини аналізованої системи, тобто вони не імітують атаки

зовнішніх зловмисників. Окрім можливостей по виявленню вразливостей, деякі системи аналізу захищеності на рівні ОС (наприклад, System Scanner компанії Internet Security Systems) дозволяють автоматично усувати частину виявлених проблем або коригувати параметри системи, що не задовольняють політиці безпеки, прийнятої в організації.

14.3. Технології виявлення атак

Мережеві і інформаційні технології міняються настільки швидко, що статичні захисні механізми, до яких відносяться системи розмежування доступу, МЕ, системи аутентифікації у багатьох випадках не можуть забезпечити ефективного захисту. Тому потрібно динамічні методи, що дозволяють оперативно виявляти і запобігати порушенням безпеки. Однією з технологій, що дозволяє виявляти порушення, які не можуть бути ідентифіковані за допомогою традиційних моделей контролю доступу, є технологія виявлення атак.

По суті, процес виявлення атак є процесом оцінки підозрілих дій, які відбуваються в корпоративній мережі. Інакше кажучи, виявлення атак (intrusion detection) — це процес ідентифікації і реагування на підозрілу діяльність, спрямовану на обчислювальні або мережеві ресурси.

14.3.1. Методи аналізу мережевої інформації

Ефективність системи виявлення атак багато в чому залежить від вживаних методів аналізу отриманої інформації. У перших системах виявлення атак, розроблених на початку 1980-х рр., використовувалися статистичні методи виявлення атак. Нині до статистичного аналізу додалися ряд нових методик, починаючи з експертних систем і нечіткої логіки і закінчуючи використанням нейронних мереж [9, 40].

Статистичний метод. Основні переваги статистичного підходу — використання вже розробленого апарату математичної статистики, що зарекомендував себе, і адаптація до поведінки суб'єкта.

Спочатку для усіх суб'єктів аналізованої системи визначаються профілі. Будь-яке відхилення використовуваного профілю від еталонного вважається несанкціонованою діяльністю. Статистичні методи універсальні, оскільки для проведення аналізу не потрібно знання про можливі атаки і використовуваних ними вразливості. Проте при використанні цих методик виникають і проблеми:

- «статистичні« системи не чутливі до порядку дотримання подій; в деяких випадках одні і ті ж події залежно від порядку їх дотримання можуть характеризувати аномальну або нормальну діяльність;
- важко задати граничні (порогові) значення відстежуваних системою виявлення атак характеристик, щоб адекватно ідентифікувати аномальну діяльність;
- «статистичні« системи можуть бути з часом »навчені« порушниками так, щоб атакуючі дії розглядалися як нормальні.

Слід також враховувати, що статистичні методи не застосовні в тих випадках, коли для користувача відсутній шаблон типової поведінки або коли для користувача типові несанкціоновані дії.

Експертні системи складаються з набору правил, які охоплюють знання людини-експерта. Використання експертних систем є поширеним методом виявлення атак, при якому інформація про атаки формулюється у вигляді правил. Ці правила можуть бути записані, наприклад, у вигляді послідовності дій або у вигляді сигнатури. При виконанні будь-якого з цих правил приймається рішення про наявність несанкціонованої діяльності. Важливою гідністю такого підходу є практично повна відсутність неправдивих тривог.

БД експертної системи повинна містити сценарії більшості відомих на сьогодні атак. Для того, щоб залишатися постійно актуальними, експертні системи вимагають постійного оновлення БД. Хоча експертні системи пропонують хорошу можливість для перегляду даних в журналах реєстрації, необхідні оновлення можуть або ігноруватися, або виконуватися адміністратором вручну. Як мінімум, це призводить до експертної системи з ослабленими можливостями. У гіршому разі відсутність належного супроводу знижує міру захищеності усієї мережі, вводячи її користувачів в оману відносно дійсного рівня захищеності.

Основним недоліком є неможливість відображення невідомих атак. При цьому навіть невелика зміна вже відомої атаки може стати серйозною перешкодою для функціонування системи виявлення атак.

Нейронні мережі. Більшість сучасних методів виявлення атак використовують деяку форму аналізу контрольованого простору на основі правил або статистичного підходу. Контрольованим простором можуть виступати журнали реєстрації або мережевий трафік. Аналіз спирається на набір заздалегідь визначених правил, які створюються адміністратором або самою системою виявлення атак.

Будь-яке розділення атаки в часі або серед декількох зловмисників є важким для виявлення за допомогою експертних систем. Через велику різноманітність атак і хакерів навіть спеціальні постійні оновлення БД правил експертної системи ніколи не дадуть гарантії точній ідентифікації усього діапазону атак.

Використання нейронних мереж є одним із способів подолання вказаних проблем експертних систем. На відміну від експертних систем, які можуть дати користувачеві певну відповідь про відповідність даних характеристик закладеним у БД правилам, нейронна мережа проводить аналіз інформації і надає можливість оцінити, чи узгоджуються дані з характеристиками, які вона навчена розпізнавати. Тоді як міра відповідності нейромережевого представлення може досягати 100 %, достовірність вибору повністю залежить від якості системи в аналізі прикладів поставленого завдання.

Спочатку нейромережу навчають правильній ідентифікації на заздалегідь підібраній вибірці прикладів предметної області. Реакція нейромережі аналізується і система настроюється так, щоб досягти задовільних результатів. На додаток до початкового періоду навчання, нейромережа набирається досвіду з часом, у міру того, як вона проводить аналіз даних, пов'язаних з предметною областю.

Важливою перевагою нейронних мереж при виявленні зловживань є їх здатність «вивчати» характеристики умисних атак і ідентифікувати елементи, які не схожі на ті, що спостерігалися в мережі раніше.

Кожен з описаних методів має ряд достоїнств і недоліків, тому зараз практично важко зустріти систему, що реалізовує тільки один з описаних методів. Як правило, ці методи використовуються в сукупності.

14.3.2. Класифікація систем виявлення атак IDS

Механізми, вживані в сучасних системах виявлення атак IDS (Intrusion Detection System), засновані на декількох загальних методах, які не є взаємовиключними. У багатьох системах використовуються їх комбінації.

Класифікація IDS може бути виконана:

- за способом реагування;
- способу виявлення атаки;
- способу збору інформації про атаку.

За способом реагування розрізняють пасивні і активні IDS. Пасивні IDS просто фіксують факт атаки, записують дані у файл журналу і видають попередження. Активні IDS намагаються протидіяти атаці, наприклад, шляхом реконфігурації МЕ або генерації списків доступу маршрутизатора.

За способом виявлення атаки системи IDS прийнято ділити на дві категорії:

- виявлення аномальної поведінки (anomaly - based);
- виявлення зловживань (misuse detection або signature - based).

Технологія виявлення аномальної поведінки заснована на наступному. Аномальна поведінка користувача (тобто атака або яка-небудь ворожа дія) часто проявляється як відхилення від нормальної поведінки. Прикладом аномальної поведінки може служити велике число з'єднань за короткий проміжок часу, високе завантаження центрального процесора і т. п.

Якщо можна було б однозначно описати профіль нормальної поведінки користувача, то будь-яке відхилення від нього можна ідентифікувати як аномальну поведінку. Проте аномальна поведінка не завжди є атакою. Наприклад, одночасну посилку великого числа запитів від адміністратора мережі система виявлення атак може ідентифікувати як атаку типу «відмова в обслуговуванні» («denial of service»).

При використанні системи з такою технологією можливі два випадки:

- виявлення аномальної поведінки, яка не є атакою, і віднесення його до класу атак;
- пропуск атаки, яка не підпадає під визначення аномальної поведінки. Цей випадок небезпечніший, ніж неправдиве віднесення аномальної поведінки до класу атак.

Технологія виявлення аномалій орієнтована на виявлення нових типів атак. Проте недолік її — необхідність постійного навчання. Поки ця технологія не

отримала широкого поширення. Пов'язано це з тим, що вона важко реалізовується на практиці.

Виявлення зловживань полягає в описі атаки у вигляді сигнатури (signature) і пошуку цієї сигнатури в контрольованому просторі (мережевому трафіку або журналі реєстрації). Сигнатурою атаки може виступати шаблон дій або рядок символів, що характеризують аномальну діяльність. Ці сигнатури зберігаються у БД, аналогічній тій, яка використовується в антивірусних системах. Ця технологія виявлення атак дуже схожа на технологію виявлення вірусів, при цьому система може виявити усі відомі атаки. Проте системи цього типу не можуть виявляти нові, ще невідомі види атак.

Підхід, реалізований в таких системах, досить простий і саме на нім засновані практично усі пропоновані сьогодні на ринку системи виявлення атак.

Найбільш популярна класифікація за способом збору інформації про атаку:

- виявлення атак на рівні мережі (network - based);
- виявлення атак на рівні хоста (host - based);
- виявлення атак на рівні застосування (application - based).

Система network - based працює за типом сниффера, «прослуховуючи» трафік в мережі і визначаючи можливі дії зловмисників. Такі системи аналізують мережевий трафік, використовуючи, як правило, сигнатури атак і аналіз «на льоту». Метод аналізу «на льоту» полягає в моніторингу мережевого трафіку в реальному або близькому до реального часу і використанні відповідних алгоритмів виявлення.

Системи host - based призначені для моніторингу, детектування і реагування на дії зловмисників на певному хості. Розташовуючись на хості, що захищається, вони перевіряють і виявляють спрямовані проти нього дії. Ці системи аналізують реєстраційні журнали ОС або застосування.

Як правило, аналіз журналів реєстрації є доповненням до інших методів виявлення атак, зокрема до виявлення атак «на льоту». Використання цього методу дозволяє проводити «розбір польотів» вже після того, як була зафіксована атака, для того, щоб виробити ефективні заходи запобігання аналогічним атакам в майбутньому.

Система application - based заснована на пошуку проблем в певному застосуванні.

Кожен з цих типів систем виявлення атак (на рівні мережі, на рівні хоста і на рівні застосування) має свої достоїнства і недоліки. Гібридні IDS, що є комбінацією різних типів систем, як правило, включають можливості декількох категорій.

14.3.3. Компоненти і архітектура IDS

На основі аналізу існуючих рішень можна привести перелік компонентів, з яких складається типова система виявлення атак [40].

Модуль стеження забезпечує збір даних з контрольованого простору (журналу реєстрації або мережевого трафіку). Різні виробники дають цьому модулю наступні назви: сенсор (sensor), монітор (monitor), зонд (probe) і т. д.

Залежно від архітектури побудови системи виявлення атак модуль стеження може бути фізично відокремлений від інших компонентів, тобто знаходитися на іншому комп'ютері.

Підсистема виявлення атак — основний модуль системи виявлення атак. Вона здійснює аналіз інформації, що отримується від модуля стеження. За результатами цього аналізу ця підсистема може ідентифікувати атаки, приймати рішення відносно варіантів реагування, зберігати відомості про атаку в сховищі даних і т. д.

База знань залежно від методів, використовуваних в системі виявлення атак, може містити профілі користувачів і обчислювальної системи, сигнатури атак або підозрілі рядки, що характеризують несанкціоновану діяльність. База знань може поповнюватися виробником системи виявлення атак, користувачем системи або третьою стороною, наприклад аутсорсинговой компанією, що здійснює підтримку цієї системи.

Сховище даних забезпечує зберігання даних, зібраних в процесі функціонування системи виявлення атак.

Графічний інтерфейс. Навіть дуже потужний і ефективний засіб не використовуватиметься, якщо у нього відсутній дружній інтерфейс. Залежно від ОС, під управлінням якої функціонує система виявлення атак, графічний інтерфейс повинен відповідати стандартам де-факто для Windows і Unix.

Підсистема реагування здійснює реагування на виявлені атаки і інші контрольовані події. Варіанти реагування будуть описані детальніше нижче.

Підсистема управління компонентами призначена для управління різними компонентами системи виявлення атак. Під терміном «управління» розуміється можливість зміни політики безпеки для різних компонентів системи виявлення атак (наприклад, модулів стеження), а також отримання інформації від цих компонентів (наприклад, відомості про зареєстровану атаку). Управління може здійснюватися як за допомогою внутрішніх протоколів і інтерфейсів, так і за допомогою вже розроблених стандартів, наприклад SNMP.

Системи виявлення атак будуються на основі двох архітектури: «автономний агент» і «агент-менеджер». У першому випадку на кожен вузол, що захищається, або сегмент мережі встановлюються агенти системи, які не можуть обмінюватися інформацією між собою, а також не можуть управлятися централізовано з єдиної консолі. Цих недоліків позбавлена архітектура «агент-менеджер». В цьому випадку в розподіленій системі виявлення атак dIDS (distributed IDS), що складається з безлічі IDS, розміщених в різних ділянках великої мережі, сервери збору даних і центральний аналізуючий сервер здійснюють централізований збір і аналіз реєстрованих даних. Управління модулями dIDS здійснюється з центральної консолі управління [39]. Для великих організацій, в яких філії рознесені по різних територіях і навіть містах, використання такої архітектури має принципове значення.

