НУ “ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ”

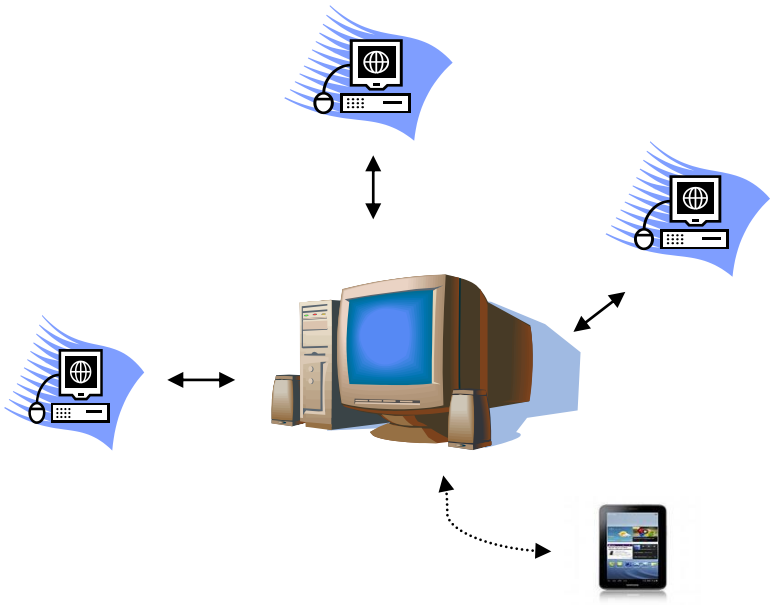
КИЇВСЬКИЙ ІНСТИТУТ
ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ПРАВА

КАФЕДРА ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ
ТА ІННОВАЦІЙНОЇ ДІЯЛЬНОСТІ

Заплотинський Б.А.

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Конспект лекцій



Київ – 2017

УДК 378.147:004:34.08

Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – КІІВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с.

Метою даного конспекта є ознайомлення студентів з основами інформаційної безпеки комп’ютерних систем, проблемами захисту інформації та підходами до їх розв’язання. Матеріал підготовлений на основі робочої навчальної програми з дисципліни “Основи ІБ” для студентів-магістрів КІІВіП зі спеціальності 073 “менеджмент”.

Головна увага приділена розкриттю не стільки глибини, скільки суті тем дисципліни в стислій і доступній для сприйняття формі.

Рецензент:
завкафедри інформаційно-аналітичної та інноваційної діяльності НУ “ОЮА”,
д.т.н., проф. **Тупкало В.М.**

Ухвалено на засіданні кафедри,
протокол № 1 від 06.09.17

Розроблено на кафедрі ІАтаІД КІІВтаП НУ “ОЮА”, обсяг 5,3 др. арк.
02121, м. Київ, вул. Харківське шосе, 210, тел. (044) 563-80-64

ЗМІСТ

	ВСТУП	5
1.	**ОСНОВНІ ПОНЯТТЯ, ВИЗНАЧЕННЯ, ЗАКОНИ**	
1.1.	Загальні поняття щодо інформаційної безпеки	8
1.2.	Основні поняття та визначення дисципліни	9
1.3.	Основні нормативно-правові документи України у сфері ІБ	12
	Контрольні запитання до розділу	20
2.	**ОСНОВНІ ЗАГРОЗИ БЕЗПЕКИ**	
2.1.	Загальні відомості	17
2.2.	Основні ненавмисні штучні загрози	18
2.3.	Основные навмисні штучні загрози	19
2.4.	Класифікація загроз безпеки	21
2.5.	Опис моделі гіпотетичного порушника	23
2.6.	Види інформації, що захищається у сфері управління	25
2.7.	Контроль якості захисту інформації	28
2.8.	Класифікаційна політика у сфері інформації	29
	Контрольні запитання до розділу	30
3.	**МЕХАНІЗМИ РЕАЛІЗАЦІЇ БЕЗПЕКИ**	
3.1.	Джерела загроз інформаційної безпеки	31
3.2.	Сертифікація: створення захищеної роботи	32
	Контрольні запитання до розділу	35
4.	**ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ СФЕРИ ДЕРЖАВИ**	
4.1.	Загальні відомості	36
4.2.	Відмінності мережі від обчислюваного центру	36
4.3.	Деталі реалізації	38
	Контрольні запитання до розділу	46
5.	**ХАРАКТЕРИСТИКА СТАНДАРТІВ ПО ЗАБЕЗПЕЧЕННЮ ІБ**	
5.1.	Характеристика ефективних стандартів щодо безпеки	47
5.2.	Усна форма разповсюдження матеріалів із стандартів по ІБ	51
	Контрольні запитання до розділу	52
6.	**РИЗИК РОБОТИ НА ПЕРСОНАЛЬНОМУ КОМП'ЮТЕРІ**	
6.1.	Визначення вразливих місць персонального комп'ютера	53
6.2.	Мережевий захист ПК	55
6.3.	Планування безпечної роботи на ПК	56
	Контрольні запитання до розділу	63
7.	**ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ**	
7.1.	Загальні відомості	64
7.2.	Принципи інженерно-технічного захисту інформації	65
7.3.	Методы захисту інформації технічними засобами	67
7.4.	Канали витоку інформації	70
7.5.	Засоби забезпечення ІБ в комп'ютерних системах	71
	Контрольні запитання до розділу	84
8.	**ЗАГАЛЬНА ХАРАКТЕРИСТИКА КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЇ. КОНФІДЕНЦІЙНІСТЬ ДОКУМЕНТУ**	
8.1.	Загальні відомості, задачі КЗІ	85
8.2.	Стратегії комплексного захисту інформації	85

8.3.	Етапи побудови КЗІ для різних стратегій	87
8.4.	Безпека цінних інформаційних ресурсів	88
8.5.	Критерії цінності інформації	89
8.6.	Виявлення та документування конфіденційних відомостей	91
8.7.	Носії конфіденційних відомостей	93
	Контрольні запитання до розділу	94
9.	**РЕЖИМНИЙ ХАРАКТЕР РОБОТИ ОРГАНІЗАЦІЇ ЯК ОСНОВА КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЇ**	
9.1.	Розробка політики безпеки	95
9.2.	Система фізичного захисту – типові задачі та способи її реалізації. Основні характеристики системи фізичного захисту	97
9.3.	Кількісний і якісний аналіз системи фізичного захисту	98
9.4.	Інженерно-технічні засоби охорони	101
	Контрольні запитання до розділу	104
10.	**МІЖНАРОДНИЙ СТАНДАРТ БЕЗПЕКИ ISO/IEC 17799**	
10.1	Загальні відомості	105
10.2.	Стислий опис розділів стандарту	105
	Контрольні запитання до розділу	118
11.	**АУДИТ ОБ'ЄКТІВ ІБ. АНАЛІЗ РИЗИКІВ КОРПОРАТИВНИХ ІС**	
11.1.	Основні етапи аудита інформаційної безпеки	119
11.2	Німецький стандарт для вибору критерія аудиту BSI	120
11.3	Порівняння підходів за стандартами ISO 17799 і BSI	121
11.4	Міжнародний стандарт з управління СУІБ ISO 27001	122
11.5	Оцінювання можливого збитку	123
11.6	Оцінювання ефективності існуючої системи захисту ІС із застосуванням спеціалізованих інструментаріїв	126
	Контрольні запитання до розділу	127
	ЛІТЕРАТУРА	128

ВСТУП

На сучасному етапі розвитку суспільства, пов'язаного з масовим використанням інформаційних технологій і створенням єдиного інформаційного простору, в рамкам якого відбувається накопичення, обробка, зберігання та обмін інформацією, проблеми інформаційної безпеки набувають першорядного значення в усіх сферах суспільної і державної діяльності. Особлива гострота і актуальність цих проблем визначається такими факторами:

• високими темпами зростання парку засобів обчислювальної техніки і зв'язку, розширенням областей використання ЕОМ, різноманіттям і повсюдним поширенням інформаційно-керуючих систем, які підлягають захисту;

• залученням до процесу інформаційної взаємодії все більшого числа людей і організацій, різким зростанням їх інформаційних потреб;

• підвищенням рівня попиту на автоматизовані системи управління і обробки інформації, використанням їх в критичних ситуаціях;

• ставленням до інформації, як до товару, переходом до ринкових відносін з властивою їм конкуренцією і промисловим шпигунством у сфері створення і надання інформаційних послуг;

• концентрацією великих обсягів інформації різного призначення на електронних носіях, вдосконалення доступу до інформаційних ресурсів;

• наявністю інтенсивного обміну інформацією між учасниками процесу;

• загостренням протиріч між об'єктивно існуючими потребами суспільства в розширенні вільного обміну інформацією і надмірними або навпаки недостатніми обмеженнями на її поширення і використання;

• рівнями втрат (збитків) від знищення, фальсифікації, розголошення або незаконного тиражування інформації;

• різноманіттям видів загроз і можливих каналів несанкціонованого доступу (НСД) до інформації;

• зростанням числа кваліфікованих користувачів обчислювальної техніки і можливостей по створенню ними програмно-математичних впливів на систему;

• відсутністю достатньої кількості кваліфікованих спеціалістів у сфері захисту інформації.

Зрозуміло, що в такій ситуації виникає потреба в захисті комп’ютерних систем захисту інформації від несанкціонованого доступу, крадіжки, знищення та інших злочинних і небажаних дій, число яких безперервно зростає. Так за оцінкою фахівців США, збиток від комп'ютерних злочинів щорічно складає

близько 35 мільярдів доларів. В середньому збиток від одного комп'ютерного злочину становить близько 500-600 тисяч доларів. При цьому необхідно зазначити, що на сьогоднішній день:

• не існує єдиної теорії захищених систем, в достатній мірі універсальної в різних предметних областях (як в державному, так і в комерційному секторі);

• виробники засобів захисту, в основному, пропонують окремі компоненти для вирішення приватних завдань, залишаючи вирішення питань формування системи захисту і сумісності цих засобів своїм споживачам;

• для забезпечення надійного захисту необхідно вирішити цілий комплекс технічних і організаційних проблем з розробкою відповідної документації.

У конспекті лекцій розглядаються тільки деякі з основних питань, зв’язаних із забезпеченням інформаційної безпеки. Матеріал підготовлений на основі робочої навчальної програми з дисципліни “Основи ІБ” для студентів-магістрів КІІВіП зі спеціальності 073 “менеджмент”. Головна увага приділена розкриттю не стільки глибини, скільки суті тем в стислій і доступній для сприйняття формі.

Далі приводяться основні відомості з РНП до дисципліни.

Дисципліна має метою навчити студентів спеціалізованим заходам у сферах інформаційної та комп’ютерної безпеки, які забезпечують захист сучасних інформаційних систем у професійній діяльності, пов’язаної з отриманням, обробкою, накопиченням і захистом особистої та юридичної інформації.

Предметом дисципліни є основи забезпечення інформаційної та комп’ютерної безпеки.

В процесі вивчення дисципліни студенти мають бути ознайомленими із сучасними підходами, методиками, засобами та пристроями для захисту інформаційно-комп'ютерних систем і персональної інформації користувача.

Після вивчення дисципліни студенти повинні знати: основні положення та терміни щодо інформаційної та комп’ютерної безпеки; складові проблеми особистої інформаційної безпеки, безпеки держави та шляхи її вирішення; уразливості інформаційного простору сучасного суспільства і методи протидії та захисту цього простору; загальні принципи та засоби протидії у втручання в персональну інформацію у віртуальному середовищі Інтернет і в комп’ютері користувача; найважливіші програмно-технічні та криптографіч-

ні методи та засоби захисту інформації від несанкціонованого доступу; стан та шляхи вирішення проблеми боротьби із комп'ютерними злочинами.

Після вивчення дисципліни студенти повинні вміти: аналізувати інформаційні погрози та протидіяти діям порушників; захищати технічні канали витоку інформації; вирішувати практичні завдання із захисту інформації в комп'ютерних системах.