Загальна схема функціонування dIDS приведена на Рис. 14.5.

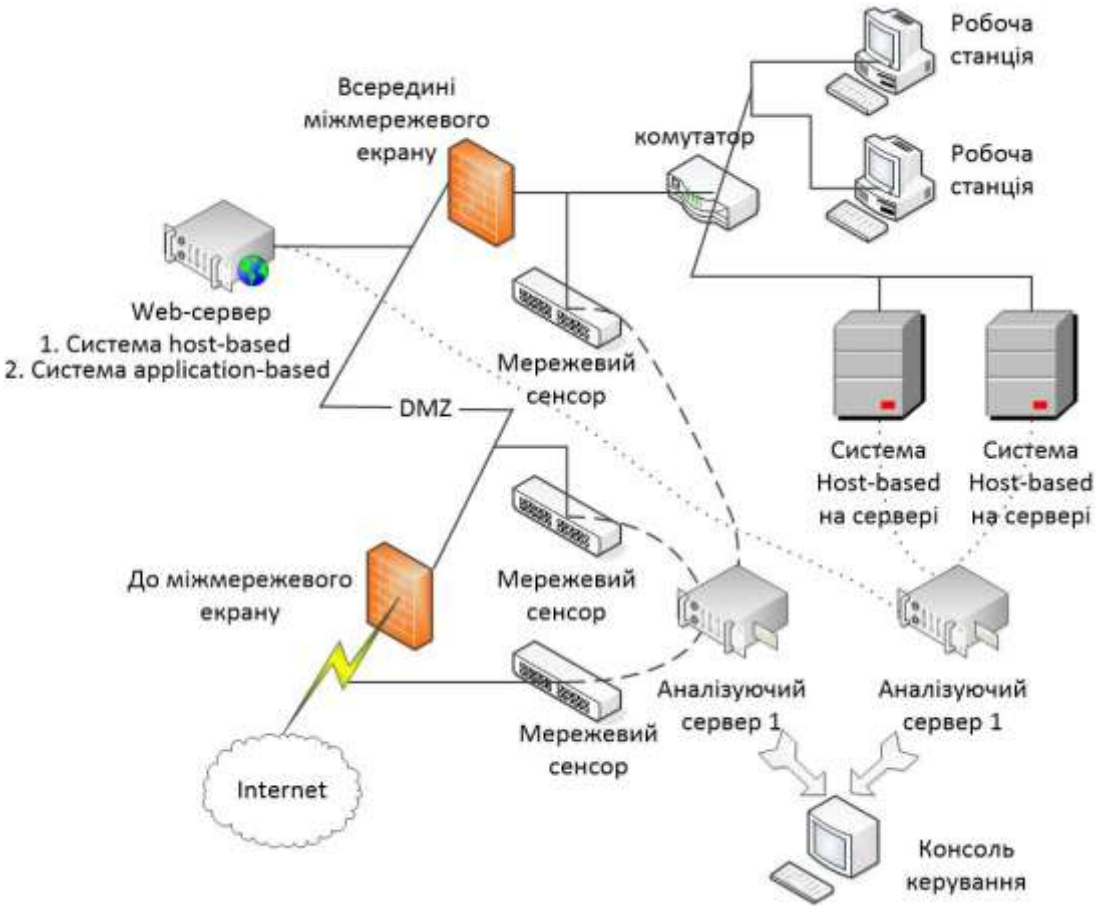

Рис. 14.5. Загальна схема функціонування розподіленої dIDS

Така система дозволяє посилити захищеність корпоративної підмережі завдяки централізації інформації про атаку від різних IDS. Розподілена система виявлення атак IDS складається з наступних підсистем: консолі управління, аналізуючих серверів, агентів мережі, серверів збору інформації про атаку. Центральний аналізуючий сервер зазвичай складається з БД і Web — сервера, що дозволяє зберігати інформацію про атаки і маніпулювати даними за допомогою зручного Web— інтерфейсу. Агент мережі — один з найбільш важливих компонентів dIDS. Він є невеликою програмою, мета якої — повідомляти про атаку на центральний аналізуючий сервер. Сервер збору інформації про атаку — частина системи IDS, що логічно базується на центральному аналізуючому сервері. Сервер визначає параметри, по яких групуються дані, отримані від агентів мережі. Угрупування даних може здійснюватися за наступними параметрами:

- IP- адресі того, що атакує;
- порту одержувача;
- номеру агента;
- даті, часу;
- протоколу;
- типу атаки і т. д.

14.3.4. Методи реагування

Атака не лише має бути виявлена, але і необхідно правильно і своєчасно зреагувати на неї. У існуючих системах застосовується широкий спектр методів реагування, які можна розділити на три категорії [9, 40]:

- повідомлення;
- збереження;
- активне реагування.

Застосування тієї або іншої реакції залежить від багатьох чинників.

Повідомлення. Найпростішим і широко поширеним методом повідомлення є відправлення адміністраторові безпеки повідомлень про атаку на консоль системи виявлення атак. Така консоль може бути встановлена не у кожного співробітника, що відповідає в організації за безпеку, крім того, цих співробітників можуть цікавити не усі події безпеки, тому потрібне застосування інших механізмів повідомлення. Цими механізмами можуть бути відправлення повідомлень по електронній пошті, на пейджер, факсом або по телефону.

До категорії «повідомлення» відноситься також посилка послідовностей, що управляють, до інших систем, наприклад до систем мережевого управління або до МЕ.

Збереження. До категорії «збереження» відносяться два варіанти реагування:

- реєстрація події у БД;
- відтворення атаки в реальному масштабі часу.

Перший варіант широко поширений і в інших системах захисту. Для реалізації другого варіанту буває необхідно «пропустити» того, що атакує в мережу компанії і зафіксувати усі його дії. Це дозволяє адміністраторові безпеки потім відтворювати в реальному масштабі часу (чи із заданою швидкістю) усі дії, здійснені таким, що атакує, аналізувати «успішні» атаки і запобігати їм надалі, а також використати зібрані дані в процесі розгляду.

Активне реагування. До цієї категорії належать наступні варіанти реагування:

- блокування роботи того, що атакує;
- завершення сесії з атакуючим вузлом;
- управлінням мережевим устаткуванням і засобами захисту.

IDS можуть запропонувати такі конкретні варіанти реагування: блокування облікового запису атакуючого користувача, автоматичне завершення сесії з атакуючим вузлом, реконфігурація МЕ і маршрутизаторів і т. д. Ця категорія механізмів реагування, з одного боку, досить ефективна, а з іншого боку, вимагає акуратного використання, оскільки неправильне застосування може привести до порушення працездатності усій КІС.

Лекція 15 ЗАХИСТ ВІД ВІРУСІВ

Комп'ютерний вірус — це своєрідне явище, що виникло в процесі розвитку комп'ютерної техніки і ІТ. Суть його полягає в тому, що програми віруси мають властивості, властиві живим організмам, — вони народжуються, розмножуються і помирають. Термін «комп'ютерний вірус» уперше використав співробітник Університету Південної Каліфорнії Фред Коен в 1984 р. на 7-й конференції з безпеки інформації, що проходила в США. Цим терміном був названий шкідливий фрагмент програмного коду. Звичайно, це була усього лише метафора. Фрагмент програмного коду схожий на справжній вірус не більше, ніж людина на робота. Проте це один з тих окремих випадків, коли значення метафори ставало з часом менш метафоричним і більше буквальним.

Комп'ютерні віруси здатні робити практично те ж, що і справжні віруси: переходити з одного об'єкту на інший, змінювати способи атаки і мутувати. Проникнувши в ІС, комп'ютерний вірус може обмежитися нешкідливими візуальними або звуковими ефектами, але може і викликати втрату або спотворення даних, просочування особистої і конфіденційної інформації. У гіршому разі ІС, уражена вірусом, виявиться під повним контролем зловмисника. Сьогодні комп'ютерам довіряють рішення багатьох критичних завдань. Тому вихід з ладу ІС може мати дуже тяжкі наслідки, аж до людських жертв.

15.1. Комп'ютерні віруси і проблеми антивірусного захисту

Існує багато визначень комп'ютерного вірусу. Історично перше визначення було дане в 1984 р. Фредом Коеном: «Комп'ютерний вірус — це програма, яка може заражати інші програми, модифікуючи їх за допомогою включення в них своїй, можливо зміненій копії, причому остання зберігає здатність до подальшого розмноження«. Ключовими поняттями в цьому визначенні є здатність вірусу до саморозмноженню і здатність до модифікації обчислювального процесу. Вказані властивості комп'ютерного вірусу аналогічні паразитуванню біологічного вірусу в живій природі. Відтоді гострота проблеми вірусів багаторазово зросла — до кінця XX ст. у світі налічувалося більше 14 300 модифікацій вірусів.

Нині під комп'ютерним вірусом прийнято розуміти програмний код, що має наступні властивості:

- здатністю до створення власних копій, не обов'язково співпадаючих з оригіналом, але що мають властивості оригіналу (самовідтворення);
- наявністю механізму, що забезпечує впровадження створюваних копій у виконувані об'єкти обчислювальної системи.

Слід зазначити, що ці властивості є необхідними, але не достатніми. Вказані властивості слід доповнити властивостями деструктивності і скритності дій цієї шкідливої програми в обчислювальному середовищі.

15.1.1. Класифікація комп'ютерних вірусів

На сьогодні відомі десятки тисяч різних комп'ютерних вірусів. Незважаючи на такий достаток, число типів вірусів, що відрізняються один від одного механізмом поширення і принципом дії, досить обмежено. Існують і комбіновані

віруси, які можна віднести одночасно до декількох типів. Віруси можна розділити на класи [38, 85]:

- по місцю існування;
- операційній системі (ОС);
- особливостям алгоритму роботи;
- деструктивним можливостям.

Основною і найбільш поширеною класифікацією комп'ютерних вірусів є класифікація за місцем існування, або по типах об'єктів комп'ютерної системи, в які

впроваджуються віруси (Рис. 15.1). По місцю існування комп'ютерні віруси можна розділити:

- на файлові;
- завантажувальні;
- макровіруси;
- мережеві.

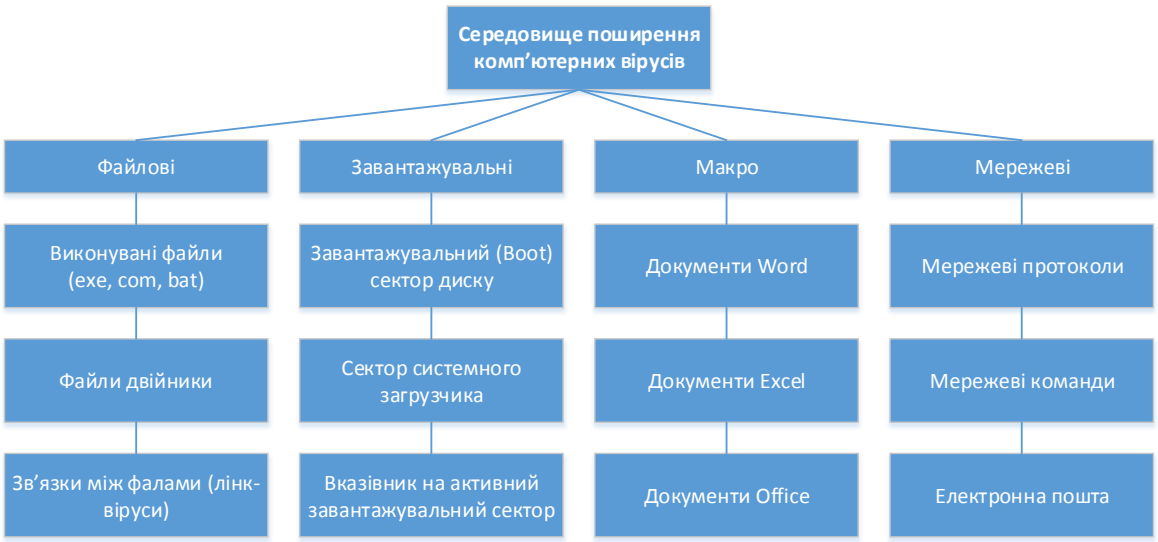

Рис. 15.1. Класифікація комп'ютерних вірусів за місцем існування

Файлові віруси або впроваджуються у виконувані файли (найбільш поширений тип вірусів) різними способами, або створюють файли двійники або використовують особливості організації файлової системи (link віруси).