НАВЧАЛЬНА ДИСЦИПЛІНА В ГОДИНАХ

Форма навчання	Курс	Семестр	Лекції	Практичні заняття	Всього ауд.годин	Курсові роботи	Контрольні роботи	Установ. лекції	Самостійна робота	Всього годин	Іспит	Залік
Денна	5	9	24	12	36	–	–	–	54	90 (3 кред)	*	
Заочна	7	11	2	4	6	–	–	–	84		*	

1. ОСНОВНІ ПОНЯТТЯ, ВИЗНАЧЕННЯ, ЗАКОНИ

1.1. Загальні поняття щодо інформаційної безпеки

В даний час інформаційні системи та інформаційно-телекомунікаційні мережі підтримують сервіси та переносять дані в таких кількостях, які важко було собі уявити ще кілька років тому. Їх готовність необхідна для роботи дуже багатьох інфраструктур, наприклад, комунальні або електричні мережі, органи державного, муніципального та регіонального управління (ДМРУ), організації, населення і т. д. Тому безпека цих систем стає необхідною умовою їх подальшого розвитку. Для кожного випадку визначення безпеки означає специфікацію політики безпеки, тобто безлічі бажаних цілей. Наприклад, електронна система голосування повинна бути встановлена таким чином, щоб голосувати могли тільки зареєстровані виборці, доступ до веб-сервера повинен здійснюватися аутентифікованими користувачами, тільки авторизовані користувачі повинні підключатися до банківської системи і т.д.

Безпека об'єкта проявляється через безпеку його найбільш важливих властивостей або властивостей структурних складових. Якщо об'єктом безпеки є людина, то його безпека полягає в захищеності від загроз йому, як живому організму, і загроз йому, як носію певних психічних і духовних якостей, тобто особистості. Якщо об'єктом безпеки є суспільство (спільність людей на певній території, яка характеризується економічною і духовною єдністю), то його безпека буде полягати в захищеності від загроз його членів, а також історично склавшимися відносинами між людьми. Відповідно, в змісті національної безпеки розрізняють державну, економічну, суспільну, оборонну, інформаційну, екологічну та іншу безпеку. Державна безпека має своїм об'єктом стан органів ДМРУ, економічна безпека – економіку суспільства, громадська безпека – соціальні інститути, екологічна безпека – навколишнє середовище і людину і т.д.

Безпека проявляється як протидія на заданому рівні спробами нанести шкоду функціонуванню або усього об’єкта захисту, або його структурним складовим. Однією з важливих структурних складовиxx багатьох об’єктів безпеки є інформація (або діяльність, предметом котрої є інформація).

1.2. Основні поняття і визначення дисципліни

Широко поширене в даний час поняття *інформаційна безпека* підкреслює важливість інформації в сучасному суспільстві і характеризує той факт, що інформаційний ресурс є сьогодні таким же багатством, як корисні копалини, виробничі і людські ресурси, і також як вони підлягає захисту від різного роду посягань, зловживань і злочинів.

Під інформаційною безпекою будемо розуміти захищеність інформації і підтримуючої інфраструктури від випадкових або преднавмисних впливів природного або штучного характеру, чреватих нанесенням шкоди власникам або користувачам інформації і підтримувальної інфраструктури.

Підхід до проблем інформаційної безпеки необхідно починати з виявлення суб'єктів, зацікавлених у забезпеченні:

- своєчасного доступу (за прийнятний час) до необхідної інформації;
- конфіденційності певної частини інформації;
- достовірності (повноти, точності, адекватності, цілісності) інформації;
- захисту від нав'язування їм неправдивої (недостовірної, перекрученої) інформації (тобто від дезінформації);
- захисту частини інформації від незаконного її тиражування (захисту авторських прав, прав власника інформації тощо);
- розмежування відповідальності за порушення законних прав (інтересів) інших суб'єктів інформаційних відносин і встановлених правил поводження з інформацією;
- можливості здійснення безперервного контролю і управління процесами обробки і передачі інформації.

Очевидно, що забезпечення цих вимог суттєво і для держави в цілому, і для окремих громадських (комерційних) організаций, і для підприємств (юридичних осіб), і для окремих громадян (фізичних осіб), які і є суб'єктами інформаційних відносин. Тому введемо наступні визначення.

Суб’єкт – це активний компонент інформаційної системи, який може стати причиною потоку інформації від об'єкта до суб'єкта або зміни стану системи.

Об’єкт – пасивний компонент системи, який зберігає, приймає або передає інформацію. Доступ до об'єкту означає доступ до інформації, яка міститься в ньому.

У якості об'єктів, які підлягають захисту в інтересах забезпечення безпеки суб'єктів інформаційних відносин, необхідно розглядати: інформацію і інформаційні ресурси, носії інформації, процеси обробки інформації.

Під інформацією розуміють відомості щодо об'єктів та явищах навколишнього середовища, їх параметрах, властивостей і стану, які зменшують ступень невизначеності.

Основними властивостями якості інформації з позиції користувача є: репрезентативность, змістовність, достатність, доступність, актуальність, своєчасність, точність, достовірність і сталість.

Інформаційні ресурси – це окремі документи та масиви документів, представлені самостійно або в інформаційних системах (бібліотеках, архівах, фондах, базах даних та інших ІС).

Інформаційні ресурси можна класифікувати:

- *за видом інформації* – правові, науково-технічні, політичні, фінансово-економічні, статистичні, метрологічні, соціальні, персональні, медичні, про надзвичайні ситуації та т.п.;

- *за режимом доступу* – відкриті, обмеженого доступу, державна таємниця, конфіденційна інформація, комерційна таємниця, професійна таємниця, службова таємниця, особиста (персональна) таємниця;

- *за формою власності* – державні, муніципальні, регіональні, приватні, колективні;

- *за видом носія* – на папері (документи, листи, медичні карти, телефонні довідники організацій, чернетки і т.п.), на екрані, в пам'яті ЕОМ, в каналі зв'язку, на гнучких і жорстких магнітних дисках, на інших носіях.

Носіями інформації можуть бути окремі люди, які володіють важливою інформацією (експерти), а також спеціально завербовані або випадкові інформатори.

Поінформованість кінцевого користувача про заходи безпеки повинна проявлятися в умінні розрізняти 4 рівні захисту комп'ютерних та інформаційних ресурсів:

- *запобігання* – доступ до інформації та технологій має тільки авторизований персонал;

- *виявлення* – зловживання стають відомими ще на ранній стадії, навіть у разі обходу механізмів захисту;

- *обмеження* – зменшення розміру втрат, якщо злочин мав місце, незважаючи на вжиті заходи щодо його запобігання;

- *відновлення* – забезпечення ефективного відновлення інформації при наявності документованих і перевірених планів проведення цієї операції.

Далі надані основні поняття щодо інформаційної безпеки комп'ютерних систем (КС).

Під безпекою КС розуміють її захищеність від випадкового або навмисного втручання в нормальний процес її функціонування, а також від спроб розкрадання, зміни або руйнування її компонентів.

Природа впливів на КС може бути найрізноманітнішою. Це і стихійні лиха (землетруси, урагани, пожежі), і вихід з ладу складових елементів КС, і помилки персоналу, і спроба проникнення зловмисника.

Безпека КС досягається вживанням заходів щодо забезпечення конфіденціальності і цілісності оброблюваної нею інформації, а також доступності та цілісності компонентів і ресурсів системи.

Під доступом до інформації розуміється ознайомлення з інформацією, її обробка, зокрема копіювання, модифікація або знищення інформації. Розрізняють санкціонований і несанкціонований доступ до інформації.

Санкціонований доступ до інформації – це доступ до інформації, що не порушує встановлені правила розмежування доступу. Ці правила служать для регламентації права суб'єктів на доступ до об'єктів.

Несанкціонований доступ (НСД) до інформації характеризується порушенням встановлених правил розмежування доступу. Це найбільш поширений вид комп'ютерних порушень.

Конфіденційність даних – це статус, наданий даними і визначає необхідний ступінь їх захисту. *За суттю конфіденційність інформації – це властивість інформації бути відомою тільки допущеним особам (авторизованим суб'єктам системи).* Для інших суб'єктів системи ця інформація повинна бути невідомою.

Цілісність інформації забезпечується в тому випадку, якщо дані в системі не відрізняються в семантичному відношенні від даних у вихідних документах, тобто якщо не відбулося їх випадкового або навмисного спотворення або руйнування.

Цілісність компонента або ресурсу системи – це властивість компонента чи ресурсу бути незмінними в семантичному сенсі при функціонуванні системи в умовах випадкових або навмисних спотворень або руйнівних впливів.

Доступність компонента або ресурсу системи – це властивість компонента чи ресурсу бути доступним для авторизованих законних суб'єктів системи.

Метою захисту систем обробки інформації є протидія загрозам безпеки.

Під загрозою безпеки КС розуміють можливі дії, які прямо або побічно можуть завдати шкоди її безпеки.

Збиток безпеки має на увазі порушення стану захищеності інформації, що міститься і обробляється в КС. З поняттям загрози безпеки тісно пов'язане поняття уразливості КС.

Комплекс засобів захисту являє собою сукупність програмних і технічних інструментів, що створюються і підтримуються для забезпечення інформаційної безпеки КС. Комплекс створюється і підтримується відповідно до прийнятої в даній організації політики безпеки.

Політика безпеки – це сукупність норм, правил і практичних рекомендацій для надійної роботи засобів захисту КС від безлічі загроз.

На практиці найважливішими є наступні аспекти информационої безпеки: *доступність, цілісність і конфіденційність*.

1.3. Основні нормативно-правові документи України у сфері ІБ

Інформаційна безпека держави

Інформаційна безпека держави – це стан її захищеності, при якому спеціальні інформаційні операції, акти зовнішньої агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам.

Відповідно до законодавства України поняття *"інформаційна безпека" має таке визначення*: *стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування*

інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

Виокремлюють три рівня забезпечення інформаційної безпеки:

- *рівень особи* (формування раціонального, критичного мислення на основі принципів свободи вибору);
- *суспільний рівень* (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам);
- *державний рівень* (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам)

Концепція державної інформаційної політики

Досі не прийнято закону, який би визначав концепцію державної інформаційної політики України. Відповідно, в країні не існує єдиного плану, єдиної державної позиції чи стратегії розвитку інформаційної галузі, а отже і забезпечення інформаційної безпеки.

Протягом 2002-2010 рр. було три спроби ухвалити концепцію державної інформаційної політики в 2002, 2009 та 2010 роках. У січні 2011 року черговий проект концепції прийняли у першому читанні за основу закону і направили на доопрацювання Комітету Верховної Ради України з питань свободи слова та інформації .

Однією з основних загроз інформаційній безпеці ЗУ "Про основи національної безпеки" називає "намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації". До інших загроз віднесено:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;

• розголошення інформації, яка становить державну таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави.

В Доктрині інформаційної безпеки України, підписаній Президентом в липні 2009 р., серед всього виділено наступні *загрози інформаційній безпеці країни*:

• поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;

• зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;

• деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності України;

• прояви сепаратизму в засобах масової інформації, а також у мережі Інтернет, за етнічною, мовною, релігійною та іншими ознаками.

Після перемоги Євромайдану почалася розробка нової Доктрини інформаційної безпеки, яка б відповідала вимогам часу.

Діяльність Міжвідомчої комісії з питань інформаційної політики та ІБ

При Раді національної безпеки і оборони (РНБО) діє Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки. До основних її завдань, зокрема, належить аналіз стану і можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики

Закони України

- Закон України «Про інформацію» від 02.10.1992 № 2657-XII
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
- Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII
- Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

Постанови КМУ

- Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373
- Постанова Кабінету міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» від 27 листопада 1998 р. №1893

Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ

- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
- Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу
- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
- НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2
- НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу
- НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
- НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу

- Техническое задание на создание автоматизированной системы. ГОСТ 34.602-89
- НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

Галузеві стандарти:

- ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD)
- ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD)

Контрольні запитання

1. Поясніть гостроту і актуальність проблеми інформаційної бепеки.
2. Надайте визначення інформації, інформаційній безпеці, суб’єкту та об’єкту.
3. Поясніть суть 4-ох рівнів захисту інформації.
4. Поясніть суть політики інформаційної безпеки.
5. В чому суть інформаційної безпеки держави?
6. Розкажіть про Концепцію державної інформаційної політики.
7. Назвіть основні нормативні документи щодо захисту інформації.

2. ОСНОВНІ ЗАГРОЗИ БЕЗПЕКИ

2.1. Загальні відомості

Надамо більш розширене тлумачення терміну "*загроза безпеки*".

Під загрозою безпеки розуміють потенційно можливі впливи, події, процеси або явища, котрі прямо чи побічно можуть нанести шкоду (збиток) інтересам об'єктів інформаційних відносин. Під таким збитком розуміють порушення стану захищеності інформації, що міститься і оброблюється в комп'ютерній системі (КС). З поняттям загрози безпеки тісно зв'язане поняття уразливості КС.

Уразливість КС – це деяке найбільш чутливе місце (властивість) системи, яке робить можливим виникнення і реалізацію загрози (атаки на КС).

Атака на комп'ютерну систему – це дія, що робиться зловмисником для пошуку і використанні тієї або іншої уразливості системи. Таким чином, атака – це реалізація загрози безпеки.

Основна *мета захисту* КС – протидія загрозам безпеки. За метою впливу розрізняють наступні основні *типи загроз безпеки*:

• порушення конфіденційності (розкриття) інформації;

• порушення цілісності інформації (її повне або часткове знищення, спотворення, фальсифікація, дезінформація);

• порушення (часткове або повне) працездатності системи. Вихід з ладу або неправомірна зміна режимів роботи компонентів системи обробки інформації, їх модифікація або підміна можуть призвести до отримання невірних результатів розрахунків, відмов системи від потоку інформації (невизнання однією з взаємодіючих сторін факту передачі або прийому повідомлень) і / або відмов в обслуговуванні кінцевих користувачів;

• несанкціоноване тиражування відкритої інформації (яка не є конфіденційною), наприклад, програм, баз даних, різного роду документації, літературних творів в порушення прав власників інформації, авторських прав і т.п. Інформація, володіючи властивостями матеріальних об'єктів, має таку особливість, як невичерпність ресурсу, що істотно ускладнює контроль за її тиражуванням.

Основными видами загроз безпеки КС та інформації (загроз інтересам суб'єктів інформаційних відносин) є:

• стихійні лиха і аварії (повінь, ураган, землетрус, пожежа і т.п.);

• збої і відмови устаткування (технічних засобів) КС;

• наслідки помилок проектування і розробки компонентів КС (апаратних засобів, технології обробки інформації, програм, структур даних і т.п.);

• помилки експлуатації (користувачів, операторів та іншого персоналу);

• навмисні дії порушників і зловмисників (скривджених осіб з числа персоналу, злочинців, шпигунів, диверсантів і т.п.).

Природні загрози – це загрози, викликані впливами на КС та її елементи об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини.

Штучні загрози – це загрози КС, викликані діяльністю людини. Серед штучних загроз, виходячи з мотивації дій, можна виділити:

• ненавмисні (випадкові) загрози, викликані помилками в проектуванні КС і її елементів, помилками в програмному забезпеченні, помилками в діях персоналу і т.п. ;

• навмисні загрози, пов'язані з корисливими намірами людей (зловмисників).

Джерела загроз по відношенню до КС можуть бути зовнішніми або внутрішніми (компоненти самої КС – її апаратура, програми, персонал).

2.2. Основні ненавмисні штучні загрози

Основними ненавмисними штучними загрозами КС (діями, які скоюють люди випадково, через незнання, неуважність або недбалість, з цікавості, але без злого умислу) є:

1) ненавмисні дії, що призводять до часткової або повної відмови системи або руйнування апаратних, програмних, інформаційних ресурсів системи (ненавмисна псування устаткування, видалення, спотворення файлів з важливою інформацією або програм, в тому числі системних і т.п.);

2) неправомірне відключення обладнання або зміна режимів роботи

пристроїв і програм;

3) ненавмисна псування носіїв інформації;

4) запуск технологічних програм, здатних при некомпетентному використанні викликати втрату працездатності системи (зависання, зациклення) або здійснюють незворотні зміни в системі (форматування або реструктуризацію носіїв інформації, видалення даних і т.п.);

5) нелегальне впровадження та використання неврахованих програм (ігрових, навчальних, технологічних та ін., які не є необхідними для виконання порушником своїх службових обов'язків) з подальшою необґрунтованою витратою ресурсів (завантаження процесора, захоплення оперативної пам’яті та пам’яті на зовнішніх носіях);

6) зараження комп'ютера вірусами;

7) необережні дії, що призводять до розголошення конфіденційної інформації, або роблять її загальнодоступною;

8) розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, перепусток тощо);

9) проектування архітектури системи, технології обробки даних, розробка прикладних програм, з можливостями, що являють небезпеку для працездатності системи і безпеки інформації;

10) ігнорування організаційних обмежень при роботі в системі;

11) вхід в систему в обхід засобів захисту (завантаження сторонньої операційної системи зі змінних носіїв і т.п.);

12) некомпетентне використання, настроювання або неправомірне відключення засобів захисту персоналом служби безпеки;

13) пересилання даних за помилковою адресою абонента (пристрою);

14) введення помилкових даних;

15) ненавмисне пошкодження каналів зв'язку.

2.3. Основні навмисні штучні загрози

Основні можливі шляхи навмисної дезорганізації роботи, виведення системи з ладу, проникнення в систему несанкціонованого доступу до інформації:

1) фізичне руйнування системи (шляхом вибуху, підпалення і т.п.) або виведення з ладу всіх або окремих найбільш вразливих компонентів комп'ютерної системи (пристроїв, носіїв важливої системної інформації, осіб з числа персоналу і т.п.);

2) відключення або виведення з ладу підсистем, які забезпечують функціонування обчислювальних систем (електроживлення, охолодження і вентиляції, ліній зв'язку тощо);

3) дії по дезорганізації функціонування системи (зміни режимів роботи пристроїв або програм, страйк, саботаж персоналу, постановка потужних активних радіоперешкод на частотах роботи пристроїв системи і т.п.);

4) впровадження агентів у число персоналу системи (в т.ч., можливо, і в адміністративну групу, яка відповідала за безпеку);

5) вербування (шляхом підкупу, шантажу і т.п.) персоналу або окремих користувачів, які мають певні повноваження;

6) застосування підслуховуючих пристроїв, дистанційна фото- і відеозйомка і т.п .;

7) перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв і ліній зв'язку, а також наведень активних випромінювань на допоміжні технічні засоби, які безпосередньо не беруть участь в обробці інформації (телефонні лінії, мережі живлення, опалення і т.п.);

8) перехоплення даних, переданих по каналах зв'язку, та їх аналіз з метою з'ясування протоколів обміну, правил входження в зв'язок і авторізації користувача та подальших спроб їх імітації для проникнення в систему;

9) розкрадання носіїв інформації (жорстких дисків, стрічок, мікросхем пам'яті, запам'ятовуючих пристроїв і ПЕОМ в цілому);

10) несанкціоноване копіювання носіїв інформації;

11) розкрадання виробничих відходів (роздруківок, записів, списаних носіїв інформації і т.п.);

12) читання залишкової інформації з оперативної пам'яті та із зовнішніх запам'ятовуючих пристроїв;

13) читання інформації з областей оперативної пам'яті, які використовуються операційною системою (в тому числі підсистемою захисту) або ін-

шими користувачами в асинхронному режимі, використовуючи недоліки мультизадачних операційних систем і систем програмування;

14) незаконне отримання паролів та інших реквізитів розмежування доступу (агентурним шляхом, використовуючи недбалість користувачів, шляхом підбору, шляхом імітації інтерфейсу системи і т.д.) з подальшим маскуванням під зареєстрованого користувача (“маскарад”);

15) несанкціоноване використання ерміналів користувачів, які мають унікальні фізичні характеристики, такі як номер робочої станції в мережі, фізичну адресу, адресу в системі зв'язку, апаратний блок кодування і т.п .;

16) розкриття шифрів криптозахисту інформації;

17) впровадження апаратних спецвкладень, програмних “закладок” та “вірусів” (“троянських коней” і “жучків”), тобто таких ділянок програм, які не потрібні для здійснення заявлених функцій, але дозволяють долати систему захисту, таємно і незаконно здійснювати доступ до системних ресурсів з метою реєстрації та передачі критичної інформації або дезорганізації функціонування системи;

18) незаконне підключення до ліній зв’язку з метою роботи “між рядків” з використанням пауз в діях законного користувача від його імені з наступним введенням помилкових повідомлень або модифікацією переданих повідомлень;

19) незаконне підключення до ліній зв’язку з метою прямої підміни законного користувача шляхом його фізичного відключення після входу в систему і успішної аутентифікації з подальшим введенням дезінформації та нав’язуванням неправдивих повідомлень.

Найчастіше для досягнення поставленої мети зловмисник використовує не один, а деяку сукупність шляхів, перерахованих вище.

2.4. Класифікація загроз безпеки

Вище було розглянуто два основні класи потенційних загроз за природою їх виникнення: природні і штучні. Але поряд з цим загрози можна класифікувати і за іншими критеріями реалізації, які наведені далі.

Класифікація загроз за метою: несанкціоноване читання інформації, несанкціонована зміна інформації, несанкціоноване знищення інформації, повне або часткове руйнування КС (від короткочасного виведення з ладу окремих модулів до фізичного стирання системних файлів);

Класифікація загроз за принципом впливу на КС: використання легальних каналів отримання інформації (наприклад, несанкціоноване читання з файлу); використання прихованих каналів отримання інформації (наприклад, недокументованих можливостей ОС); створення нових каналів отримання інформації (наприклад, за допомогою програмних закладок).

Класифікація загроз за характером впливу на КС: активний вплив – несанкціоновані дії в системі; пасивний вплив – несанкціоноване спостереження за процесами в системі.

Класифікація загроз, що виникають через слабкий захист: неадекватна політика безпеки (в т.ч. помилки адміністратора); помилки і недокументовані можливості ПЗ (так звані “люки” – вбудовані в систему спеціальні входи, призначені для тестування або налагодження, але випадково залишені, що дозволяє обходити систему захисту); раніше впроваджені програмні закладки.

Класифікація загроз за способом впливу на об’єкт атаки: безпосереднє перевищення користувачем своїх повноважень; робота від імені іншого користувача або перехоплення результатів його роботи.

Класифікація загроз за способом дій порушника: в інтерактивному режимі (вручну) або в пакетному режимі (за допомогою спеціальних програм, без участі користувача).

Класифікація загроз за використовуваними засобами атаки: штатні засоби без використання додаткового ПЗ; ПЗ третіх фірм (віруси, шкідливі програми; ПЗ, розроблене для інших цілей – відладчики, мережеві монітори і т. д.).

Класифікація загроз за об’єктом атаки: апаратні засоби (обладнання); програмне забезпечення, дані, персонал.

Можливі шляхи реалізації загроз безпеки для перерахованих об’єктів атаки представлені в таблиці 2.1.

Таблиця 2.1

Шляхи реалізації загроз безпеки

Об'єкти впливу	*Порушення конфіденційності інформації*	*Порушення цілостності інформації*	*Порушення працездатності системи*
Апаратні засоби	НСД – підключення; використання ресурсів; розкрадання носіїв	НСД - підключення; використання ресурсів; модифікація, зміна режимів	НСД - зміна режимів; виведення з ладу: руйнування
ПЗ	НСД –копіювання; викрадення	НСД, засилання вірусів	НСД – спотворення; видалення: підміна
Дані	НСД – копіювання; викрадення; перехоплення	НСД - спотворення; модифікація	НСД - спотворення; видалення; підміна
Персонал	Розголошення; передача відомостей про захист; недбалість	"Маскарад": вербування, підкуп персоналу	Залишення робочого міся без нагляду, фізичне усунення працівника

2.5. Опис моделі гіпотетичного порушника

Важливою складовою успішного аналізу ризиків та визначення вимог до складу і характеристик системи захисту інформації є підготовка гіпотетичної моделі потенційного порушника. При цьому необхідно враховувати, що:

• кваліфікація порушника може бути на рівні розробника даної системи;

• порушником може бути як стороння особа, так і законний користувач системи;

• порушнику відома інформація про принципи роботи системи;

• порушник вибере найбільш слабку ланку в захисті.

Крім того, при розробці моделі порушника необхідно:

1) визначити, до якої категорії осіб він може належати: з числа внутрішніх суб'єктів (безпосередній персонал системи), чи з числа зовнішніх (сторонніх) осіб (клієнти, відвідувачі, представники систем життєзабезпечення, конкуренти, найманці, випадкові люди);

2) виявити цілі і мотиви дій порушника (безвідповідальність, самоутвердження, корисливий інтерес);

3) врахувати можливі обмеження на дії порушника.

Усіх порушників можна класифікувати в такий спосіб.

За рівнем знань про КС порушник: знає функціональні особливості КС, основні закономірності формування в ній масивів даних і потоків запитів до них, вміє користуватися штатними засобами; володіє високим рівнем знань і досвідом роботи з технічними засобами системи та їх обслуговування; володіє високим рівнем знань в області програмування та обчислювальної техніки, проектування і експлуатації автоматизованих інформаційних систем; знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.

За рівнем можливостей (використовуваним методам і засобам) порушник: застосовує чисто агентурні методи отримання відомостей; застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи); використовує тільки штатні засоби та недоліки систем захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні носії інформації, які можна приховано пронести через пости охорони; застосовує методи і засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передачі даних, впровадження програмних закладок і використання спеціальних інструментальних і технологічних програм).