Завантажувальні віруси записують себе або в завантажувальний сектор диска (bootсектор), або в сектор, системний завантажувач вінчестера (Master Boot Record), що містить. Завантажувальні віруси заміщають код програми, одержуючої управління при завантаженні системи. В результаті при перезавантаженні управління передається вірусу. При цьому оригінальний bootсектор зазвичай переноситься в інший сектор диска. Іноді завантажувальні віруси називають бутовими вірусами.

Макровіруси заражають макропрограми і файли документів сучасних систем обробки інформації, зокрема файли документи і електронні таблиці популярних редакторів Microsoft Word, Microsoft Excel та ін. Для розмноження макровіруси використовують можливості макромов і при їх допомозі переносять себе з одного зараженого файлу в інші. Віруси цього типу отримують управління при відкритті

зараженого файлу і інфікують файли, до яких згодом йде звернення з відповідного офісного застосування.

Мережеві віруси використовують для свого поширення протоколи або команди комп'ютерних мереж і електронної пошти. Іноді мережеві віруси називають програмами типу «черв'як». Мережеві черв'яки підрозділяються на Internetчерви (поширюються по Internet), LANчерви (поширюються по локальній мережі), IRCчерви Internet Relay Chat (поширюються через чати). Існують також змішані типи, які поєднують в собі відразу декілька технологій.

Існують багато комбінованих типів комп'ютерних вірусів, наприклад, відомий мережевий макровірус, який заражає редаговані документи, а також розсилає свої копії по електронній пошті. В якості іншого прикладу вірусів комбінованого типу можна вказати файловозагрузочні віруси, що заражають як файли, так і завантажувальні сектори дисків. Такі віруси мають ускладнений алгоритм роботи і застосовують своєрідні методи проникнення в систему.

Іншою ознакою ділення комп'ютерних вірусів на класи є операційна система, об'єкти якої піддаються зараженню. Кожен файловий або мережевий вірус заражає файли однієї або декількох ОС — DOS, Windows XP і т. д. Макровіруси заражають файли форматів Word, Excel, Microsoft Office. На певні формати розташування системних даних в завантажувальних секторах дисків також орієнтовані завантажувальні віруси.

Природно, ці схеми класифікації не є єдино можливими, існують багато різних схем типізації вірусів. Проте обмежимося доки класифікацією комп'ютерних вірусів за місцем існування, оскільки вона є базовою, і перейдемо до розгляду загальних принципів функціонування вірусів. Аналіз основних етапів «життєвого циклу» цих шкідливих програм дозволяє виділити їх різні ознаки і особливості, які можуть бути покладені в основу додаткових класифікацій.

15.1.2. Життєвий цикл вірусів

Як і у будь-якої програми, у комп'ютерних вірусів можна виділити дві основні стадії життєвого циклу — зберігання і виконання.

Стадія зберігання відповідає періоду, коли вірус просто зберігається на диску спільно з об'єктом, в який він впроваджений. На цій стадії вірус є найуразливішим з боку антивірусного ПЗ, оскільки він не активний і не може контролювати роботу ОС з метою самозахисту.

Деякі віруси на цій стадії використовують механізми захисту свого коду від виявлення. Найбільш поширеним способом захисту є шифрування більшої частини тіла вірусу. Його використання спільне з механізмами мутації коду (про це йде мова нижче) робить неможливим виділення сигнатур — стійких характеристичних фрагментів коду вірусів.

Стадія виконання комп'ютерних вірусів, як правило, включає п'ять етапів:

1) завантаження вірусу в пам'ять;
2) пошук жертви;
3) зараження знайденої жертви;
4) виконання деструктивних функцій;
5) передача управління програмі носію вірусу.

Розглянемо ці етапи детальніше [38, 70].

1. Завантаження вірусу. Завантаження вірусу в пам'ять здійснюється ОС одночасно із завантаженням виконуваного об'єкту, в який вірус впроваджений. Наприклад, якщо користувач запустив на виконання програмний файл, що містить вірус, то, очевидно, вірусний код буде завантажений в пам'ять як частину цього файлу. У простому випадку процес завантаження вірусу є не що інше, як копіювання з диска в оперативну пам'ять, супроводжуване іноді налаштуванням адрес, після чого відбувається передача управління коду тіла вірусу. Ці дії виконуються ОС, а сам вірус знаходиться в пасивному стані. У складніших ситуаціях вірус може після отримання управління виконувати додаткові дії, які необхідні для його функціонування. У зв'язку з цим розглядаються два аспекти.

Перший аспект пов'язаний з максимальним ускладненням процедури виявлення вірусів. Для забезпечення захисту на стадії зберігання деякі віруси використовують досить складні алгоритми. До таких ускладнень можна віднести шифрування основного тіла вірусу. Проте використання тільки шифрування є півзаходом, оскільки у відкритому виді повинна зберігатися та частина вірусу, яка забезпечує розшифрування вірусу на стадії завантаження. Для уникнення подібної ситуації розробники вірусів використовують механізми «мутацій» коду того, що розшифровує. Суть цього методу полягає в тому, що при впровадженні в об'єкт копії вірусу частина її коду, що відноситься до того, що розшифровує, модифікується так, щоб виникли текстуальні відмінності з оригіналом, але результати роботи залишилися незмінними. Зазвичай застосовують наступні прийоми модифікації коду:

- зміна порядку незалежних інструкцій;
- заміну деяких інструкцій на еквівалентні по результату роботи;
- заміну використовуваних в інструкціях регістрів на інші;
- введення випадковим чином зашумляючих інструкцій.

Віруси, що використовують подібні механізми мутації коду дістали назву поліморфних вірусів. При спільному використанні механізмів шифрування і мутації впроваджувана копія вірусу виявиться відмінною від оригіналу, оскільки одна її частина буде змінена, а інша виявиться зашифрованою на ключі, згенерованому спеціально для цієї копії вірусу. А це істотно ускладнює виявлення вірусу в обчислювальній системі.

Поліморфні віруси (polymorphic) — це віруси, що важко виявляються, не мають сигнатур, т. е. що не містять жодної постійної ділянки коду. У більшості випадків два зразки одного і того ж поліморфного вірусу не матимуть жодного збігу. Поліморфізм зустрічається у вірусах усіх типів — файлових, завантажувальних і макровірусах.

Додаткові дії, які виконують поліморфні віруси на етапі завантаження, полягають в розшифровці основного тіла вірусу.

При використанні стелсалгоритмов віруси можуть повністю або частково приховати себе в системі. Найбільш поширений стелс алгоритм здійснює перехоплення системних запитів з метою контролю дій ОС. Віруси, використовуючі стелс алгоритми, називаються стелс вірусами.

Стелс віруси (Stealth) здатні приховувати свою присутність в системі і уникати виявлення антивірусними програмами. Ці віруси можуть перехоплювати запити ОС на читання/запис заражених файлів, при цьому вони або тимчасово

лікують ці файли, або «підставляють» замість себе незаражені ділянки інформації, емулючи «чистоту» заражених файлів.

У разі макровірусів найбільш популярним способом являється заборона викликів меню перегляду макросів. Одним з перших файлових стелсвірусів був вірус «Frodo», першим завантажувальним стелсвірусом був вірус «Brain».

Нерідко у вірусах використовуються різні нестандартні прийоми з метою глибше сховатися в ядрі ОС, або захистити від виявлення свою резидентну копію, або утруднити лікування від вірусу і т. п.

Другий аспект пов'язаний з так званими резидентними вірусами. Оскільки вірус і об'єкт, в який він впроваджений, є для ОС єдиним цілим, то після завантаження вони розташовуються, природно, в єдиному адресному просторі. Після завершення роботи об'єкту він вивантажується з оперативної пам'яті, при цьому одночасно вивантажується і вірус, переходячи в пасивну стадію зберігання. Проте деякі типи вірусів здатні зберігатися в пам'яті і залишатися активними після закінчення роботи вірусоносія. Ці віруси дістали назву резидентних.

Резидентні віруси при інфікуванні комп'ютера залишають в оперативній пам'яті свою резидентну частину, яка потім перехоплює звернення ОС до об'єктів зараження і впроваджується в них. Резидентні віруси знаходяться в пам'яті і є активними аж до виключення комп'ютера або перезавантаження ОС.

Резидентними можна рахувати макровіруси, оскільки для більшості з них виконуються основні вимоги — постійна присутність в пам'яті комп'ютера на увесь час роботи зараженого редактора і перехоплення функцій, використовуваних при роботі з документами. При цьому роль ОС бере на себе редактор, а поняття «Перезавантаження операційної системи» трактується як вихід з редактора.

Нерезидентні віруси не заражають пам'ять комп'ютера і зберігають активність обмежений час. Деякі віруси залишають в оперативній пам'яті невеликі резидентні програми, які не поширюють вірус. Такі віруси вважаються нерезидентними.

Слід зазначити, що ділення вірусів на резидентні і нерезидентні справедливо в основному для файлових вірусів. Завантажувальні віруси, як і макровіруси, відносяться до резидентних вірусів.

2. Пошук жертви. За способом пошуку жертви віруси можна розділити два два класи.

До першого класу відносяться віруси, що здійснюють «активний» пошук з використанням функцій ОС. Прикладом є файлові віруси, що використовують механізм пошуку виконуваних файлів в поточному каталозі.

Другий клас складають віруси, що реалізовують «пасивний» механізм пошуку, т. е. віруси, що розставляють «пастки» для програмних файлів. Як правило, файлові віруси влаштовують такі пастки шляхом перехоплення функції Exec ОС, а макровіруси — за допомогою перехоплення команд типу Save as з меню File.

3. Зараження жертви. У простому випадку зараження є самокопирование коду вірусу у вибраний в якості жертви об'єкт. Класифікація вірусів на цьому етапі пов'язана з аналізом особливостей цього копіювання і способів модифікації об'єктів, що заражаються.

Особливості зараження файловими вірусами. За способом інфікування жертви віруси можна розділити на два класи.

До першого класу відносяться віруси, які не впроваджують свій код безпосередньо в програмний файл, а змінюють ім'я файлу і створюють новий, такий, що містить тіло вірусу.

Другий клас складають віруси, що впроваджуються безпосередньо у файлижертви. Вони характеризуються місцем впровадження. Можливі наступні варіанти.

Впровадження в початок файлу. Цей спосіб є найбільш зручним для COMфайлів MSDOS, оскільки цей формат не передбачає наявність службових заголовків. При впровадженні цим способом віруси можуть або робити конкатенацію власного коду і коду програми жертви, або переписувати початковий фрагмент файлу в кінець, звільняючи місце для себе.

Впровадження в кінець файлу. Це — найбільш поширений тип впровадження. Передача управління коду вірусів забезпечується модифікацією перших команд програми (COM) або заголовка файлу (EXE).

Впровадження в середину файлу. Як правило, цей спосіб використовується вірусами стосовно файлів із заздалегідь відомою структурою (наприклад, до файлу COMMAND.COM) або ж до файлів, що містять послідовність байтів з однаковими значеннями, довжина якої достатня для розміщення вірусу. У другому випадку віруси архівують знайдену послідовність і заміщають власним кодом. Окрім цього віруси можуть впроваджуватися в середину файлу, звільняючи собі місце шляхом перенесення фрагментів коду програми в кінець файлу або ж «розсовуючи» файл.

Особливості зараження завантажувальними вірусами визначаються особливостями об'єктів, в які вони впроваджуються, — завантажувальними секторами гнучких і жорстких дисків і головним завантажувальним записом (MBR) жорстких дисків. Основною проблемою є обмежений розмір цих об'єктів. У зв'язку з цим вірусам необхідно зберегти на диску ту свою частину, яка не уміщалася на місці жертви, а також перенести оригінальний код інфікованого завантажувача. Існують різні способи рішення цієї задачі. Нижче наводиться класифікація, запропонована Е. Касперским [38, 85].

Використовуються псевдозбійні сектори. Вірус переносить необхідний код у вільні сектори диска і позначає їх як збійні, захищаючи тим самим себе і завантажувач від перезапису.

Використовуються рідко вживані сектори у кінці розділу. Вірус переносить необхідний код в ці вільні сектори у кінці диска. З точки зору ОС ці сектори виглядають як вільні.

Використовуються зарезервовані області розділів. Вірус переносить необхідний код в області диска, зарезервовані під потреби ОС, а тому невживані.

Короткі віруси можуть уміщатися в один сектор завантажувача і повністю узяти на себе функції MBR або завантажувального сектора.

Особливості зараження макровірусами. Процес зараження зводиться до збереження вірусного макрокоду у вибраному документежертве. Для деяких систем обробки інформації це зробити не просто, оскільки формат файлів документів може не передбачати можливість збереження макропрограм. У якості прикладу приведемо Microsoft Word 6.0. Збереження макрокоду для цієї системи можливе тільки у файлах шаблонів (що мають за умовчанням розширення .DOT). Тому для свого збереження вірус повинен контролювати обробку команди Save as з меню File, яка викликається всякий раз, коли відбувається перше збереження

документу на диск. Цей контроль потрібний, щоб у момент збереження змінити тип файла-документа (що має за умовчанням розширення .DOC) на тип файлашаблона. В цьому випадку на диску виявляться і макрокод вірусу, і вміст документу.