За часом дії порушник працює: в процесі функціонування КС (під час роботи системи); в період неактивності компонентів системи (в неробочий час, під час планових перерв у її роботі, перерв для обслуговування і ремонту і т.п.); як в процесі функціонування КС, так і в період неактивності компонентів системи.

За місцем дії порушник отримує інформацію: без доступу на контрольовану територію організації; з контрольованої території без доступу в будівлі і споруди; всередині приміщень, але без доступу до технічних засобів КС; з робочих місць кінцевих користувачів (операторів) КС; з доступом в зону даних (баз даних, архівів і т.п.); з доступом в зону управління засобами забезпечення безпеки КС.

Крім того можуть враховуватися такі обмеження і припущення про характер дій можливих порушників:

• робота з підбору кадрів і спеціальні заходи ускладнюють можливість

створення коаліції порушників, тобто об’єднання (змови) і цілеспрямованих дій з подолання підсистеми захисту двох і більше порушників;

• порушник, плануючи спроби несанкціонованого доступу, приховує свої несанкціоновані дії від інших співробітників;

• НСД може бути наслідком помилок користувачів, адміністраторів, персоналу, який експлуатує і обслуговує систему захисту, а також недоліків прийнятої технології обробки інформації.

Визначення конкретних значень характеристик можливих порушників в значній мірі суб’єктивно. *Модель порушника, побудована з урахуванням особливостей конкретної предметної області і технології обробки інформації, може бути представлена перерахуванням декількох варіантів його вигляду*. Кожен вид порушника має бути охарактеризований значеннями характеристик, наведених вище.

2.6. Види інформації, що захищається в сфері управління

Загальнодоступна (відкрита) інформація суб’єкта (образно – його надводна частина), як правило, менш ємна, ніж інформація обмеженого доступу (підводна частина). Навіть в умовах, так званого, відкритого суспільства це співвідношення має місце для будь-якого суб’єкта, що зберігає стійкість. Під впливом численних загроз, обумовленим конкуренцією і стихією ринку, суб’єкт повинен створювати ресурс конфіденційної інформації (ноу-хау та ін.), необхідної для виживання в певному середовищі. Фактично співвідношення (баланс) ємностей відкритого і закритого інформаційного ресурсу є неодмінна умова його сталого розвитку. Причому в поняття “ємність” в даному випадку вкладається інтегральна оцінка: обсяг, помножений на цінність інформації.

Досвід показує, що в загальній системі управління (як в розвитку економіки і управління, так і в підготовці і веденні суспільно-політичних компаній) найбільш важливим елементом з роками стає досягнення переваги в інформаційній сфері. Цими обставинами і визначається існування інститутів таємниць, що створюють можливість проводити незалежну інформаційну

політику, захищати свої інтереси, здійснювати управління суспільством, регіоном, муніципальним освітою.

Основу нормативно-правового забезпечення захисту інформації обмеженого доступу складають Конституція України, Закони "Про інформацію","Про захист інформації в інформаційно-телекомунікаційних системах", " Про державну таємницю","Про захист персональних даних" та ін.

У чинному законодавстві країни згадуються різні види таємниць (державна, службова, комерційна, банківська, особиста, сімейна таємниця, таємниця слідства, зв'язку, поштових відправлень та інші). Наведемо найбільш важливі визначення в даній області і дамо необхідну класифікацію.

Захищаємою інформацією називають інформацію, яка підлягає захисту відповідно до вимог правових документів або вимогами, встановленими власником інформації. Володарем інформації може бути громадянин (фізична особа), юридична особа, держава, суб'єкт господарювання, муніципальне утворення. До інформації, що захищається, відноситься інформація з обмеженим доступом, а також відкрита інформація, що представляє цінність.

Інформацією з обмеженим доступом називають інформацію, доступ до якої обмежується відповідно до Закону України з метою захисту прав і законних інтересів суб'єктів права на таємницю. Вона складається з державної таємниці та конфіденційної інформації. Конфіденційна інформація, в свою чергу, включає безліч видів таємниці, які зводяться до шести основних видів: персональні дані, таємниця слідства і судочинства, службова таємниця, професійна таємниця, комерційна таємниця, таємниця винаходу (корисної моделі чи промислового зразка). Особливу важливість з точки зору безпеки держави має захист інформації, яка становить державну та службову таємницю.

Державна таємниця – захищені державою відомості в області його військової зовнішньополітичної, економічної, розвідувальної, контррозвідувальної і оперативно-розшукової діяльності, поширення яких може завдати шкоди безпеці країни.

Конфіденційна інформація – інформація, що не становить державну таємницю, доступ до якої обмежується відповідно до законодавства України.

Персональні дані – відомості про факти, події і життя громадянина, що дозволяють ідентифікувати його особу, за винятком відомостей, що підлягають поширенню в засобах масової інформації у встановлених законами випадках.

Таємниця слідства і судочинства – конфіденційна інформація, що стала відомою в органах слідства та судочинства тільки на законних підставах, а також службова інформація про діяльність органів слідства і судочинства, доступ до якої обмежений законами або в силу службової необхідності.

Службова таємниця – конфіденційна інформація, що стала відомою в державних органах та органах місцевого самоврядування тільки на законних підставах і в силу виконання їх представниками службових обов'язків, а також службова інформація про діяльність державних органів, доступ до якої обмежений законами України.

Професійна таємниця – відомості, пов'язані з професійною діяльністю, доступ до яких обмежено відповідно до Конституції і відповідниминими законами України (лікарська, нотаріальна, адвокатська таємниця, таємниця листування, телефонних переговорів, поштових відправлень, телеграфних або інших повідомлень, банківська таємниця і так далі).

Комерційна таємниця – науково-технічна, технологічна, комерційна, організаційна або інша використовувана в економічній діяльності інформація, що має дійсну цінність в силу її невідомості третім особам, до якої немає вільного доступу на законній підставі і по відношенню до якої приймаються адекватні її цінності заходи охорони.

Таємниця винаходу, корисної моделі або промислового зразка – відомості про сутність винаходу, корисної моделі чи промислового зразка до офіційної публікації про них.

У ряді випадків немає чіткої межі між класифікаційними групами інформації обмеженого доступу. Так, наприклад, відомості, що становлять комерційну таємницю фірми, при передачі їх в органи державної влади стають в той же час службовою таємницею цих органів. Персональні дані при передачі їх в органи державної влади також стають в той же час службовою таємницею цих органів. Інформація, яка становить особисту таємницю, в медичних установах стає лікарською таємницею.

Можна виділити первинні і вторинні види таємниць. До первинних видів таємниць відносяться особиста, комерційна, державна таємниці. Всі інші види таємниць вторинні, вони виникають при передачі первинних таємниць іншим власникам або користувачам.

2.7. Контроль якості інформації

Якісна виробнича інформація має деякі характеристики. До них відносяться цілісність, надійність і конфіденційність. Надамо ще раз суть цих понять, але вже з позицій поняття "якісна інформація".

Поняття цілісності означає, що інформація має точність до ступеня, очікуваної користувачем, є закінченою і вільна від неавторизованих змін. Відзначимо, що інформація не є вільною від помилок на всі 100%, але якість інформації виправдовує очікування користувача. Цілісність передбачає, що інформація захищена від недбалого поводження або навмисного несанкціонованого змінювання, що вона не обробляється за допомогою ненадійних програм і що дані контролюються на різних етапах обробки. Такі перевірки включають нумерацію пакетів, посилку підтверджень, перевірку достовірності, загальний контроль і заходи забезпечення безпеки.

Поняття надійності означає, що інформація отримана авторизованими користувачами, в потрібному місці і в потрібний час; що вона вільна від несанкціонованих змін, руйнування або копіювання. При неможливості проходження інформації через деякі ділянки система управління повинна бути в змозі замінити або обійти відповідний вузол або лінію зв'язку. Інфраструктура мережі, лінії зв'язку, центральні комп'ютери або периферійні робочі станції повинні бути захищені від фізичного або логічного нападу, яке може впливати на якість інформації або припинити її користування підприємством. Надійність також означає, що файли користувачів мережі і центральні бази даних періодично копіюються для запобігання незворотної втрати даних. Основні виробничі процеси повинні бути оборотними на випадок помилок обробки за допомогою певних процедур відновлення системи.

Поняття конфіденційності означає впевненість в тому, що дані в усіх формах (письмовій, електронній, ментальній) захищені від викрадення або несанкціонованого спостереження. У мережах це означає захист від прони-

кнення в контрольовані мережеві пристрої, файли і контури. Для обчислювальних мереж ступінь уразливості є високою, оскільки кожна робоча станція, сервери і кабельна структура можуть розглядатися як потенційні мішені для неавторизованого спостереження за даними. Конфіденційність також означає, що для захисту цінної інформації використовується шифрування при її проходженні по лініях зв'язку, які безпосередньо не контролюються власником інформації. Для важливої інформації, що проходить через міжмережеві з'єднання, шифрування є найважливішою виробничою вимогою.

Ось дії, які спільно утворюють елементи якості інформації: управління виробничою інформацією, як найважливішим ресурсом; якісне проектування системи для забезпечення ефективних інформаційних процесів; ефективне керівництво і контроль обробки і передачі інформації; захист інформації в системах обробки і передачі даних.

2.8. Класифікаційна політика у сфері інформації

Класифікаційна політика повинна указати імена та критерії для інформації так, щоб рішення щодо цінности інформації згідно списку основних її елементів були вільними від протиріч і одночасно достататньо строгими. Визначення класифікацій, які наведені в табл.2.2, є стислими і носять виключно ілюстративний характер.

Таблиця 2.2.

Приклад класифікаційної політики в сфері інформації

Класифікації	**Позначка конфіденційності**		
Суб'єктивні	**Для службового користування**	**Конфіденційна**	**Персональна**
Визначення	Розкриття може нанести в перспективі збиток економіці підприємства	Розкриття може нанести серйозний збиток економіці підприємства	Розкриття може негативно вплинути на співробітників та претендентів на посаду
Об'єктивні	**На зберіганні**	**На поточному контролі**	
Визначення	Неналежна якість може привести в перспективі до серйозних правових або економічних наслідків	Неналежна якість може оказати вплив на виробничу сферу	

Керівництво підприємства, безумовно, має розробити більш повний и всеосяжний опис для ефективної діяльності у сфері класифікації.

Контрольні запитання

1. Що таке загроза безпеки? Назвіть основні типи загроз.
2. Поясніть суть ненавмисних штучних загроз.
3. Поясніть суть навмисних штучних загроз на підприємстві?
4. Надайте класифікацію загрозам бепеки.
5. В чому суть моделі гіпотетичного порушника?
6. Розкажіть про види інформаціх, що захищаються у сфері управління.
7. Назвіть та поясніть суть поняття “якість інформації”.
8. Наведіть приклад класифікаційної політики у сфері інформації.

3. МЕХАНІЗМИ РЕАЛІЗАЦІЇ БЕЗПЕКИ

3.1. Джерела загроз інформаційної безпеки

Фактично, реалізація захисту має дві частини: код і настроювання (setup). *Код* – це програми в довірчій обчислювальній базі (в комплексі засобів захисту). Настроювання – це всі дані, які управляють операціями цих програм: списки контролю доступу, членство в групі, користувацькі паролі, ключі шифрування і т.д.

Задача реалізації захисту повинна бути спроможна протидіяти загрозам, які зустрічаються в трьох основних формах:

- погані (помилкові або ворожі) програми;
- погані (ворожі) агенти – користувачі (або програми), які надають хорошим, але легковірним програмам свідомо помилкові команди;
- погані агенти, які підключаються до комунікацій і заповнюють їх своїми повідомленнями.

У загальному випадку існують чотири стратегії захисту.

1. *Нікого не впускати*. Це повна ізоляція. Вона забезпечує найкращий захист, але перешкоджає використанню інформації або послуг від інших, і передачі їх іншим користувачам. Це непрактично для всіх.

2. *Не впускати порушників*. Програми всередині цього захисту можуть бути легковірними. Це дозволяє зробити електронні цифрові підписи програм і міжмережеві екрани (МЕ).

3. *Пустити порушників, але перешкодити їм в заподіянні шкоди*. Традиційним способом захисту служить динамічне ПЗ типу sandboxing на основі процесів операційної системи, або в сучасному вигляді, у віртуальній машині Java. Динамічне ПЗ типу sandboxing створює в комп’ютері захищений простір (sandbox), в якому може виконуватися підозрілий код, і в типовому випадку використовує контроль доступу до ресурсів, щоб визначити порушення. Програми, доступні із зазначеного захищеного простору, повинні мати підвищену стійкість.