Окрім простого копіювання коду вірусу в об'єкт, що заражається, на цьому етапі можуть використовуватися складніші алгоритми, що забезпечують захист вірусу на стадії зберігання. Таких вірусів належать описані вище поліморфні віруси.

4. Виконання деструктивних функцій. Віруси можуть виконувати окрім самокопіювання деструктивні функції.

По деструктивних можливостях віруси можна розділити на нешкідливі, безпечні, небезпечні і дуже небезпечні [85].

Нешкідливі віруси — це віруси, в яких реалізований тільки механізм самораспространения. Вони не завдають шкоди системі, за винятком витрати вільної пам'яті на диску в результаті свого поширення.

Безпечні віруси — це віруси, присутність яких в системі пов'язана з різними ефектами (звуковими, відео) і зменшенням вільної пам'яті на диску, але які не завдають шкоди програмам і даним.

Небезпечні віруси — це віруси, які можуть привести до серйозних збоїв в роботі комп'ютера. Наслідком збою може стати руйнування програм і даних.

Дуже небезпечні віруси — це віруси, в алгоритм роботи яких свідомо закладені процедури, що безпосередньо призводять до руйнувань програм і даних, а також до стирання інформації, записаної в системних областях пам'яті і необхідної для роботи комп'ютера.

На «міру небезпеки» вірусів робить істотний вплив те середовище, під управлінням якої віруси працюють.

Так, віруси, створені для роботи в MSDOS, мають практично необмежені потенційні можливості.

Поширення вірусів під управлінням Windows NT/2000 обмежується розвиненою системою розмежування доступу.

Можливості макровірусів безпосередньо визначаються можливостями макромів, на яких вони написані. Зокрема, мова Word Basic дозволяє створити потужні макровіруси, здатні причинити користувачам серйозні неприємності.

Доповнюючи цю класифікацію, можна відмітити також ділення вірусів на віруси, що завдають шкоди системі взагалі, і віруси, призначені для цілеспрямованих атак на певні об'єкти.

5. Передача управління програмі носію вірусу. Тут слід вказати на ділення вірусів на ті, що руйнують і неруйнівні.

Руйнівні віруси не піклуються про збереження працездатності інфікованих програм, тому для них цей етап функціонування відсутній.

Для неруйнівних вірусів цей етап пов'язаний з відновленням в пам'яті програми в тому вигляді, в якому вона повинна коректно виконуватися, і передачею управління програмі носію вірусу.

Шкідливі програми інших типів

Окрім вірусів прийнято виділяти ще декілька видів шкідливих програм. Це троянські програми, логічні бомби, хакерські утиліти прихованого адміністрування видалених комп'ютерів, програми, що крадуть паролі доступу до ресурсів Інтернет і іншу конфіденційну інформацію. Чіткого розділення між ними не існує: троянські

програми можуть містити віруси, у віруси можуть бути вбудовані логічні бомби і т. д.

Троянські програми не розмножуються і не розсилаються самі. Зовні вони виглядають абсолютно нешкідливо і навіть пропонують корисні функції. Але коли користувач завантажить таку програму у свій комп'ютер і запустить її, вона може непомітно виконувати шкідливі функції. Найчастіше троянські програми використовуються для первинного поширення вірусів, для діставання видаленого доступу до комп'ютера через Інтернет, крадіжки даних або їх знищення.

Логічною бомбою називається програма або її окремі модулі, які за певних умов виконують шкідливі дії. Логічна бомба може, наприклад, спрацювати після досягнення певної дати або тоді, коли у БД з'явиться або зникне запис, і т. п. Така бомба може бути вбудована у віруси, троянські програми і навіть в звичайні програми.

15.1.3. Основні канали поширення вірусів і інших шкідливих програм

Для того, щоб створити ефективну систему антивірусною зашиті комп'ютерів і корпоративних мереж, необхідно чітко уявляти собі, звідки загрожує небезпека. Віруси знаходять самі різні канали поширення, причому до старих способів постійно додаються нові.

Класичні способи поширення

Файлові віруси поширюються разом з файлами програм в результаті обміну дискетами і програмами, завантаження програм з мережевих каталогів, з Web або Лрсерверов. Завантажувальні віруси потрапляють на комп'ютер, коли користувач забуває заражену дискету в дисководі, а потім перезавантажує ОС. Завантажувальний вірус також може бути занесений на комп'ютер вірусами інших типів. Макрокомандні віруси поширюються в результаті обміну зараженими файлами офісних документів, такими як файли Microsoft Word, Excel, Access.

Якщо заражений комп'ютер підключений до локальної мережі, вірус легко може виявитися на дисках файлсервера, а звідти через каталоги, доступні для запису, потрапити на усі інші комп'ютери мережі. Так починається вірусна епідемія. Системному адміністраторові слід пам'ятати, що вірус має в мережі такі ж права, що і користувач, на комп'ютер якого цей вірус пробрався. Тому він може потрапити в усі мережеві каталоги, доступні користувачеві. Якщо ж вірус завівся на робочій станції адміністратора мережі, наслідки можуть бути дуже важкими.

Електронна пошта

Нині глобальна мережа Internet є основним джерелом вірусів. Велике число заражень вірусами відбувається при обміні листами по електронній пошті у форматах Microsoft Word. Електронна пошта служить каналом поширення макрокомандних вірусів, оскільки разом з повідомленнями часто вирушають офісні документи.

Зараження вірусами можуть здійснюватися як ненавмисно, так і по злому наміру. Наприклад, користувач зараженого макровірусом редактора, сам того не підозрюючи, може розсилати заражені листи адресатам, які у свою чергу відправляють нові заражені листи і т. д. З іншого боку, зловмисник може навмисно послати по електронній пошті разом з вкладеним файлом виконуваний модуль вірусної або троянської програми, шкідливий програмний сценарій Visual Basic

Script, заражену або троянську програму збереження екрану монітора, словом — будь-який небезпечний програмний код.

Розповсюджувачі вірусів часто користуються для маскування тим фактом, що діалогова оболонка Microsoft Windows за умовчанням не відображає розширення зареєстрованих файлів. Наприклад, файл з ім'ям FreeCreditCard.txt.exe, буде показаний користувачеві як FreeCreditCard.txt. Якщо користувач спробує відкрити такий файл, буде запущена шкідлива програма.

Повідомлення електронної пошти часто приходять у вигляді документів HTML, які можуть включати посилання на елементи управління ActiveX, аплети Java і інші активні компоненти. Изза помилок в поштових клієнтах зловмисники можуть скористатися такими активними компонентами для впровадження вірусів і троянських програм на комп'ютери користувачів. При отриманні повідомлення у форматі HTML поштовий клієнт показує його вміст у своєму вікні. Якщо повідомлення містить шкідливі активні компоненти, вони відразу ж запускаються і виконують закладені в них функції. Найчастіше у такий спосіб поширюються троянські програми і черв'яки.

Троянські Webсайти

Користувачі можуть «отримати» вірус або троянську програму під час простого серфінгу сайтів Інтернету, відвідавши троянський Web-сайт. Помилки у браузерах користувачів частенько призводять до того, що активні компоненти троянських Web-сайтів (елементи управління ActiveX або аплети Java) впроваджують на комп'ютери користувачів шкідливі програми. Тут використовується той же самий механізм, що і при отриманні повідомлень електронної пошти у форматі HTML. Але зараження відбувається непомітно: активні компоненти Web-сторінок можуть зовні ніяк себе не проявляти. Запрошення відвідати троянський сайт користувач може отримати в звичайному електронному листі.

Локальні мережі

Локальні мережі також є шляхом швидкого зараження. Якщо не приймати необхідних заходів захисту, то заражена робоча станція при вході в локальну мережу заражає один або декілька службових файлів на сервері. В якості таких файлів можуть виступати службовий файл LOGIN.COM, Exceltаблиці і стандартні документишаблони, вживані у фірмі. Користувачі при вході в цю мережу запускають заражені файли з сервера, і в результаті вірус дістає доступ на комп'ютери користувачів.

Інші канали поширення шкідливих програм

Одним з серйозних каналів поширення вірусів є піратські копії ПЗ. Часто нелегальні копії на дискетах і CDдисках містять файли, заражені різноманітними типами вірусів. До джерел поширення вірусів слід також віднести електронні конференції і файлсервери ftp і BBS. Часто автори вірусів закладають заражені файли відразу на декілька файлсерверів ftp/BBS або розсилають одночасно по декількох електронних конференціях, причому заражені файли зазвичай маскують під нові версії програмних продуктів і навіть антивірусів. Комп'ютери, встановлені в учбових закладах і Інтернетцентрах і працюючі в режимі загального користування, також можуть легко виявитися джерелами поширення вірусів. Якщо один з таких комп'ютерів виявився зараженим вірусом з дискети чергового

користувача, тоді дискети і усіх інших користувачів, працюючих на цьому комп'ютері, виявляться зараженими.

У міру розвитку комп'ютерних технологій удосконалюються і комп'ютерні віруси, пристосовуючись до нових для себе сфер мешкання. У будь-який момент може з'явитися комп'ютерний вірус, троянська програма або «черв'як» нового, невідомого раніше типу, або відомого типу, але націленого на нове комп'ютерне устаткування. Нові віруси можуть використати невідомі або не існуючі раніше канали поширення, а також нові технології впровадження в комп'ютерні системи. Щоб виключити загрозу вірусного зараження, системний адміністратор корпоративної мережі повинен впроваджувати методики антивірусного захисту і постійно відстежувати новини у світі комп'ютерних вірусів.

15.2. Антивірусні програми і комплекси

Для захисту від комп'ютерних вірусів можуть використовуватися:

- загальні методи і засоби захисту інформації;
- спеціалізовані програми для захисту від вірусів;
- профілактичні заходи, що дозволяють зменшити вірогідність зараження вірусами.

Загальні засоби захисту інформації корисні не лише для захисту від вірусів. Вони використовуються також як страховка від фізичного псування дисків, неправильно працюючих програм або помилкових дій користувача. Існують дві основні різновиди цих засобів:

- засоби копіювання інформації (застосовуються для створення копій файлів і системних областей дисків);
- засоби розмежування доступу (запобігають несанкціонованому використанню інформації, зокрема забезпечують захист від змін програм і даних вірусами, неправильно працюючими програмами і помилковими діями користувачів).

При зараженні комп'ютера вірусом важливо його виявити. До зовнішніх ознак прояву діяльності вірусів можна віднести наступні:

- висновок на екран непередбачених повідомлень або зображень;
- подання непередбачених звукових сигналів;
- зміна дати і часу модифікації файлів;
- зникнення файлів і каталогів або спотворення їх вмісту;
- часті зависання і збої в роботі комп'ютера;
- повільна робота комп'ютера;
- неможливість завантаження ОС;
- істотне зменшення розміру вільної оперативної пам'яті;
- припинення роботи або неправильна робота раніше успішно функціонуючих програм;
- зміна розмірів файлів;
- несподіване значне збільшення кількості файлів на диску.

Проте слід зауважити, що перелічені вище явища необов'язково викликаються діями вірусу, вони можуть бути слідством і інших причин. Тому правильна діагностика стану комп'ютера завжди ускладнена і зазвичай вимагає залучення спеціалізованих програм.

Антивірусні програми

Для виявлення і захисту від комп'ютерних вірусів розроблені декілька видів спеціальних програм, які дозволяють виявляти і знищувати комп'ютерні віруси. Такі програми називаються антивірусними. Практично усі антивірусні програми забезпечують автоматичне відновлення заражених програм і завантажувальних секторів. Антивірусні програми використовують різні методи виявлення вірусів.

Методи виявлення вірусів

До основних методів виявлення комп'ютерних вірусів можна віднести наступні:

- метод порівняння з еталоном;
- евристичний аналіз;
- антивірусний моніторинг;
- метод виявлення змін;
- вбудовування антивірусів в BIOS комп'ютера та ін. [85].

Метод порівняння з еталоном. Найпростіший метод виявлення полягає в тому, що для пошуку відомих вірусів використовуються так звані маски. Маскою вірусу є деяка постійна послідовність кода, специфічна для цього конкретного вірусу. Антивірусна програма послідовно переглядає (сканує) файли, що перевіряються, в пошуку масок відомих вірусів. Антивірусні сканери здатні знайти тільки вже відомі віруси, для яких визначена маска.