4. *Захопити порушників і переслідувати їх*. Це роблять аудит і силові структури.

Так звана дискреційна (вибіркова, на основі списків, мандатна, розмежувальна) модель управління доступом забезпечує структуру для цих страте-

гій. У цій моделі диспетчер доступу управляє доступом запитів на обслуговування до ресурсів, які зазвичай вміщені в об’єктах, за наступною схемою: принципал (джерело запиту) → запитувана операція → диспетчер доступу (сторож) → об’єкт (ресурс).

Робота диспетчера доступу полягає в тому, щоб вирішити: чи може джерело запиту, зване принципалом, отримати доступ до об’єкта. Щоб вирішити це, використовують два види інформації: аутентіфікаційна інформація, яка ідентифікує принципала, і авторизаційна інформація, яка говорить, кому дозволено зробити щось на об’єкті.

У першому випадку, наприклад, якщо необхідно, щоб файлова система мала квоти (обмеження) на дискову пам’ять тільки для нових користувачів, є два способи це зробити: мати окремі методи для того, щоб писати з квотами і без, і не дозволяти новим користувачам записувати без квот; мати окремий об’єкт “квота”, який файлова система викликає за запитом користувача.

В іншому випадку конфіденційність повинна протистояти атакам з боку поганих програм. Цей варіант мандатного доступу організований за такою схемою: інформація (джерело) → диспетчер доступу (сторож) → принципал (стік). Вона, грубо кажучи, є протилежною першому випадку управління доступом. В ній сторож вирішує, чи може інформація текти до аутентифікованого принципалу.

У кожному випадку існують три основні механізми для здійснення захисту. Разом, вони формують “золотий стандарт”: аутентіфікація принципалів (хто це сказав?) або (хто отримує цю інформацію?); авторизація доступу (кому дозволено робити такі операції на цьому об'єкті?); аудит рішень диспетчера доступу, для того, щоб пізніше можна було з'ясувати, що трапилося і чому .

3.2. Сертифікація: створення захищеної роботи

Що означає зробити роботу захищеною? Відповідь заснована на понятті комплексу засобів захисту (КЗЗ) – набору апаратних засобів, програмного забезпечення та інформації з налаштування (setup), від якої залежить захист системи.

Взагалі кажучи, не просто з'ясувати, що повинно знаходитися в КЗЗ для даної політики захисту. Щоб захист працював досконалим чином, специфі-

кації для всіх компонент КЗЗ повинні бути досить серйозними, і кожен компонент повинен задовольняти своєї специфікації. Цей рівень сертифікації рідко досягається. По суті, часто погоджуються на щось набагато більш слабке. У будь-якому випадку, має бути ясно, що чим менше розмір КЗЗ – тим краще.

Хороший спосіб запобігання шкоди, що можуть заподіяти дефекти в КЗЗ – використовувати захист в глибину (ешелоновану оборону), тобто надлишкові механізми захисту. При цьому порушникові буде складно одночасно використовувати слабкості різних систем на всіх рівнях. Ешелонована оборона не дає строгих гарантій, але насправді, практично допомагає. Наприклад, система могла б включати:

- мережевий рівень безпеки;
- рівень безпеки ОС, використовуючи sandboxing, щоб ізолювати програми. Це може бути зроблено на базовій ОС, такій як Windows (або Unix), або на високорівневій ОС, яку має віртуальна машина Java;
- рівень безпеки програми, який додатково перевіряє авторизацію.

Більшість рішень щодо безпеки було зосереджено на програмних засобах. Але інший важливий компонент КЗЗ – інформація про конфігурацію, кнопки і вимикачі, які говорять програмному забезпеченню, що зробити (setup). Хоча настроювання набагато простіше ніж програма, воно зазвичай робиться менш кваліфікованими людьми, ніж розробники програм, і в той час, як програма написана одноразово, настроювання різне для кожної інсталяції. Проблема погіршується тим, що настроювання повинно бути засноване на документації для програмного забезпечення, яка є, зазвичай, великою за обсягом, не цілком ясною і неповною.

Єдине рішення цієї проблеми полягає в тому, щоб зробити частину настроювання, що відповідає за безпеку, більш простою як для адміністраторів, так і для користувачів. Не слід робити це, змінюючи базову ОС, так як зміни там важко здійснимі. Замість цього, можна використовувати в своїх інтересах модель безпеки з невеликим числом параметрів настроювання, і потім компілювати ці параметри в численні кнопки і вимикачі базової системи. Яку форму має прийняти ця модель?

Користувачі мають потребу в дуже простій моделі, приблизно з трьома рівнями захисту: я, моя група або підприємство, інші – з повноваження-

ми, які прогресивно зменшуються. Сьогодні браузери класифікують мережу саме таким чином. Персональна інформація, конфіденційні і відкриті відомості повинні бути в трьох частинах файлової системи: мої документи, документи моєї групи і загальні документи. Це комбінує захист даних з тією частиною файлової системи, де вони зберігаються так само, як в реальному світі. Наприклад, так зроблено з дошками оголошень, папками, замкнутими в столах і сейфами. Цей прийом знайомий усім, вимагає меншої роботи, при цьому відразу можна оцінити надійність захисту кожного елемента даних.

Адміністратори також потребують досить простої моделі, але вони потребують навіть ще більше в можливості обробити багато користувачів і систем однорідним способом, так як вони не можуть ефективно мати справу з великою кількістю індивідуальних випадків. Одним із способів є визначення, так званих, низькорівневих політик безпеки (НПБ), правил налаштування безпеки, які автоматично застосовуються до груп ПК. Вони включають наступне:

- кожен користувач має право на читання / запис у своїй домашній папці на сервері, і ніхто більше не має цей доступ;

- користувач, зазвичай, член однієї з робочих груп, який має доступ до групових домашнім папок на всіх машинах членів групи і на сервері;

- системні папки повинні містити набори файлів, які формують версію ПЗ (реліз), схвалену постачальником;

- всі виконувані програми повинні бути підписані повноважними сторонами.

Щоб робити НПБ керованими, адміністраторам треба визначати групи користувачів і ресурсів, на які вони претендують, і потім коротко сформулювати НПБ в термінах цих груп. В ідеалі, групи ресурсів відображені в структурі файлової системи, але повинні бути й інші шляхи до їх визначення, щоб прийняти до уваги химерні угоди щодо існуючих мереж, ОС і додатків.

Розробники потребують безпечну типизовану мову, яка подібна мові Java. Це усуне безліч дефектів програм. На жаль, більшість дефектів, які ушкоджують захист, знаходяться в системному програмному забезпеченні, яке, наприклад, забезпечує комунікації з мережами. Тому потрібно прагнути до того, щоб системні програми також записувалися подібним чином.

Контрольні запитання

1. Назвіть та поясніть 4 стратегії захисту інформації від загроз.
2. В чому полягає робота диспетчера при використанні дискреційної моделі?
3. В чому суть “золотого стандарту” захисту?
4. В чому суть поняття “комплекс засобів захисту (КЗЗ)?
5. Розкажіть про важливий компонент КЗЗ – інформацію про конфігурацію.
6. Чому не слід спрощувати частину системи захисту setup, яка відповідає за безпеку, шляхом змін базової ОС?
7. Що пропонує модель безпеки з невеликим числом параметрів настроювання для користувачів та адміністраторів?

4. ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ СФЕРИ ДЕРЖАВИ

4.1. Загальні відомості

За останні роки комп'ютер приніс серйозні зміни в технологію роботи з інформацією у виробничому середовищі. Більшість організацій має кілька великих комп'ютерів, розташованих на обчислювальних центрах. Ці великі комп'ютери, що забезпечують роботу з базами даних, пов'язані між собою за допомогою однієї або декількох мереж, що використовують ті чи інші доступні мережеві технології. Центральні процесори можуть відноситися до різних машинних архітектур, пристосованим для оптимального виконання конкретних програм. Мережі, що зв'язують цю суміш машин з різними операційними системами, дозволяють окремим співробітникам спільно використовувати дані з інформаційних банків даних і виконувати індивідуальні обчислювальні процеси на персональних комп'ютерах або робочих станціях. Крім того, локальні обчислювальні мережі (ЛОМ) об'єднують робочі станції і служби на виробничих територіях, всередині будівель і в функціональних підрозділах.

Можливі сотні робочих станцій або персональних комп'ютерів, пов'язаних один з одним, а також з центральними процесорами і серверами ЛВС. Якщо розглядати питання безпеки, то користувач, з'єднавшись з такою мережею, фактично стає адміністратором даних. Можна виділити дані, обробити їх за допомогою своих нетестованих прикладних програм і послати результат за будь-якою мережевою адресою. За допомогою персонального комп'ютера користувач може змінити свої права доступу і подолати існуючі процедури локального контролю.

4.2. Відмінності мережі від обчислювального центру

Вид, різноманітність і серйозність проблем, з якими зустрічаються при захисті інформації на мережевих комп'ютерах, помітно відрізняються від того, з чим мають справу на обчислювальних центрах або при роботі додатків в режимі поділу часу, де ряд термінальних пристроїв приєднаний до

центральної машині. Важливі відмінності з точки зору безпеки показані в табл. 4.1.

Таблиця 4.1

Відмінності мережі від обчислювального центру з позицій ІБ

Об'єкт	***Обчислювальний центр***	***Розподілена мережа***
Середа	*В межах ідентифікованої групи користувачів, які працюють з додатком*	*Потенційно відкрита через міжмережеві з'єднання*
Інформаційна база	*Визначена і контрольована*	*Невизначена: засоби контролю у користувача*
Інформаційний потік	*Двосторонній*	*Необмежений*
Фізичний контроль доступу	*Залежіть від фізичної структури банку даних*	*Відносно менш важливий, оскільки дані розподілені*
Логічний контроль доступу	*Захищає файли*	*Захищає файли і цілісність мережі*

На відміну від засобів фізичного і логічного контролю, зосереджених в одному місці, що типово для схеми безпеки обчислювального центру, мережа вимагає наступних заходів інформаційної безпеки:

- контроль доступу до всіх інформаційних файлів як по внутрішній, так і по зовнішній мережі;

- контроль роботи авторизованого працівника з файлом, з яким йому дозволено працювати;

- контроль доступу до мережевого трафіку;

- встановлення ефективних засобів ідентифікації та аутентифікації для кожного учасника, будь то фізична особа або логічний об'єкт, а також для кожного компонента мережі;

- контроль доступу до мережевих ресурсів (включаючи центри реєстрації та обліку, комунікаційні контролери, вхідні пристрої та різні сервери) як з центральних доменів, жорстко пов'язаних або безпосередньо підключених пристроїв, так з віддалених пунктів, по телефону або через міжмережеві з'єднання;

- контроль поширення інформації з метою запобігання її несанкціонованого розподілу або витоку до неавторизованих мережевих станцій або користувачів.

До захищених систем відносяться такі апаратні і програмні засоби, які розроблені з урахуванням вимог безпеки обробки інформації, що містяться у відповідних державних документах і є перевіреними в ході відповідних сертифікаційних випробувань (табл. 4.2).

Таблиця 4.2

Ризики безпеки і заходи, що використовуються в кожному випадку

Ризик	**Елементи безпеки**		
	Фізичні	**Технічні**	**Організаційні**
Неавторизований доступ до інформації на мережевих файлах	*захищені файл-сервери*	*система контролю доступу; шифрування входу в мережу*	*процес авторизації*
Прослуховування за допомогою фізичного підключення та реєстрації рівня випромінювання:	*захищені файл-сервери; екранування термінальних пристроїв*	*шифрування*	
Робота з файлом: неавторизована; авторизована, але недостатньо		*контроль доступу до файлу; гранульованість контролю входу в мережу*	
Несанкціонований розподіл інформації		*програмні обмеження, зв'язані з позначками конфіденційності*	*адміністративний контроль за використанням списків розсилки*
Несанкціоноване використання привілейованого доступу	*захищені мережеві пристрої*	*гранульованість контролю входу в мережу*	*обмеження привілегій*
Фізичний напад на мережеві компоненти	*захищені мережеві пристрої*		

4.3. Деталі реалізації

Доступ до файлів зазвичай контролюється через профіль користувача, який описує індивідуального користувача в термінах, пов'язаних з його роботою. Коли користувач підтверджує контролюючій системі необхідну ідентичність, використовуючи пізнавальний знак (наприклад, пароль або фізичний ідентифікатор, такий як відбиток пальця або пластикову карту),

система визначає права доступу користувача до інформації, звертаючись до наявної таблиці прав доступу.