Якщо вірус не містить постійної маски або довжина цієї маски недостатньо велика, то використовуються інші методи. Застосування простих сканерів не захищає комп'ютер від проникнення нових вірусів. Для вірусів, що шифруються і поліморфних, здатних повністю змінювати свій код при зараженні нової програми або завантажувального сектора, неможливо виділити маску, тому антивірусні сканери їх не виявляють.

Евристичний аналіз. Для того, щоб розмножуватися, комп'ютерний вірус повинен здійснювати якісь конкретні дії: копіювання в пам'ять, запис в сектори і т. д. Евристичний аналізатор (який є частиною антивірусного ядра) містить список таких дій і перевіряє програми і завантажувальні сектори дисків і дискет, намагаючись виявити в них код, характерний для вірусів. Евристичний аналізатор може виявити, наприклад, що програма, що перевіряється, встановлює резидентний модуль в пам'яті або записує дані в здійснимий файл програми. Виявивши заражений файл, аналізатор зазвичай виводить повідомлення на екрані монітора і робить запис у власному або системному журналі. Залежно від налаштувань, антивірус може також направляти повідомлення про виявлений вірус адміністраторові мережі. Евристичний аналіз дозволяє виявляти невідомі раніше віруси. Перший евристичний аналізатор з'явився на початку 1990х рр. Практично усі сучасні антивірусні програми реалізують власні методи евристичного аналізу. Як приклад такої програми можна вказати сканер McAfiee VirusScan.

Антивірусний моніторинг. Суть цього методу полягає в тому, що в пам'яті комп'ютера постійно знаходиться антивірусна програма, що здійснює моніторинг усіх підозрілих дій, що виконуються іншими програмами. Антивірусний моніторинг дозволяє перевіряти усі програми, що запускаються, створювані документи, файли програм і документів, отримані через Інтернет або скопійовані на жорсткий диск з дискети або компакт-диск диска, що відкриваються і зберігаються. Антивірусний монітор повідомить користувача, якщо програма

спробує виконати потенційно небезпечну дію. Приклад такої програми — сторож Spider Guard, який входить в комплект сканера Doctor Web і виконує функції антивірусного монітора.

Метод виявлення змін. При реалізації цього методу антивірусні програми, що називаються ревізорами диска, запамятовують заздалегідь характеристики усіх областей диска, які можуть піддатися нападу, а потім періодично перевіряють їх. Заражаючи комп'ютер, вірус змінює вміст жорсткого диска: наприклад, дописує свій код у файл програми або документу, додає виклик програмивіруса у файл AUTOEXEC.BAT, змінює завантажувальний сектор, створює файлспутник. При зіставленні значень характеристик областей диска антивірусна програма може виявити зміни, зроблені як відомим, так і невідомим вірусом.

Вбудовування антивірусів в BIOS комп'ютера. У системні плати комп'ютерів вбудовують прості засоби захисту від вірусів. Ці засоби дозволяють контролювати усі звернення до головного завантажувального запису жорстких дисків, а також до завантажувальних секторів дисків і дискет. Якщо програма намагається змінити вміст завантажувальних секторів, спрацьовує захист, і користувач отримує відповідне попередження. Проте цей захист не дуже надійний. Відомі віруси, які намагаються відключити антивірусний контроль BIOS, змінюючи деякі осередки в енергонезалежній пам'яті (CMOSпамяти) комп'ютера.

Види антивірусних програм

Розрізняють наступні види антивірусних програм [85]:

- програми фаги (сканери);
- програми ревізори (CRC-сканери);
- програми блокувальники;
- програми імунізатори.

Програми фаги (сканери) використовують для виявлення вірусів метод порівняння з еталоном, метод евристичного аналізу і деякі інші методи. Програми фаги здійснюють пошук характерної для конкретного вірусу маски шляхом сканування в оперативній пам'яті і у файлах і при виявленні видають відповідне повідомлення. Програмифаги не лише знаходять заражені вірусами файли, але і «лікують» їх, т. е. видаляють з файлу тіло Програми-віруса, повертаючи файли в початковий стан. На початку роботи Програмифаги сканують оперативну пам'ять, виявляють віруси і знищують їх і тільки тоді переходять до «лікування» файлів. Серед фагов виділяють полифаги — Програмифаги, призначені для пошуку і знищення великого числа вірусів.

Програмифаги можна розділити на дві категорії — універсальні і спеціалізовані сканери. Універсальні сканери розраховані на пошук і знешкодження усіх типів вірусів незалежно від ОС, на роботу в якій розрахований сканер. Спеціалізовані сканери призначені для знешкодження обмеженого числа вірусів або тільки одного їх класу, наприклад макровірусів. Спеціалізовані сканери, розраховані тільки на макровіруси, виявляються зручнішим і надійнішим рішенням для захисту систем документообігу в середовищах MS Word і MS Excel.

Програмифаги діляться також на резидентні монітори, що виробляють сканування «на льоту», і нерезидентні сканери, що забезпечують перевірку системи тільки за запитом. Резидентні монітори забезпечують надійніший захист системи, оскільки вони негайно реагують на появу вірусу, тоді як нерезидентний сканер здатний пізнати вірус тільки під час свого чергового запуску.

До достоїнств програмфагов усіх типів відноситься їх універсальність. До недоліків слід віднести відносно невелику швидкість пошуку вірусів і відносно великі розміри антивірусних баз.

Найбільш відомі Програмифаги: Aidstest, Scan, Norton AntiVirus, Doctor Web. Враховуючи, що постійно з'являються нові віруси, Програмифаги швидко застарівають, і потрібно регулярне оновлення версій.

Програмиревізори (CRC-сканери) використовують для пошуку вірусів метод виявлення змін. Принцип роботи CRC-сканерів заснований на підрахунку CRC-сумм (кодів циклічного контролю) для присутніх на диску файлів/системних секторів. Ці CRC-сумми, а також деяка інша інформація (довжини файлів, дати їх останньої модифікації та ін.) потім зберігаються у БД антивіруса. При подальшому запуску CRC-сканери звіряють дані, що містяться у БД, з реально підрахованими значеннями. Якщо інформація про файл, записана у БД, не співпадає з реальними значеннями, то CRC-сканери сигналізують про те, що файл був змінений або заражений вірусом. Як правило, порівняння станів роблять відразу після завантаження ОС.

CRC-сканери, використовуючі алгоритми антистелс, є досить потужним засобом проти вірусів: практично 100 % вірусів виявляються виявленими майже відразу після їх появи на комп'ютері. Проте у CRC-сканерів є недолік, що помітно знижує їх ефективність: вони не можуть визначити вірус в нових файлах (у електронній пошті, на дискетах, у файлах, відновлюваних з backup або при розпаковуванні файлів з архіву), оскільки в їх БД відсутня інформація про ці файли.

CRC-сканерів належить широко поширена в Росії програма ADinf (Advanced Diskinfoscope) і ревізор AVP Inspector. Разом з ADinf застосовується модуль ADinf Cure Module (ADinfExt), що лікує, який використовує зібрану раніше інформацію про файли для їх відновлення після поразки невідомими вірусами. До складу ревізора AVP Inspector також входить модуль, що лікує, здатний видаляти віруси.

Програми блокувальники реалізують метод антивірусного моніторингу. Антивірусні блокувальники — це резидентні програми, перехоплюючі «вірусонебезпечні» ситуації і що повідомляють про це користувачеві. До «вірусонебезпечним» ситуацій відносяться виклики, які характерні для вірусів в моменти їх розмноження (виклики на відкриття для запису у виконувані файли, запис в завантажувальні сектори дисків або MBR вінчестера, спроби програм залишитися резидентний і т. п.).

При спробі програми виконати вказані дії блокувальник посилає користувачеві повідомлення і пропонує заборонити відповідну дію. До достоїнств блокувальників відноситься їх здатність виявляти і зупиняти вірус на самій ранній стадії його розмноження, що буває особливо корисно у випадках, коли регулярно з'являється давно відомий вірус. Проте вони не «лікують» файли і диски. Для знищення вірусів вимагається застосовувати інші програми, наприклад фаги. До недоліків блокувальників можна віднести існування шляхів обходу їх захисту і їх «настирливість» (наприклад, вони постійно видають попередження про будь-яку спробу копіювання виконуваного файлу).

Слід зазначити, що створені антивірусні блокувальники, виконані у вигляді апаратних компонентів комп'ютера. Найбільш поширеною є вбудована в BIOS захист від запису в MBR вінчестера.

Програми імунізатори — це програми, що запобігають зараженню файлів. Імунізатори діляться на два типи: Імунізатори, що повідомляють про зараження, і Імунізатори, блокуючі зараження типом вірусу. Імунізатори першого типу зазвичай записуються в кінець файлів і при запуску файлу кожного разу перевіряють його на зміну. У таких імунізаторів є один серйозний недолік — вони не можуть виявити зараження стелс вірусом. Тому цей тип імунізаторов практично не використовуються нині.

Імунізатор другого типу захищає систему від поразки вірусом певного виду. Він модифікує програму або диск так, щоб це не відбивалося на їх роботі, вірус при цьому сприймає їх зараженими і тому не впроваджується. Такий тип імунізації не може бути універсальним, оскільки не можна імунізувати файли від усіх відомих вірусів. Проте в якості півзаходу подібні Імунізатори можуть цілком надійно захистити комп'ютер від нового невідомого вірусу аж до того моменту, коли він визначатиметься антивірусними сканерами.

Критерії якості антивірусної програми

Якість антивірусної програми можна оцінити за декількома критеріями [85]:

- надійність і зручність роботи — відсутність «зависань» антивіруса і інших технічних проблем, що вимагають від користувача спеціальної підготовки;
- якість виявлення вірусів усіх поширених типів, сканування усередині файл документ/таблиць (MS Word, Excel, Office), упакованих файлів, що архівуються; можливість лікування заражених об'єктів;
- існування версій антивіруса під усі популярні платформи (DOS, Windows, Novell NetWare, OS/2, Alpha, Linux і т. д.); наявність режимів сканування «за запитом» і «на льоту», існування серверних версій з можливістю адміністрування мережі;
- швидкість роботи і інші корисні особливості.

Надійність роботи антивіруса є найбільш важливим критерієм, оскільки навіть «абсолютний» антивірус може виявитися даремним, якщо він не в змозі довести процес сканування до кінця, т. е. «повисне» і не перевірить частину дисків і файлів і, в результаті, вірус залишиться непоміченим в системі.

Якість виявлення вірусів стоїть на наступному місці з цілком природної причини. Головний обов'язок антивірусних програм — виявляти 100 % вірусів і лікувати їх. При цьому антивірусна програма не повинна мати високого рівня неправдивих спрацьовувань.

Наступний по важливості критерій — багатоплатформеність антивіруса, оскільки тільки програма, розрахована на конкретну ОС, може повністю використати функції цієї системи. Моментальна і примусова перевірка файлів, що приходять на комп'ютер, і дискет, що вставляються, — це практично 100% я гарантія від зараження вірусом. Якщо в серверному варіанті антивіруса є присутньою можливість антивірусного адміністрування мережі, то його цінність ще більше зростає.

Швидкість роботи також є важливим критерієм якості антивірусної програми. У різних антивірусах використовуються різні алгоритми пошуку вірусів, один алгоритм може виявитися швидшим і якіснішим, інший — повільним і менш якісним.

Профілактичні заходи захисту

Своєчасне виявлення заражених вірусами файлів і дисків, повне знищення виявлених вірусів на кожному комп'ютері дозволяють уникнути поширення вірусної епідемії на інші комп'ютери. Абсолютно надійних програм, що гарантують виявлення і знищення будь-якого вірусу, не існує. Важливим методом боротьби з комп'ютерними вірусами є своєчасна профілактика. Щоб істотно зменшити вірогідність зараження вірусом і забезпечити надійне зберігання інформації на дисках, необхідно виконувати наступні заходи профілактики:

- застосовувати тільки ліцензійне ПЗ;
- оснастити комп'ютер сучасними антивірусними програмами і постійно поновлювати їх версії;
- завжди перевіряти дискети на наявність вірусів (запускаючи антивірусні програми свого комп'ютера) перед прочитуванням з них інформації, записаній на інших комп'ютерах;
- при перенесенні на свій комп'ютер файлів у виді, що архівується, перевіряти їх відразу ж після розархівування на жорсткому диску, обмежуючи область перевірки тільки знову записаними файлами;
- періодично перевіряти на наявність вірусів жорсткі диски комп'ютера, запускаючи антивірусні програми для тестування файлів, пам'яті і системних областей дисків із захищеної від запису дискети, заздалегідь завантаживши ОС із захищеної від запису системної дискети;
- завжди захищати свої дискети від запису при роботі на інших комп'ютерах, якщо на них не робитиметься запис інформації;
- обов'язково робити на дискетах архівні копії цінної для користувача інформації;
- не залишати в кишені дисковода А дискети при включенні або перезавантаженні ОС, щоб виключити зараження комп'ютера завантажувальними вірусами;
- використати антивірусні програми для вхідного контролю усіх виконуваних файлів, що отримуються з комп'ютерних мереж.

Антивірусні програмні комплекси

У кожного типу антивірусних програм є свої достоїнства і недоліки. Тільки комплексне використання декількох типів антивірусних програм може привести до прийнятного результату. Програмні засоби захисту є комплексом алгоритмів і програм, націлених на контроль і виключення проникнення несанкціонованої інформації.

Існує спектр програмних комплексів, призначених для профілактики зараження вірусом, виявлення і знищення вірусів [9]. Вони мають універсальність, гнучкість, адаптивність та ін.

15.3. Побудова системи антивірусного захисту корпоративної мережі

Проблема антивірусного захисту — одна з пріоритетних проблем безпеки корпоративних інформаційних ресурсів організації. Її актуальність пояснюється:

- лавиноподібним зростанням числа комп'ютерних вірусів;
- незадовільним станом антивірусного захисту в існуючих корпоративних комп'ютерних мережах. Сьогодні мережі компаній знаходяться в постійному розвитку. Проте разом з ним постійно росте і число точок проникнення

вірусів в корпоративні мережі Інтернет/интранет. Як правило, такими точками є: шлюзи і сервери Інтернет, сервери файлових додатків, сервери групової роботи і електронної пошти, робочі станції.

Для невеликих підприємств, що використовують до 10 вузлів, доцільні рішення по антивірусному захисту, що мають зручний графічний інтерфейс і допускають локальну конфігурацію без застосування централізованого управління. Для великих підприємств прийнятніше за систему антивірусного захисту з декількома консолями і менеджерами управління, підлеглими деякому єдиному загальному центру. Такі рішення дозволяють забезпечити оперативне централізоване управління локальними антивірусними клієнтами і дають можливість при необхідності інтегруватися з іншими рішеннями в області безпеки корпоративних мереж.

Лекція 16 МЕТОДИ УПРАВЛІННЯ ЗАСОБАМИ МЕРЕЖЕВОЇ БЕЗПЕКИ

Система інформаційної безпеки повинна захистити інформаційні ресурси мережі від найбільш поширених зовнішніх і внутрішніх атак, спрямованих на виведення із ладу серверів і знищення даних, від небажаного проникнення в локальні обчислювальні мережі через «діри» в ОС, від цілеспрямованого вторгнення в систему для отримання конфіденційної інформації.

Для успішного використання сучасних ІТ потрібне надійне і ефективне управління не лише самими мережами, але і засобами мережевої безпеки. І якщо раніше завдання полягало в управлінні окремими серверами, мережами і маршрутизаторами, то зараз вимагається забезпечити інформаційну безпеку корпоративних бізнес процесів. Усе це пред'являє жорсткі вимоги до управління засобами мережевої безпеки.

Найважливішим компонентом системи управління корпоративною мережею є система інформаційної безпеки. Ця система повинна:

- централізований і оперативно здійснювати дії, що управляють, на засоби мережевої безпеки;
- проводити регулярний аудит і моніторинг, що дають об'єктивну інформацію про стан інформаційної безпеки для ухвалення оперативних рішень.

16.1. Завдання управління системою мережевої безпеки

Сформулюємо основні завдання управління системою мережевої безпеки масштабу підприємства. Функціонально система управління засобами захисту інформації в розподіленій мережі масштабу підприємства повинна вирішувати наступні завдання:

- управління глобальною політикою безпеки (ГПБ) у рамках мережі підприємства, формування локальних політик безпеки (ЛПБ) окремих пристроїв і доведення ЛПБ до усіх облаштувань захисту інформації;
- управління конфігурацією об'єктів і суб'єктів доступу; включає управління складом, версіями, компонентами пристроїв і ПЗ захисту, а також управління патчами (patch), які служать для закриття дір, виявлених в поставлених продуктах забезпечення безпеки;
- надання сервісів захисту розподіленим прикладним системам, а також реєстрацію захищених застосувань і їх ресурсів. Застосування цієї групи повинні забезпечувати, передусім, інтерфейс (API) для забезпечення управління сервісами захисту з боку прикладних систем;
- управління криптозасобами, зокрема — ключове управління (ключова інфраструктура). Ключова інфраструктура повинна функціонувати у складі інфраструктурних (системотворних) служб;
- подієве протоколювання; включає налаштування видачі лігв на різні пристрої, управління рівнем деталізації лігв, управління складом подій, по яких ведеться протоколювання;
- аудит безпеки ІС; забезпечує отримання і оцінку об'єктивних даних про поточний стан захищеності ІС, іноді під аудитом безпеки розуміють аналіз лігв,

пошук порушників і дір в існуючій системі, проте ці функції покриваються, швидше, завданнями управління балками;

- моніторинг безпеки системи; забезпечує отримання інформації в реальному часі про стан, активності пристроїв і про події з контекстом безпеки, що відбуваються в пристроях, наприклад про потенційні атаки;
- забезпечення роботи спеціальних захищених застосувань, наприклад нотаріального нагляду за операціями, підтримка регламентних заходів (зміна ключів, паролів, облаштувань захисту, випуск смарт-карт та ін.);
- забезпечення роботи проектно-інвентаризаційної групи застосувань; ця група застосувань повинна здійснювати:
  - визначення точок установки засобів захисту в мережі підприємства;
  - облік вживаних засобів захисту;
  - контроль модульного складу засобів захисту;
  - контроль стану засобів захисту та ін.

Існує проблема комплексування і організації взаємодії традиційних систем управління мережами і систем управління засобами захисту інформації в мережі. Для вирішення цієї проблеми застосовуються два основні підходи.

Перший підхід полягає в інтеграції засобів мережевого або системного управління з механізмами управління засобів зашиті. Засоби мережевого і системного управління орієнтовані, в першу чергу, на управління мережею або ІС, т. е. підтримують традиційні дії і послуги: управління обліковими записами користувачів, управління ресурсами і подіями, маршрутизацію, продуктивність і т. п. Ряд компаній — Cisco Systems, Computer Associates, Hewlett Packard, Tivoli Systems — пішли шляхом інтеграції механізмів управління засобів захисту в традиційні системи управління мережами. Проте такі комплексні системи управління часто відрізняються високою вартістю і, крім того, деякі аспекти управління безпекою залишаються за межами уваги цих систем.

Другий підхід полягає у використанні засобів, призначених для вирішення тільки завдання управління безпекою. Наприклад, Open Security Manager (OSM) від Check Point Software Technologies дає можливість централізований управляти корпоративною політикою безпеки і інсталювати її на мережеві пристрої по усій компанії. Продукт OSM є одним з основних компонентів технології OPSEC (Open Platform for Secure Enterprise Connectivity), розробленою компанією Checkpoint, він створює інтерфейс для управління облаштуваннями мережевої безпеки різних виробників (наприклад, Cisco, Bay, 3Com).

16.2. Архітектура управління засобами мережевої безпеки

Для забезпечення безпеки інформаційних ресурсів підприємства засобу захисту інформації зазвичай розміщуються безпосередньо в корпоративній мережі. МЭ контролюють доступ до корпоративних ресурсів, відбиваючи атаки зловмисників ззовні, а шлюзи віртуальних приватних мереж (VPN) забезпечують конфіденційну передачу інформації через відкриті глобальні мережі, зокрема Інтернет. Для створення надійного ешелонованого захисту нині застосовуються також такі засоби безпеки, як системи виявлення вторгнень IDS (Intrusion Detection Systems), засоби контролю доступу за змістом інформації, антивірусні системи та ін.

Більшість КІС побудовані на основі програмних і апаратних засобів, що поставляються різними виробниками.

Кожен з цих засобів вимагає ретельної і специфічної конфігурації, що відбиває взаємозв'язки між користувачами і доступними їм ресурсами. Щоб забезпечити в гетерогенній КІС надійний захист інформації, потрібна раціонально організована система управління безпекою КІС, яка забезпечила б безпеку і правильне налаштування кожного компонента КІС, постійно відстежувала зміни, що відбуваються, встановлювала «латочки» на знайдені в системі проломи, контролювала роботу користувачів. Очевидно, що чим різнорідніше ІС, тим складніше забезпечити управління її безпекою.

16.2.1. Основні поняття

Досвід провідних підприємств-виробників засобів мережевої безпеки показує, що компанія зможе успішно реалізувати свою політику безпеки в розподіленій КІС, якщо управління безпекою буде централізованим і не залежатиме від використовуваних ОС і прикладних систем. Крім того, система реєстрації подій, що відбуваються в КІС (події НСД, зміна привілеїв користувачів і т. д.), має бути єдиною, щоб адміністратор зміг скласти повну картину змін, що відбуваються в КІС.

Для вирішення ряду завдань управління безпекою потрібно застосування єдиних вертикальних інфраструктур типу каталогу X. 500. Наприклад, політика мережевого доступу вимагає знання ідентифікаторів користувачів. Ця інформація потрібна і іншим застосуванням, наприклад в системі кадрового обліку, в системі одноразового доступу до застосувань (Single Sign - On) і т. д. Дублювання одних і тих же даних призводить до необхідності синхронізації, збільшення трудомісткості і можливої плутанини. Тому, щоб уникнути такого дублювання, часто використовують єдині вертикальні інфраструктури.

До таких вертикальних структур, використовуваних різними призначеними для користувача підсистемами, працюючими на різних рівнях OSI/ISO, відносяться:

- інфраструктури управління відкритими ключами PKI. Слід зазначити цікавий аспект, поки що не отримав широкого поширення, але важливий для управління. Цей

година в основному використовуються цифрові сертифікати у вигляді так званих «посвідчень особи» (identity certificates), але вже розвиваються і подекуди застосовуються цифрові сертифікати у вигляді так званих «вірчих грамот» (credential certificates); видаючи і відкликаючи такі «вірчі грамоти», можна гнучкіше управляти доступом;

- каталоги (наприклад, ідентифікаторів користувачів і інших відомостей про користувачів, необхідних в системах управління доступом); відмітимо, що каталоги часто використовуються не лише як сховища даних — в них також часто розташовуються політики доступу, сертифікати, списки доступу та ін.;
- системи аутентифікації (зазвичай RADIUS, сервери TACACS, TACACS+);

- системи подієвого протоколювання, моніторингу і аудиту. Слід зазначити, що ці системи не завжди вертикальні, часто спеціалізуються і працюють автономно в інтересах конкретних підсистем.

Концепція глобального управління безпекою, що дозволяє побудувати ефективну систему ієрархічного управління безпекою гетерогенної мережі компанії, розроблена компанією TrustWorks Systems [9]. Організація централізованого управління безпекою КІС заснована на наступних принципах:

- управління безпекою корпоративної мережі повинно здійснюватися на рівні ГПБ — набору правил безпеки для безлічі взаємодій між об'єктами корпоративної мережі, а також між об'єктами корпоративної мережі і зовнішніми об'єктами;
- ГПБ повинна відповідати бізнес-процесам компанії. Для цієї властивості безпеки об'єктів і необхідні сервіси безпеки мають бути описані з урахуванням їх бізнес-ролей в структурі компанії.
- для окремих засобів захисту формуються ЛПБ. Трансляція ЛПБ повинна здійснюватися автоматично на основі аналізу правил ГПБ і топології мережі, що захищається.

Враховуючи, що методологія централізованого управління мережевою безпекою досить повно відбиває сучасні тенденції розвитку технологій безпеки, розглянемо детальніше цю методологію і деякі аспекти її реалізації.

16.2.2. Концепція глобального управління безпекою

У основі централізованого управління безпекою КІС лежить концепція глобального управління безпекою GSM (Global Security Management). Концепція GSM дозволяє побудувати комплексну систему управління і захисту інформаційних ресурсів підприємства з наступними властивостями:

- управління усіма існуючими засобами захисту на базі політики безпеки підприємства, що забезпечує цілісність, несуперечність і повноту набору правил захисту для усіх ресурсів підприємства (об'єктів політики безпеки) і погоджене виконання політики безпеки засобами захисту, різними виробниками, що поставляються;
- визначення усіх інформаційних ресурсів підприємства через єдиний (розподілений) каталог середовища підприємства, який може актуалізуватися як за рахунок власних засобів опису ресурсів, так і за допомогою зв'язку з іншими каталогами підприємства (у тому числі по протоколу LDAP);
- централізоване, засноване на політиці безпеки (policy - based) управління локальними засобами захисту інформації;
- строга аутентифікація об'єктів політики в середовищі підприємства з використанням PKCS#11токенов і інфраструктури відкритих ключів PK1, включаючи можливість застосування додаткових локальних коштів аутентифікації LAS (по вибору споживача);
- розширені можливості адміністрування доступу до визначених в каталозі ресурсів підприємства або частин усього каталогу (з підтримкою понять груп користувачів, доменів, департаментів підприємства), управління ролями як набором прав доступу до ресурсів підприємства, введення в політику безпеки елементів непрямого визначення прав через атрибути прав доступу (credentials);

- забезпечення підзвітності (реєстрації усіх операцій взаємодій розподілених об'єктів системи в масштабах корпоративної мережі) і аудиту, моніторингу безпеки, тривожної сигналізації;
- інтеграція з системами загального управління, інфраструктурними системами безпеки (PKI, LAS, IDS).