В даний час ряд аутентифікаційних систем, розроблених для мережевого застосування, забезпечує захищений інтерфейс для універсальних комп'ютерів. У них користувач зазвичай має пластикову карту або генератор сигналу, який підтверджує сигнал від процесора, який підключається на центральному вузлі. Такі системи дозволяют координувати профіль користувача на центральному процесорі з процесом індивідуальної мережевої аутентифікації.

Контрольована активність на файловому рівні

Після підключення користувач може бути обмежений у своїй діяльності. Ці обмеження пов'язані з роботою, яка дозволена користувачеві. Наприклад, інспектор відділу кадрів може мати доступ до відомості по зарплаті в певному вузлі мережі, але не може змінювати значень виплат. У порівнянні з роботою користувача за одним комп'ютером, такі обмеження діяльності в середовищі ЛОМ набувають критичне значення, так як існує велика потенційна можливість того, що неавторизована сторона виявиться здатною знайти шлях до файлу.

Порядок дій:

- переконатися, що власник даних для кожного файлу встановив права діяльності кожного користувача або класу користувачів, що мають авторизований доступ;

- переконатися, що привілеї авторизованої діяльності відповідають поточним виробничим потребам. Одним із способів є періодичне отримання від власника даних сигналу про закінчення привілеїв. Це слід робити, щонайменше, один раз на рік для кожного файл-сервера ЛОМ.

Контрольована активність на рівні записів

Всередині файлу, записаного на диску файл-сервера ЛОМ, можна знайти різні набори записів. *Запис* – сукупність даних. Зазвичай записи зберігаються як бази або документи. *Базовий запис* – це документ, який пов'язаний з паперовим документом. Він може мати одну або кілька сторінок даних, що розміщуються як текст, таблиці, графіка або їх

комбінація. Один або декілька документів можуть бути збережені в файлі бази даних.

Для мінімальних цілей захисту слід обмежити доступ до секцій файлу, подібно до того, як це робиться у фізичному процесі роботи над письмовим документом. Бажано, з урахуванням комп'ютерної потужності, щоб можна було також визначати дозвіл при зверненні до вкладених розділів і записів. Таким чином, логічний носій файлів міг би бути відкритим для загального доступу, але, встановлюючи обмеження, засновані на аутентифікації користувача, можна було б відкидати доступ до окремих записів або документів. У багатьох випадках це бажано.

Контролюваний доступ до мережевого трафіку

У випадках, коли мережевий трафік повинен бути захищений, шифрування є єдиним ефективним засобом захисту. Шифрована інформація – потік даних, який кодується за допомогою проходження через складний алгоритм, що виробляє неповторюваний шифр. Шифрування зазвичай виконується автоматично комп'ютерними апаратними пристроями. У деяких випадках шифрування може виконуватися за допомогою сервісної програми.

Сьогодні ряд систем шифрування заснований на алгоритмі шифрування даних AES (Rijndael). Більш перспективна методика для мережевих додатків – система шифрування з відкритими ключами. Криптосистема з відкритим ключем використовує властивості великих простих чисел, щоб дозволити кожному користувачеві ввести ключ, потім розшифрувати або декодувати вхідні повідомлення, використовуючи другий, секретний ключ. Серед переваг такої системи – здатність підписати повідомлення (тобто довести ідентичність автора або справжність тексту) і усунення обтяжливих вимог щодо розподілу ключів.

Порядок дій:

- розуміти процес шифрування, доступний на вашій локальній обчислювальній мережі, або встановити програмне забезпечення, або обладнання для шифрування;

- визначити важливі / ризиковані операції мереж підприємства. Економно застосовувати шифрування в потрібному випадку. Випадкове важливе виробниче повідомлення може вважатися в безпеці, якщо воно змішане з

іншим трафіком. Але якщо важливі повідомлення часто зустрічаються в даному ланцюгу мережі, то шифрують цей ланцюг.

Встановлення ефективної ідентифікації та аутентифікації

Рішення полягає в використанні ідентифікаторів, в яких застосовується ієрархічний підхід, і які пов'язані з конкретним підрозділом. Розглянемо мережеве ім'я, яке складається з трьох частин: об'єкт, підрозділ (або інший організаційний рівень) і країна. Ім'я користувача могло б бути наступним "Василь Петренко / Виробництво / Україна". Слід звернути увагу, що дана проблема є більш складною, ніж традиційний ідентифікатор, який використовується для доступу до одиночного, автономного комп'ютера. З потенціалом для 10000 імен і 1000 положень, і з можливою наявністю декількох В. Петренків, гарантія унікальних ідентифікаторів вимагає планування. Той же самий підхід може використовуватися для інших об'єктів, наприклад, при використанні тієї ж самої організації і країни: "Принт-сервер_2 / Виробництво / Україна". Цей тип ідентифікатора нагадує схему адресації в мережі і дозволяє провести швидкий, ефективний пошук та ідентифікацію.

Аутентифікація відноситься до доведення необхідної тотожності. Хоча пароль – найтиповіший розпізнавальний знак, проте він має недоліки. Більш достовірна аутентифікація включає використання фізичних характеристик або біометричних даних, таких як відбитки пальців, голос, сканування сітківки, які не можуть бути змінені і, з великою достовірністю, унікальні. Кращими є також системи "запит-відповідь", які засновані на знанні користувачем процедури доступу, і фізичні розпізнавальні знаки, такі як кишенькові генератори коду, які скоординовані з центром безпеки мережі.

Але більшість мережевих систем на даний час продовжують використовувати парольну аутентифікацію, оскільки вона простіше і дешевше. При використанні паролів, слід переконати користувачів добре дотримуватися дисципліни. Сьогодні майже всі неавторизовані проникнення в мережеві комп'ютерні системи походять від недбалості в проектуванні (або реалізації) системи, включно з помилками користувачів, або нехтування парольною дисципліною. Для розумної ефективності паролі повинні складатися не менше ніж з шести символів, не бути легко вгадувані і змінюватися не рідше, ніж

кожні 90 днів. Чим довше пароль, тим більше складнощів для зловмисника, щоб його вгадати або обчислити.

Конструкція пароля прямо впливає на безпечний час, протягом якого користувач може відчувати безпеку від перехоплювача, який намагається вгадати (або обчислити) пароль. Як приклад можна стверджувати, що збільшення довжини пароля тільки на один символ помітно збільшує безпечний час: якщо очікуваний безпечний час для трехсімвольного пароля становить близько трьох місяців, безпечний час для пароля з чотирьох символів становить сімдесят вісім місяців.

Так само важлива форма пароля. Користувач повинен бути в змозі впевненно його пам'ятати (і не відчувати незручностей від неможливості його записувати), але пароль також повинен бути дуже складним для вгадування іншими. Телефонний номер шкільної подруги або назва вулиці – приклади правильних форм.

Контрольований доступ до мережевої інфраструктури

До цього підрозділу обговорювався логічний або електронний доступ до системи, але слід також дбати про фізичну безпеку доступу до інфраструктури мережі. Вона включає центри зв'язку, центри даних, мережеві сервери і комунікаційні світчи. *Всі ресурси ЛОМ повинні вважатися привілейованими*, *тобто випадкові користувачі не повинні отримувати дозвіл на доступ або маніпуляцію серверами ЛОМ. Ефективний фізичний контроль доступу в офісі є мінімальною вимогою. Кімнати, що містять мережеві контрольні вузли, такі як облікові, комунікаційні та файл-сервери, повинні строго контролюватися і спостерігатися. Доступ повинен обмежуватися особами, які формально уповноважені адміністратором мережі*.

Мережевим або системним адміністраторам необхідний привілейований доступ з метою супроводу системи. Ці привілеї повинні бути визначені на рівні, який дозволяє точно контролювати, хто і що може робити. Наприклад, системний адміністратор повинен бути обмежений привілеями, необхідними для виконання запропонованих завдань і не більше. Адміністратор, відповідальний за архівування файлів, наприклад, не повинен мати привілей доступу до облікового сервера або комунікаційним службам ЛОМ.

Строго кажучи, підключені принтери також мають перебувати в безпеці. Вартість і порядок логічних частин системи зводяться нанівець, якщо випадковий відвідувач може розглядати секретну інформацію, що контролюється у інших частинах системи. Рекомендується використання замкнутих приймачів або черг на друк, контрольованих паролями.

На деяких ЛОМ досвідчені користувачі, що мають фізичний доступ до мережевих облікових серверів, можуть змінити аутентифікатор і, таким чином, видаючи себе за справжнього користувача, мати доступ до захищених файлів цього користувача. Слід уважно стежити за скасуванням прав фізичного доступу і логічної аутентифікації при переході працівника на іншу роботу або звільнення з підприємства.

Порядок дій:

- планувати засоби підтримки мережі з урахуванням вимог безпеки та сервісного обслуговування. ЛОМ не може бути просто додана, подібно клавіатурі або дисплею. Потрібна серйозна адміністративна підтримка, така як персонал і приміщення з контроліаруемим доступом.

- організувати логічний доступ до мережевих пристроїв. Такий доступ може бути із самої мережі – авторизованими або менш важливими користувачами, або через телефонний зв’язок. Неправильне підключення до мережевих серверів або термінальних пристроїв для користувача може завдати серйозної шкоди обслуговування ЛОМ та її надійності.

Сувора мережева конфігураційна політика необхідна для контролю дозволених видів зовнішнього доступу. Загалом, будь-яке підключення ззовні до мережі підприємства має бути обмеженим, виходячи з функціональної діяльності і певної мережевої адреси користувача.

Захист від неавторизованих модемних з’єднань

Загальнодоступна телефонна мережа є готовим, зручним і дешевим способом для неавторизованих осіб спробувати отримати доступ до комп’ютерів і комп’ютерних мереж. Все, що потрібно, це – термінальний пристрій, модем і, звичайно, телефон. Багато ЛОМ для зручності пропонує з’єднання по телефону.

Захист від неавторизованих абонентів, які прагнуть отримати доступ до комп’ютера, а потім до мережі, залежить від контрольного пристрою

порту. На них часто посилаються, як на пристрої зворотного зв'язку, підкреслюючи цим одну з їхніх властивостей. Наприклад, Національне бюро стандартів США встановило шість типів контрольного обладнання портів.

Односторонні пристрої забезпечують контроль тільки з боку комп'ютера (або мережі) і мають такі різновиди.

1. Пристрої захисту хост-порту, поміщені між хостом і модемом або між модемом і телефоном. Вони містять таблицю паролів і можуть приховувати або маскувати хост, надаючи унікальне зображення екрану або відповідаючи так, що абонент не може з'ясувати, присутній комп'ютер на лінії чи ні. Ці пристрої можуть сигналізувати оператору про атаку. Вони не з'єднуються самостійно з абонентом.

2. Захищені модеми, контрольовані паролями, які являють собою модеми з підвищеними властивостями, оснащені пристроями для виконання зворотного зв'язку з абонентом після прийому пароля.

Двосторонні пристрої, в яких апаратний блок встановлений на обох кінцях лінії (абонента і хоста/мережі), мають такі різновиди.

1. Системи ідентифікації, в яких абонент повинен представити апаратний ключ або портативний пристрій для генерації аутентифікаційного коду, таким чином, завершуючи з'єднання.

2. Термінальні аутентифікаційні пристрої, які використовують додатковий пристрій, вбудований в термінал, або підключений до терміналу, щоб аутентифікувати цей пристрій для хоста. Ця аутентіфікація може використовуватися для обмеження користувача певними терміналами.

3. Лінійні шифрувальні пристрої, що запобігають неавторизованому трафіку і, отже, доступу, оскільки неавторизований абонент не має ключа для відправки правильних форм даних.

4. Пристрої аутентифікації даних і повідомлень, зазвичай маючих місце в електронних системах передачі платежів, які використовують електронний цифровий підпис. Це вимагає взаємної аутентифікації відправника та одержувача.

Застосування контрольних пристроїв порту, в дійсності, є доповненням до інших рівнів безпеки вже згаданим в цьому розділі. Повинен бути локально встановлений основний мережевий і файловий контроль, який повинен управлятися належним чином.

Порядок дій:

1. Встановити, як має управлятися мережа. Більшість виробничих програм ЛОМ вимагає наявності спеціального персоналу адміністративної служби для підтримки контролю доступу, встановлення рахунків користувачів, архівування файлів і т.д.

2. Обмежити число осіб, які мають особливі привілеї в мережі. Установити керівний контроль над цією авторизацією.

3. Встановити привілеї на досить гранульованому рівні так, щоб можна було отримати реальний контроль. Один системний адміністратор не повинен виконувати всі дії, відповідальність повинна бути розподілена всередині персоналу. Доступ до критичних об’єктів мережі повинен бути таким, щоб атака на найважливіші файли могла мати місце тільки в результаті змови.

4. Визначити, чи буде корисним в даній ситуації контрольний пристрій порту.

5. Підготуватися до ситуацій з підвищеним ризиком, коли особи, які обслуговують мережу, можуть бути відсутніми.

Контроль над розповсюдженням і витоком інформації

Потужність сучасних мереж і причина, за якій вони використовуються, щоб отримати максимальну вигоду від вкладення в комп’ютерні ресурси, полягає в здатності швидкої передачі інформації. Це також представляє проблему безпеки. Мережева інформація, отримана з бази даних або послана по електронній пошті, може легко вийти з-під контролю. Вона може помилково виявитися в поштовій скриньці іншої особи, або може бути зібрана, на перший погляд, з нешкідливих бітів даних в критично небезпечну інформацію, котра розкриває виробничі плани, стратегії ринку або бізнес-плани.

Існують три шляхи витоку інформації. По-перше, інформація може залишитися незахищеною в різних місцях мережі (мереж), що дозволяє цікавому користувачеві, навмисному зломщику або промисловому шпигунові збирати інформацію. Навіть маючи відносно низький рівень доступу, користувачі можуть бути в змозі перевіряти сотні місць в мережі, які містять інформацію.

По-друге, адреса призначення може містити помилку, в результаті якої інформація буде надіслана помилкового учаснику. Ще більшу небезпеку

становлять списки розсилки, тому що реальні отримувачі є відносно невидимими. У багатьох випадках у користувачів ЛОМ немає впевненості в тому, що члени списку розсилки відповідають поточній виробничій ситуації; деякі члени можуть находитися за межами мережі або навіть поза підприємством.

По-третє, слабкий контроль керівництва може дозволити використання мережі неідентифікованим об'єктам. Прикладом можуть бути так звані гостьові рахунки, які використовуються для демонстрації або для інших цілей. Якщо виробничі цілі виправдовують використання ЛОМ сторонніми особами, підприємство повинно встановити ефективний авторизаційний та ідентифікаційний контроль для подібних випадків. Наприклад, ідентифікатор гостя повинен явно показувати спонсора, можливо, таким чином: "Гість / Спонсор: Домен: Мережа".

Порядок дій.

1. Встановити процедури для розподілу особливо важливої інформації. Списки розсилки, в загальному випадку, не повинні використовуватися.

2. Вимагати, щоб кожен користувач був ідентифікований як фізична особа. Іншими словами, зробити явним, щоб кожну конкретну дію в мережі можна було б простежити аж до конкретного співробітника.

Контрольні запитання

1. Назвіть відмінності мережі від обчислювального центру з позиції ІБ.
2. Які заходи ІБ мають бути прийняті для мережі?
3. Що потрібно зробити для контролю доступу до файлів, які доступні як по внутрішній, так і по зовнішній мережі?
4. Чому необхідний контроль доступу до мережевого трафіка?
5. Що необхідно зробити для ефективної ідентифікації та аутентіфікаціі кожного учасника інформаційного обміну, будь то фізична особа або логічний об'єкт, а також для кожної компоненти мережі.
6. Що треба зробити для контролю доступу до мережевих ресурсів, особливо, по телефону?
7. Що рекомендуеться робити для запобігання витоку інформації?

5. ХАРАКТЕРИСТИКА СТАНДАРТІВ ІЗ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Наш час – період скептицизму. Особливо це відноситься до безпеки, оскільки багато заходів з безпеки визивають у людей досаду і здаються зайвими. Щоб позбавитися від подібних сумнівів, треба дотримуватися Правил безпеки або стандартів. Зрозуміло, що такі стандарти мають бути засновані на переконливих керівних вказівках (політиці), сприяючи створенню робочого середовища підприємства.

Не має значення те, що на підприємстві з метою ІБ застосовуються прямі розпорядження керівництва та системи фізичної і логічної безпеки. Від цього буде мало користі до тих пір, поки співробітники не переконаються, що правила є доречними і ефективними.

5.1. Характеристика ефективних стандартів з безпеки

Хороші стандарти з безпеки мають певні характеристики незалежно від того, де вони застосовуються. *Стандарти мають бути:*

- повними. Вони повинні включати всі обставини і ситуації, які відбуваються під час звичайних виробничих операцій.

- доступними. Вони повинні бути представлені співробітникам, як мотиватор і джерело детальної інформації.

- корисними. Стандарти повинні переконливо доводити, що вони дають внесок в виконання трудових обов'язків співробітників в повному обсязі.

- узгодженими. Вимоги захисту повинні бути узгодженими за різними видами діяльності підприємства та за різними типами і формами інформації.

- актуальними. Хороші стандарти з безпеки відображають сучасну технологію і практику поточних виробничих операцій.

- представленими в різних формах. Вони повинні бути доступні в різних формах так, щоб постійно підтримувалося живе, доречне і мотивоване спілкування.

Розглянемо докладніше, як можна забезпечити ці характеристики в програмі стандартів з безпеки.

Стандарти мають бути повними

Стандарти з безпеки повинні відображати всі ситуації та обставини, з якими можна зустрітися в діяльності підприємства. Розглянемо типове підприємство, де використовуються мережеві робочі станції на виробництві, в філіях і центральному відділенні підприємства, в дослідницьких лабораторіях, інженерних центрах, в торгових відділах, на складах і в багатьох інших місцях. Стандарти з безпеки повинні давати відповіді на питання: “Що слід виконати, щоб захистити інформацію підприємства?”

Це не означає, що слід публікувати окремий стандарт на кожну робочу ситуацію. Треба забезпечити стандартами ті випадки, які значно відрізняються за вимогами до безпеки. Одна з причин полягає в тому, щоб спростити доступ до правил з безпеки для всіх працівників. Не можна очікувати, щоб кожен секретар читав про речі, які призначаються фахівцям, і навпаки.

Можна розглянути двовимірну матрицю, що представляє вимоги до повноти ефективності стандартів з безпеки (табл. 5.1). По одній стороні відкладені основні типи робіт, які можуть включати роботу секретарів і конторських працівників, дослідний і інженерний персонал, адміністрацію, бухгалтерію, плановий відділ і так далі. По іншій стороні перераховані види діяльності, призначені для кожного типу робіт. Пункти матриці будуть відрізнятися для різних підприємств, але сама матриця є важливою, оскільки дозволяє бачити інструкції з безпеки, які повинні бути включені в стандарти для впевненості в їхній повноті.

Таблиця 5.1

Вимоги до повноти ефективних стандартів з безпеки

Процес	***Повнота ефективності***
Обмін повідомленнями	***Шифрування дуже важливих повідомлень***
Робота з файлами	***Захист паролем***
Створення документів	***Не застосовується***
Маркировка важливої інформації	***Створення позначок***
Використання списку розсилки, САПР і т.д.	***Не застосовується***

Остаточно, *повні стандарти повинні забезпечити необхідний інструментарій для контролю. Інспектори мають право очікувати, що співробітники додержуються опублікованих правил, які безпосередньо пов'язані з їх роботою*.

Стандарти мають бути доступними

Часто багато співробітників заявляють, що досить складно знайти документ або те місце в ньому, де конкретно вказано, що вони повинні робити з безпеки на своєму робочому місці. Це, зрозуміло, слабке виправдання, але й одночасно сигнал для розробників нормативних документів. Отримання стандартів з безпеки повинно бути в такій формі і в такий спосіб, який найбільш зручний в робочій обстановці, наприклад:

- стандарти з безпеки повинні бути в загальнодоступному файлі в мережі для співробітників, що працюють на настільних робочих станціях або персональних комп'ютерах. Для таких людей найзручніше читати стандарти з безпеки безпосередньо з файлу. Якщо стандарти запропоновані групою користувачів, то цей метод розміщення є найбільш зручним;

- стандарти з безпеки можуть бути опубліковані у виданні кишенькового формату і вручені при призначенні на роботу. Людям подобається брати в руки привабливо оформлену друковану продукцію. Можливо, що вона відразу ж буде переглянута;

- стандарти з безпеки можуть поширюватися через керівництво груп або підрозділів, наприклад, для всіх інженерів через старшого інженера. Використовуючи для доставки вертикаль керівництва (зверху вниз), можна зробити важливою будь-яку інструкцію. Коли начальник вручає директиву, малоймовірно, щоб вона відразу ж була б відкинута;

- кожен керівник з безпеки повинен мати довідник підприємства з безпеки. Ключем до розуміння повинно бути безпосереднє пояснення вимог з безпеки. Координатори та керівники з безпеки повинні бути готові відповісти на питання або, у важких випадках, знайти на нього відповідь.

Хороші стандарти повинні бути завжди доступні для тих, хто хоче отримати інформацію.

Стандарти мають бути корисними і актуальними

Взагалі-то, *створювати корисні стандарти нелегко*. Корисні стандарти не можуть бути розроблені в центрі або відділі безпеки, скоріше, вони можуть бути написані людьми, які мають практичний досвід у різних областях виробничої діяльності. Стандарти з безпеки можуть бути підготовлені комісією, що представляє різні робочі групи, підрозділи або види діяльності. Стандарти, які на 100 відсотків коректні в очах вищого керівництва або вищестоящого персоналу, можуть їх задовольняти, але з цього не випливає, що весь персонал підприємства буде дотримуватися їх автоматично.

Хороші стандарти узагальнюють весь позитивний досвід, накопичений на підприємстві. Наприклад, деякі керівники можуть вважати, що паролі слід міняти кожні 30 днів, але якщо цю вимогу інші групи вважатимуть необгрунтованою, то краще прийняти компромісне рішення – кожні 60 днів, ніж вимогу, яка неминуче буде ігноруватися деякими групами.

Корисний стандарт – це такий стандарт, до якого більшість співробітників відноситься як до практичного керівництва по роботі з інформацією, створюваної в оперативному середовищі або доступною в ході звичайної виробничої діяльності підприємства.

Крім того стандарти з безпеки завжди повинні бути узгоджені з іншими керівними вказівками і практичною діяльністю підприємства. Суперечливі інструкції або правила, які мають очевидні розбіжності, замість ефективного впливу на співробітників здатні зруйнувати їх інтерес до проблеми захисту інформації.

Добре написані керівні вказівки (політика) підприємства не повинні переглядатися частіше, ніж раз в 5 років. Якщо вони часто переглядаються, то, можливо, в них присутня велика домішка процедур або стандартів. З іншого боку, стандарти повинні регулярно переглядатися і оновлюватися. Мінімальний цикл, заснований на типових технологічних розробках і застосуваннях в сьогоднішньої виробничій сфері, вказує на перегляд стандартів кожні два роки. Прикладами додатків, які зажадали зміни стандартів, служать використання ЛОМ, завантаження даних в персональний комп’ютер, радіохвильове випромінювання від дисплеїв, а також застосування САПР. Нові технології та програми майже завжди сприяють критичному обговоренню стандартів з безпеки.

Актуальність стандартів з безпеки означає, що співробітники знайдуть в них відповіді на питання по сучасній економічній діяльності, новим технологіям і встановленим додаткам.

Стандарти мають бути представлені в різних формах

Стандарти з безпеки повинні бути опубліковані в окремій книзі, такий як керівництво з безпеки. Копії можуть бути поміщені в керівництво по операційним системам і в настільну книгу керівника з безпеки. Але копії стандартів не можуть бути ефективними для середнього співробітника з двох причин. Можливо, що йому немає необхідності переглядати зміст стандартів повністю, і у нього не було слушної нагоди скопіювати листи, які його цікавлять. Крім того, дані за межами палітурки або електронного файлу через деякий час втрачаються.

Стандарти з безпеки слід публікувати, як буклети, в зручному форматі, настільному або кишеньковому. Виклад матеріалу має бути направлений на конкретну аудиторію, наприклад, папка або листівка під назвою "Керівництво з безпеки для користувачів офісних систем". Буклети або листівки можуть поставлятися разом з інсталяцією обладнання.

У великій організації заслуговують на увагу періодичні публікації, що розглядають нові розробки з безпеки. Вони стимулюють готовність і нагадують співробітникам про стандарти. Плакати, оголошення та канцелярське приладдя (папки зі спеціальними наклейками, лінійки з написами і так далі) також є хорошим засобом нагадати співробітникам про важливість захисту інформації.