У рамках цієї концепції управління, засноване на політиці безпеки, — PBM (Policy based management) — визначається як реалізація набору правил управління, сформульованих для бізнес-об'єктів підприємства, яка гарантує повноту охоплення бізнес-області об'єктами і несуперечність використовуваних правил управління.

Система управління GSM, орієнтована на управління безпекою підприємства на принципах PBM, задовольняє наступним вимогам:

- політика безпеки підприємства є логічно і семантично пов'язану, формовану, редаговану і аналізовану як єдине ціле структуру даних;
- політика безпеки підприємства визначається в єдиному контексті для усіх рівнів захисту як єдине ціле мережевої політики безпеки і політики безпеки інформаційних ресурсів підприємства;
- для полегшення адміністрування ресурсів і політики безпеки підприємства число параметрів політики мінімізується.

Для того, щоб мінімізувати число параметрів політики, використовуються наступні прийоми:

1) групові визначення об'єктів безпеки;
2) непрямі визначення, наприклад визначення на основі вірчих (credential) атрибутів;
3) мандатне управління доступом (на додаток до фіксованого доступу), коли рішення про доступ визначається на основі зіставлення рівня доступу, який має суб'єкт, і рівня конфіденційності (критичності) ресурсу, до якого здійснюється доступ.

Система управління GSM забезпечує різноманітні механізми аналізу політики безпеки за рахунок засобів багатокритерійної перевірки відповідності політики безпеці формальним моделям концепції безпеки підприємства.

Нижче наводиться концепція визначення ГПБ (GSP — Global Security Policy) мережі підприємства і опис побудованою на базі ГПБ системи управління безпекою (policy based security management).

16.2.3. Глобальна і локальна політики безпеки

Глобальна політика безпеки корпоративної мережі є кінцевою безліччю правил безпеки (Рис. 16.1), які описують параметри взаємодії об'єктів корпоративної мережі в контексті інформаційної безпеки:

- необхідний для з'єднання сервіс безпеки (правила обробки, захисту і фільтрації трафіку);
- напрям надання сервісу безпеці;
- правила аутентифікації об'єктів;
- правила обміну ключами;
- правила запису результатів подій безпеки в системний журнал;
- правила сигналізації про тривожні події та ін.

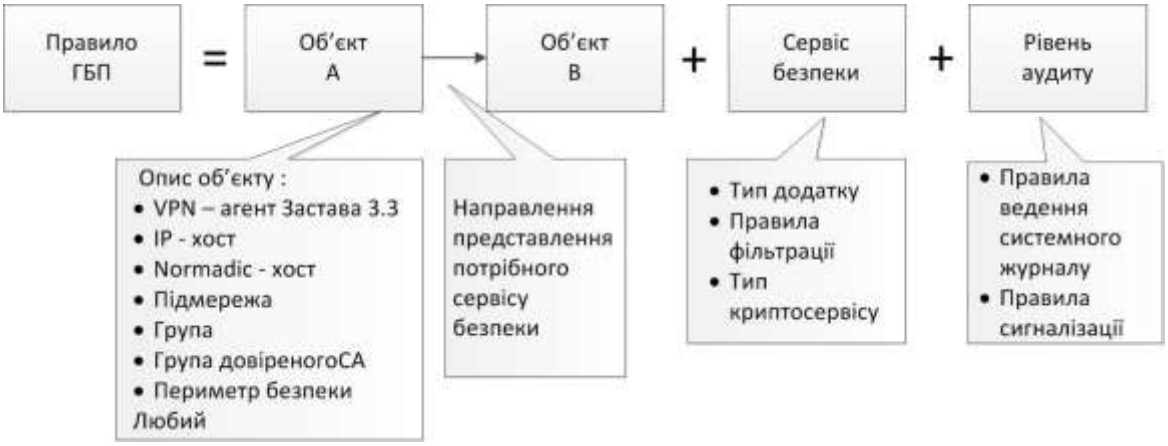

Рис. 16.1. Структура правила глобальної політики безпеки

При цьому об'єктами ГПБ можуть бути як окремі робочі станції і підмережі, так і групи об'єктів, які можуть включати цілі структурні підрозділи компанії (наприклад, відділ маркетингу або фінансовий департамент) або навіть окремі компанії (що входять, наприклад, в холдинг). Політика безпеки для кожного об'єкту в групі автоматично копіюється усім об'єктам групи.

Завдання захисту бізнес-об'єктів розподіленої корпоративної системи можна сформулювати в термінах правил, оскільки мережеву взаємодію можна представити як просту передачу інформації між суб'єктом Subj і об'єктом Obj доступу на основі деякого мережевого сервісу захисту SecSrv, налагодженого за допомогою параметрів P. В результаті глобальна політика безпеки підприємства представляється як набір правил виду

$$(\text{Subj, Obj, SecSrv } (P)).$$

При цьому відсутність правила для об'єкту Obj означає заборону будь-якого доступу до цьому Obj.

Для простоти визначення цілей безпеки підприємства в GSM передбачений два типи об'єктів, що виступають в якості Subj і Obj. Це — користувач (U) і ресурс (R).

Ресурс R може бути інформаційним (IR) або мережевим (NR).

Користувач і ресурс можуть виступати у будь-якій з форм агрегації, підтримуваних в системі: групи, домени, ролі, департаменти, розділи каталогу.

Приклад: правило $(U, IR, S1)$ є правилом захисту 64, забезпечуване при доступі користувача U до інформаційного ресурсу IR. Правило (IR1, IR2, S2) означає дозвіл мережевої взаємодії двох інформаційних модулів (програм) з необхідністю забезпечення властивостей захисту S2.

Політика за умовчанням для доступу до будь-якого об'єкту корпоративної системи, що захищається, є заборонним правилом: все, що не дозволено явно — заборонено. Таке правило забезпечує повноту захисту інформації в мережі підприємства і апріорну відсутність «дір» у безпеці.

Щоб забезпечити взаємодію пристроїв в мережі, для них створюється і доставляється (у загальному випадку не по каналах мережі) стартова конфігурація, що містить необхідні правила налаштування пристроїв тільки для їх централізованого управління, — стартова політика безпеки пристрою.

Правила ГПБ можуть бути поширені як на мережеві взаємодії, так і на функції контролю і управління самої системи.

Функціонально правила ГПБ розбиті по групах:

- правила VPN. Правила цього тиру реалізуються за допомогою протоколів IPSec; агентом виконання правила є драйвер VPN в стеку клієнтського пристрою або шлюзу безпеки (fP IP2, VPNRule);
- правила пакетної фільтрації. Вони забезпечують пакетну фільтрацію типу stateful і stateless; виконання цих правил забезпечують ті ж агенти, що виконують VPN- правила (IP1, IP2, PacketRule);
- proxy- правила, включаючи антивірусний захист «на льоту». Ці правила відповідають за фільтрацію трафіку, що передається під управлінням заданих прикладних протоколів; їх старанним агентом є proxy- агент, наприклад (User, Protocol, ProxyRule) або (Application, Protocol, Proxy - Rule);
- правила аутентифікованого/авторизованого доступу, включаючи правила Single Sign — On. Управління доступом Single Sign — On забезпечує цьому користувачеві роботу на єдиному паролі або іншій аутентифікаційній інформації з багатьма інформаційними ресурсами; зрозуміло, що символічний запис правила мережевого доступу легко поширюється на Single Sign — On (User, Application, Authentication Scheme). Правила цієї групи можуть комбінований виконуватися агентами різного рівня, від VPN— драйвера до proxy-агентів; крім того, агентами виконання таких правил можуть бути системи аутентифікації запит-відгук і продукти третіх розробників;
- правила, що відповідають за сигналізацію і подієве протоколювання. Політика протоколювання може оперативно і централізований управлятися агентом протоколювання; виконавцями правил є усі компоненти системи.

Набір правил ГПБ є логічно цілісним і семантично повним описом політики безпеки в масштабах мережі, на основі якої може будуватися локальна політика безпеки окремих пристроїв.

Локальна політика безпеки. Будь-якому засобу захисту, що реалізовує який-небудь сервіс інформаційної безпеки, потрібна для виконання його роботи ЛПБ — точний опис налаштувань для коректної реалізації правил аутентифікації користувачів, управління доступом, захисту трафіку та ін. При традиційному підході адміністраторові доводиться окремо настроювати кожен засіб захисту або копіювати якісь прості налаштування на велике число вузлів з подальшим їх коригуванням. Очевидно, що це неминуче призводить до великого числа помилок адміністрування і, як наслідок, істотного зниження рівня захищеності корпоративної мережі.

Після формування адміністратором ГПБ Центр управління на основі інтерпретації ГПБ автоматично обчислює і, якщо це необхідно, коригує окремі ЛПБ для кожного засобу захисту і автоматично завантажує потрібні налаштування в модулі відповідних засобів захисту, що управляють.

В цілому, ЛПБ мережевого пристрою включає повний набір правил дозволених з'єднань цього пристрою, що виконуються для забезпечення якої-небудь інформаційної послуги з необхідними властивостями захисту інформації.

Відмінність між правилами, реалізовуючими ГПБ в мережі, і правилами, реалізовуючими ЛПБ конкретного пристрою, полягає в тому, що в правилах групи ГПБ об'єкти і суб'єкти доступу можуть бути розподілені довільним чином в межах

мережі, а правила групи ЛПБ, включаючи суб'єкти і об'єкти ЛПБ, призначені і доступні тільки в межах простору одного з мережевих пристроїв.

16.3. Функціонування системи управління засобами безпеки

Структурними елементами системи управління засобами безпеки TrustWorks є агенти безпеки (Trusted Agent), Центр управління (Trusted GSM Server) і Консоль управління (Рис. 16.2).

Призначення основних засобів безпеки

Агент безпеки (Trusted Agent), встановлений на персональному комп'ютері клієнта, орієнтований на захист індивідуального користувача, що виступає, як правило, клієнтом в застосуваннях клієнт-сервер.

Агент безпеки, встановлений на сервері застосувань, орієнтований на забезпечення захисту серверних компонентів розподілених застосувань.

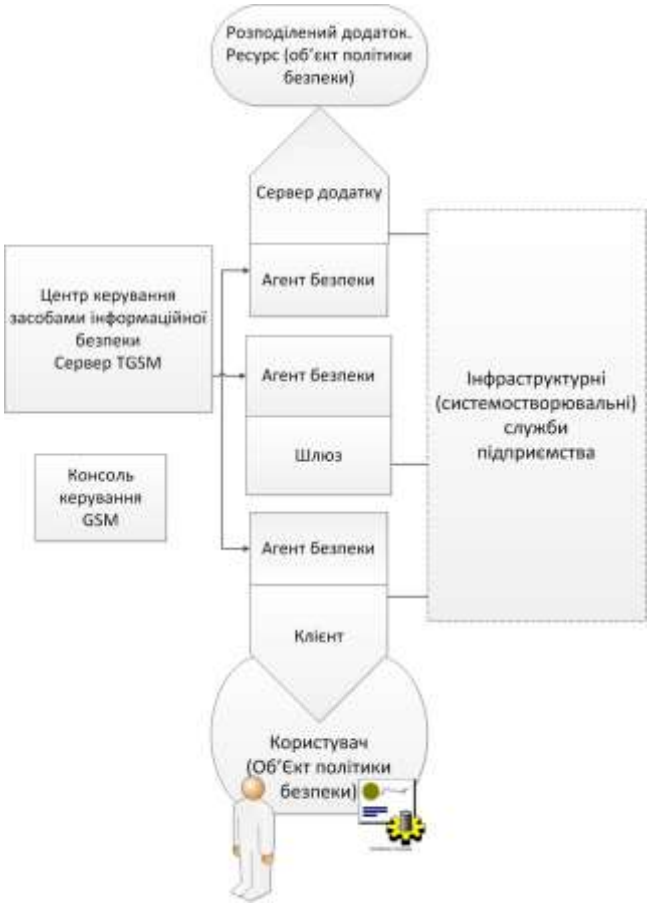

Рис. 16.2. Загальна структурна схема системи управління засобами інформаційної безпеки

Агент безпеки, встановлений на шлюзовому комп'ютері, забезпечує розв'язку сегментів мережі усередині підприємства або між підприємствами.

Центр управління (Trusted GSM Server) забезпечує опис і зберігання глобальної політики безпеки в масштабах мережі, трансляцію глобальної політики в локальні політики безпеки облаштувань захисту, завантаження облаштувань захисту і контроль станів усіх агентів системи. Для організації розподіленої схеми управління безпеки підприємства в системі GSM передбачається установка декількох (до 65 535) серверів GSM.

Консоль управління (Trusted GSM Console) призначена для організації робочого місця адміністратора (адміністраторів) системи. Для кожного з серверів GSM може бути встановлені декілька консолей, кожна з яких настроюється згідно з ролевими правами кожного з адміністраторів системи GSM.

Локальний Агент безпеки (Trusted Agent) є програмою, що розміщується на крайовому пристрої (клієнтові, сервері, шлюзі) і виконує наступні функції захисту:

- аутентифікацію об'єктів політики безпеки, включаючи інтеграцію різних сервісів аутентифікації;
- визначення користувача в системі і подій, пов'язаних з цим користувачем;
- забезпечення централізованого управління засобами безпеки і контролю доступу;
- управління ресурсами в інтересах застосувань, підтримку управління доступом до ресурсів прикладного рівня;
- захист і аутентифікацію трафіку;
- фільтрацію трафіку;
- подієве протоколювання, моніторинг, тривожну сигналізацію.

Додаткові функції Trusted Agent:

- постачання криптосервіса (multiple concurrent pluggable modules);
- управління периметрами Single Sign - On (як підзадача аутентифікації користувачів);
- сервіс в інтересах захищених застосувань (криптосервіс, сервіс доступу до PKI, доступ до управління безпекою);
- стискування трафіку (IPcomp, pluggable module);
- управління резервуванням мережевих ресурсів (QoS);
- функції локального агента мережевого антивірусного захисту.

Центральним елементом локального агента є процесор локальної політики безпеки (LSP processor), що інтерпретує локальну політику безпеки і розподіляє виклики між іншими компонентами.

Захист ресурсів

Аутентифікація і авторизація доступу. У рамках рішення реалізуються різні по функціональності схеми аутентифікації, кожна з яких включає тип аутентифікації і спосіб (механізм) ідентифікації об'єктів.

Для вибору типу аутентифікації передбачені наступні можливості: аутентифікація користувача при доступі до середовища GSM або локальній ОС, аутентифікація користувача при доступі в мережу (сегмент мережі), взаємна мережева аутентифікація об'єктів (застосування-застосування). Для вибору способу ідентифікації передбачені наступні варіанти, що припускають їх будь-яке спільне використання: токен (смарт-карта), пароль, «зовнішня» аутентифікація.

Контроль доступу при мережевих взаємодіях. При ініціалізації захищеного мережевого з'єднання від локальної ОС або при отриманні запиту на встановлення зовнішнього з'єднання локальні агенти безпеки Trusted Agent на кінцях з'єднання (і/або на проміжному шлюзі) звертаються до ЛПБ пристрою і перевіряють, чи дозволено встановлення цього з'єднання. У разі, якщо таке з'єднання дозволене — забезпечується необхідний сервіс захисту цього з'єднання, якщо заборонено — мережеве з'єднання не надається.

Контроль доступу на рівні прикладних об'єктів. Для незахищених розподілених застосувань в GSM забезпечується сервіс розмежування прав доступу на рівні внутрішніх об'єктів цього застосування. Контроль доступу на рівні об'єктів прикладного рівня забезпечується за рахунок застосування механізму proxy. Proxy розробляється для кожного прикладного протоколу. Передвстановленим є протокол http.

Для побудови розподіленої схеми управління і зниження завантаження мережі в GSM використовується архітектура розподілених проксі-агентів (Proxy Module у складі Trusted Agent), кожен з яких:

- має абстрактний універсальний інтерфейс, що забезпечує модульне підключення різних pгоху-фільтрів;
- має інтерфейс до системи управління, але використовує тимчасовий кеш для управління параметрами фільтрації, а фільтрація управляється узагальненими правилами типу:
  - аутентифікувати суб'єкт X в застосуванні-об'єкті К;
  - дозволити доступ суб'єктові X до об'єкту Y з параметрами Р;
  - заборонити доступ суб'єктові X до об'єкту Z;
  - семантика правил управління pгоху-фільтром і опису суб'єктів і об'єктів доступу залежать від конкретного прикладного протоколу, проте центр управління має можливість реєструвати pгоху-фільтри і забезпечувати управління ними в контексті загальної глобальної політики безпеки.

Proxy Agent може бути встановлений на шлюзі безпеки, безпосередньо на сервері, що виконує контрольовані застосування, і на клієнтському місці системи.

Управління засобами захисту

Найважливішим елементом рішення Trust Works є централізована, заснована на політиці (policy based) система управління засобами мережевої і інформаційної безпеки масштабу підприємства. Ця система забезпечує наступні якісні споживчі характеристики:

- високий рівень захищеності системи управління (шляхом виділення захищеного периметра управління усередині мережі підприємства);
- розширюваність системи управління інформаційної безпекою;
- високий рівень надійності системи управління і ключових її компонентів;
- інтеграцію з корпоративними системами загального мережевого і інформаційного управління;
- просте, інтуїтивно сприймане, ергономічне і інфраструктурне середовище опису, формування, моніторингу і діагностики політики безпеки масштабу підприємства (enterprise level policy based management).

Управління здійснюється спеціальним ПЗ адміністратора — Консоллю управління (Trusted GSM Console). Кількість і функції кожного з екземплярів встановленого в системі ПЗ Trusted GSM Console задаються головним адміністратором системи залежно від організаційної структури підприємства. Для призначення функцій кожного з робочих місць Trusted GSM Console використовується рольовий механізм розмежування прав по доступу до функцій управління (менеджменту) системи.

Функції управління GSM. Залежно від виду керованих об'єктів набір функцій, що управляють, в GSM можна умовно розбити на три категорії.

1. Управління інформаційним каталогом. Функції управління інформаційним каталогом визначають інформаційну складову GSM:

- формування розділів каталогу;
- опис послуг каталогу;
- призначення і контроль мережевих ресурсів, потрібних для виконання послуги;
- реєстрацію опису послуги;
- контроль стану послуг або розділів каталогу послуг;
- моніторинг виконання послуг;
- підготовку і пересилку звітів (протоколів) за станом каталогу.

2. Управління користувачами і правами доступу. Для управління правами доступу користувачів системи до послуг (інформаційним або мережевим ресурсам) GSM забезпечує наступні функції:

- формування груп користувачів по ролях і/або привілеях доступу до послуг системи;
- формування ієрархічних агрегацій користувачів по адміністративних, територіальних або іншим критеріям (домени і/або департаменти);
- формування ролей доступу користувачів до послуг (інформаційним або мережевим ресурсам);
- призначення рівнів секретності для послуг і користувачів системи (підтримка мандатного механізму розмежування прав);
- призначення фіксованих прав доступу групам, ролям, агрегаціям користувачів або окремим користувачам системи до інформаційних або мережевих ресурсів системи;
- підготовку і пересилку звітів (протоколів) по доступу користувачів до послуг системи;
- підготовку і пересилку звітів (протоколів) по роботі адміністраторів системи

3. Управління правилами ГПБ. Правила ГПБ ставлять у відповідність конкретні властивості захисту (як для мережевих з'єднань, так і для доступу користувачів до інформаційних послуг) передвстановленим рівням безпеки системи. Контроль за дотриманням правил ГПБ виконує спеціальний модуль у складі сервера системи — Security Policy Processor, що забезпечує:

- визначення кожного з рівнів безпеки набором параметрів захисту з'єднань, схеми аутентифікації і розмежування прав;
- призначення рівнів безпеки конкретним послугам або розділам каталогу послуг;
- призначення рівнів безпеки користувачам або будь-яким агрегаціям користувачів системи (групам, ролям, доменам, департаментам);
- контроль за цілісністю ГПБ (повнотою правил);
- обчислення політик безпеки ЛПБ локальних облаштувань захисту — агентів безпеки — і контроль їх виконання;
- контроль за виконанням ГПБ за різними критеріями;
- підготовку і пересилку звітів (протоколів) за станом системи і усіх спроб порушення ГПБ.

Кожен з адміністраторів системи аутентифікується і працює з системою через Trusted GSM Console згідно з передвстановленими для нього правами (на каталог

ресурсів або його частину, на визначений ролями набір функцій управління, на групи або інші набори користувачів). Усі дії будь-якого з адміністраторів протоколюються і можуть попарно контролюватися.

16.4. Аудит і моніторинг безпеки

Для організацій, комп'ютерні мережі яких налічують не один десяток комп'ютерів, що функціонують під управлінням різних ОС, на перше місце виступає завдання управління безліччю різноманітних захисних механізмів в таких гетерогенних корпоративних мережах. Складність мережевої інфраструктури, різноманіття даних і застосувань приводять до того, що при реалізації системи інформаційної безпеки за межами уваги адміністратора безпеці можуть залишитися багато загроз. Тому потрібне здійснення регулярного аудиту і постійного моніторингу безпеки ІС.

Аудит безпеки інформаційної системи

Поняття аудиту безпеки. Аудит є незалежною експертизою окремих областей функціонування підприємства. Однією із складових аудиту підприємства є аудит безпеки його ІС.

Нині актуальність аудиту безпеки ІС різко зросла. Це пов'язано зі збільшенням залежності організацій від інформації і ІС. Зросла уразливість ІС за рахунок підвищення складності елементів ІС, появи нових технологій передачі і зберігання даних, збільшення об'єму ПЗ. Розширився спектр загроз для ІС із-за активного використання підприємствами відкритих глобальних мереж для передачі повідомлень і транзакцій.

Аудит безпеки ІС дає можливість керівникам і співробітникам організацій отримати відповіді на питання:

- як оптимально використати існуючу ІС при розвитку бізнесу;
- як вирішуються питання безпеки і контролю доступу;
- як встановити єдину систему управління і моніторингу ІС;
- коли і як необхідно провести модернізацію устаткування і ПЗ;
- як мінімізувати риски при розміщенні конфіденційної інформації в ІС організації, а також намітити шляхи рішення виявлених проблем.

На ці і інші подібні питання не можна миттєво дати однозначна відповідь. Достовірну і обгрунтовану інформацію можна отримати, тільки розглядаючи усі взаємозв'язки між проблемами. Проведення аудиту дозволяє оцінити поточну безпеку ІС, оцінити риски, прогнозувати і управляти їх впливом на бізнес-процеси організації, коректно і обгрунтовано підійти до питання забезпечення безпеки інформаційних ресурсів організації.

Цілі проведення аудиту безпеки ІС:

- оцінка поточного рівня захищеності ІС;
- локалізація вузьких місць в системі захисту ІС;
- аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки відносно ресурсів ІС;
- вироблення рекомендацій по впровадженню нових і підвищенню ефективності існуючих механізмів безпеки ІС;
- оцінка відповідності ІС існуючим стандартам в області інформаційної безпеки.

У число додаткових завдань аудиту ІС можуть також входити вироблення рекомендацій по вдосконаленню політики безпеки організації і постановка завдань для ІТ персоналу, що стосуються забезпечення захисту інформації.

Проведення аудиту безпеки інформаційних систем. Роботи по аудиту безпеки ІС складаються з послідовних етапів, які в цілому відповідають етапам проведення комплексного ІТ аудиту автоматизованої системи:

- ініціації процедури аудиту;
- збору інформації аудиту;
- аналізу даних аудиту;
- вироблення рекомендацій;
- підготовки аудиторського звіту.

Аудиторський звіт є основним результатом проведення аудиту. Звіт повинен містити опис цілей проведення аудиту, характеристику обстежуваної ІС, результати аналізу даних аудиту, виведення, що містять оцінку рівня захищеності АС або відповідності її вимогам стандартів, і рекомендації по усуненню існуючих недоліків і вдосконаленню системи захисту.

Моніторинг безпеки системи

Функції моніторингу безпеки ІС виконують засоби аналізу захищеності і засобу виявлення атак (див. л. 14). Засоби аналізу захищеності досліджують налаштування елементів захисту ОС на робочих станціях і серверах, БД. Вони досліджують топологію мережі, шукають незахищені або неправильні мережеві з'єднання, аналізують налаштування МЕ.

У функції системи управління безпекою входить вироблення рекомендацій адміністраторові по усуненню виявлених вразливостей в мережах, застосуваннях або інших компонентах ІС організації.

Використання моделі адаптивного управління безпекою мережі дає можливість контролювати практично усі загрози і своєчасно реагувати на них, дозволяючи не лише усунути уразливості, які можуть привести до реалізації загрози, але і проаналізувати умови, що призводять до їх появи.