Ефективні стандарти, що містять важливі повідомлення, завжди повинні бути представлені в декількох різних формах, дозволяючи співробітникам вибрати ту, яка найбільш підходить до ситуації щодо захисту інформації.

5.2. Усна форма розповсюдження матеріалів зі стандартів

Мережа координаторів з безпеки є хорошим середовищем для поширення матеріалів зі стандартів. Люди слухають рівних собі більш уважно, ніж кого-небудь ще. Координатори з безпеки, будучи співробітниками на робочому рівні, знаходяться в чудовому стані для поширення матеріалів з безпе-

ки, листівок і плакатів, і пояснення співробітникам, чому так важливо їх участь. Як тільки захист інформації стає прийнятним на практиці більшістю співробітників, спостереження з боку оточуючих стає ефективною частиною контролю.

Підтримка безпечної роботи з інформацією усіма співробітниками в процесі роботи в мережі або використання інформаційних систем вимагає від них підготовки і зацікавленості. Створення відповідної комісії є найкращим способом розробки і періодичного поновлення цих стандартів.

Контрольні запитання

1. Які характеристики мають ефективні стандарти?
2. В чому суть повноти ідоступності стандартів?
3. В чому суть актуальності і корисності стандартів?
4. Для чого потрібні різні форми подання стандартів?
5. В чому суть усної форми розповсюдження матеріалів із стандартів?

6. РИЗИК РОБОТИ НА ПЕРСОНАЛЬНОМУ КОМП'ЮТЕРІ

Персональний комп'ютер (ПК), можливо, є найбільш значимим технічним досягненням в історії по своєму потенційному впливу на економіку. ПК, або, точніше, різні форми мікрокомп'ютерів, дозволяють в одному програмно-апаратному пристрої завантажувати дані (отримувати файли з центрального комп'ютера), виконувати локальну обробку за допомогою розроблених або куплених програм, зберігати їх, а потім знову направляти файли або елементи даних на центральний процесор. На додаток, *сучасна телекомунікаційна інфраструктура і ряд служб дозволяють користувачеві ПК майже з однаковою легкістю передавати інформацію як всередині свого відділу, так і по всьому світу. Все це означає, що слід заново переглянути концепцію інформаційної безпеки і ретельно спланувати, як слід застосовувати персональні комп'ютери*.

6.1. Визначення вразливих місць персонального комп'ютера

ПК в офісних компаніях мають такі ж вразливі місця, як ПК у великих організаціях (наприклад,в обчислювальному центрі), але ступінь захищеності в них менша через відсутність відділу безпеки. Як правило, функції контролю за ІБ виконує одна людина. Користувач офісного ПК може виконувати такі дії.

1. Отримати дані або файли з центрального комп'ютера або з приєднаного через ЛОМ файл-сервера. Фактично, ПК можна розглядати як віддалений термінал.

2. Обробити ці дані, використовуючи ПЗ підприємства (куплене, самостійно вироблене, вільно розповсюджуване або отримане через мережу хакерів). Програмне забезпечення, не вироблене і не перевірене на підприємстві відповідно до процедури сертифікації, повинно, в кращому випадку, вважатися підозрілим.

3. Спрямувати отримані результати в центральну інформаційну систему, файл-сервер ЛОМ, принтер, плоттер або через мережу в будь-яке місце земної кулі. Тобто існує реальний привід для занепокоєння, незалежно від того, чи буде занесений в журнал цей файл чи ні, і чи буде він, фактично, отриманий тією або іншою особою.

4. Комбінувати результати обробки з іншими файлами, котрі зберігаються локально, або на віддалених файл-серверах ЛОМ, або є файлами баз даних центрального комп'ютера. Стає ще важче ідентифікувати дані, що мають приховані помилки, оскільки вони змішані з іншою, офіційно санкціонованою інформацією.

5. Відкрити численні файли, які є загальними для користувачів мережі або для яких користувач має повноваження, витягувати інформацію і складати колекції даних. До тих пір, поки контроль доступу до файлів не буде широко застосовуватися і не стане ефективним, цікаві особи можуть наштовхуватися на секретні і, можливо, потенційно небезпечні поєднання елементів інформації.

6. Не маючи авторизованого доступу до файлів, користувач ПК може виявитися здатним локально запускати програми, що виробляють паролі доступу, і таким чином вторгнутися в контрольовані файли або процеси. Користувач ПК може виконати складні маніпуляції з контролем безпеки або обдурити авторизованих користувачів, щоб отримати права доступу, що належать іншим.

7. Виконувати всі процеси, перераховані в попередніх пунктах, працюючи вдома (використовуючи віддалений доступ до мережі по телефону), а також під час відрядження або подорожі (в готелі, через віддалений доступ по телефону, в літаку або в залі очікування аеропорту). Найбільш серйозною загрозою для конфіденційної інформації є доступ до комп'ютерної системи по телефону.

Розглянемо, кожен з цих пунктів (перелік не є повним) і покажемо для кожного випадку кілька способів, за допомогою яких можуть бути порушені вимоги якісної інформації підприємства.

Фізичні загрози включають: крадіжку даних на носіях або всієї системи цілком; випадкове спостереження секретної інформації на дисплеї ПК; крадіжку надрукованих документів і незаконне використання клавіатури або інших пристроїв введення для проникнення через засоби контролю безпеки і т.п.

Програмно-апаратні загрози включають: підрив операційної системи або її управління за допомогою незаконного (несанкціонованого) використання клавіатурного введення; підрив системи контролю ПК через віддале-

ний доступ або її оману, використовуючи мережеве з'єднання; розміщення троянських коней і часових бомб, які надійшли разом з вільним або придбаним ПЗ; втрату секретності даних в результаті несанкціонованого навмисного або випадкового перегляду файлів даних, які можуть перебувати на жорсткому диску ПК або на файл-сервері ЛОМ. Крім того розроблені вірусні програми, які можуть подорожувати по мережі від одного комп'ютера до іншого, попутно руйнуючи файли, або отримуючи управління операційною системою.

Організаційні загрози включають: розкриття даних через те, що користувач, недооцінивши значення локально створеної інформації, забув провести класифікацію відповідно до стандартів підприємства і забезпечити захист; вторгнення в контрольовані файли або робочі області через легко вгадувані паролі або тривале використання старих паролів, які вже розкриті; втрату або виявлення секретної інформації через те, що мережевий принтер недостатньо захищений, або користувачі ПК не забрали або не захистили надруковані документи; відсутність плану на випадок форс-мажорних обставин, таких як пожежа, крадіжка, втрата даних внаслідок технічних помилок файлової системи та ін.

Новий рівень ризику виникає, коли співробітники працюють вдома через мережеве з'єднання зі своїм відділом або сервером баз даних. Порядок в цьому випадку майже цілком грунтується на добрій волі співробітників слідувати правильній процедурі. Зупинити співробітника від передачі паролів членам сім'ї або від використання носіїв з даними підприємства для інших цілей в цих обставинах може тільки мотивація.

6.2. Мережевий захист персонального комп'ютера

В даний час безпека більшості обчислювальних центрів підтримується на досить високому рівні. Тут майже немає винятків. Встановлено численні рівні безпеки, як фізичної, так і технічної. Штат фахівців з безпеки і озброєна охорона роблять очевидним, що захист інформації відповідає стандартам підприємства з безпеки.

На протилежність ОЦ комп'ютери в звичайній комерційній фірмі знаходяться в приміщеннях, які практично відвідуються вільно. Слід відмітити, що комплекс персональних комп'ютерів середньої фірми, з'єднаний з ЛОМ,

яка пов'язана з файл-серверами, комунікаційними серверами і принтерами, є значно потужнішим, ніж середній обчислювальний центр. Однак там немає технічного штату з безпеки, немає центральної програмної системи безпеки, що має налагоджений супровід і містить профілі авторизованих користувачів, немає навіть закритих приміщень, куди дозволений доступ тільки авторизованому персоналу. Замість цього вся відповідальність покладається на колектив групи користувачів. Вони самі собі керівники обчислювального центру та посадові особи з безпеки. Безумовно, тут можна застосувати теорію слабкої ланки.

Ефективна безпека для ПК в мережі вимагає, щоб:

1) були встановлені правильні форми виробничої діяльності людей;

2) ця діяльність стала для них бажаною. Мотивація вже згадувалась, тому далі будуть розглянуті лише вимоги щодо безпеки для ПК.

6.3. Планування безпечної роботи на персональному комп'ютері

Треба визнати, що виробничі стосунки грунтуються на управлінні інформаційними засобами і вимагають прийняття певних рішень. Ці рішення по структурі, вартості та захисту інформації складають основу, на якій будується ефективна програма з безпеки ПК.

Оскільки прикладні завдання перейшли від великих комп'ютерів на ПК, а сучасні нові додатки розробляються для мереж ПК, керівництво повинно забезпечити процес, який гарантує продовження рівня якості інформації на основі стандартів.

Стандарти підприємства щодо використання ПК

Кожне підприємство має прийняти стандарти, які встановлюють засоби контролю за застосуванням ПК. До рішення керівництва, яке є попередньою умовою прийняття стандартів, має входити наступне.

1. *Аналіз ризику, що виникає на підприємстві внаслідок використання мережевих ПК, на роботі або в домашніх умовах*. Цей аналіз дозволить вивести основні вимоги політики в області ІБ. Настанови і стандарти, які розглядають використання ПК, повинні забезпечити механізм контролю, що гарантує персональну відповідальність користувача при роботі на ПК з інформацією підприємства.

2. *Процедура отримання, використання та контролю ПК*. Комп’ютери не повинні розглядатися, як простий елемент інформаційного устаткування відділу з кількох причин, які включають сумісність з іншим обладнанням і інформаційний контроль. Так як ПК дешеві, співробітники можуть купувати їх довільним чином, використовуючи гроші, які виділяються на потреби відділу. Підприємство повинно мати строгі правила щодо того, як потрібно придбати будь-яке комп'ютерне обладнання, або, більш того, підприємство має вказати, які ПК можна використовувати, з якими операційними системами можна працювати, а також обмеження, що накладаються на прикладні програми.

3. *Формальне ухвалення відповідальності співробітниками в разі, коли вони хочуть використовувати ПК або інший термінальний пристрій за межами підприємства*. З метою захисту інтересів виробництва кожен співробітник повинен підписати контракт, в якому обумовлюються його зобов’язання перед підприємством. Контракт повинен встановлювати в письмовій формі відповідальність співробітника щодо захисту інформації підприємства під час роботи з нею, і те, що співробітник обіцяє брати до уваги практику підприємства з безпеки. Порушення умов контракту може привести до юридичної відповідальності співробітника, що в подальшому може спричинити його звільнення із займаної посади.

4. *Засоби контролю, що перешкоджають випадковому доступу до мереж або великих комп’ютерів*. Звичайно, підприємство не може контролювати діяльність кожного співробітника, але воно може контролювати доступ до портів комп’ютера, а це, за суттю, пункт контролю за сполуками ПК з серверами баз даних або мережами.

Одним із способів захисту є застосування однієї з систем контролю порту, доступних в даний час. Інший спосіб вимагає від користувача наявності електронного ключа, який генерує код в процесі аутентифікації. Така система гарантує точну ідентифікацію незалежно від того, яке обладнання використовується або з якого місця запитується доступ.

5. *Опубліковані керівні вказівки щодо використання ПЗ з місць поза підприємства*. Це важливо для гарантії підтримки контролю, особливо коли пристрої з’єднані з мережами. Системи так званих електронних дошок оголошень пропонують безкоштовне (умовно-безкоштовне) ПЗ, яке користувача

просять оплатити. Застосування таких програм є дуже ризикованим; підприємство повинно чітко встановити в письмовій формі в контракті з кожним співробітником зобов'язання не використовувати ПЗ, яке не отримало офіційного схвалення.

Програмне забезпечення для ПК не тільки є джерелом фінансових витрат, але також може представляти джерело занепокоєння для підприємства, якщо співробітники порушують контрактні зобов'язання, прийняті при покупці ПЗ для виробничої діяльності. Все програмне забезпечення для ПК, таке як утиліти для операційних систем або прикладні програми (такі як розроблені програмістами підприємства системи аналізу кошторисів) мають бути захищені. Слабкі сторони програмного забезпечення ПК включають:

- нелегальне копіювання або нелегальне застосування ПО, яке має авторські права і куплено за ліцензією;

- потайна зміна операційної системи, контролю безпеки або прикладної програми на диску для обману або з іншими таємними цілями;

- втрату ПО, що настала як внаслідок необдуманого перезапису або стирання програм, так і крадіжки диска.

Програми повинні бути захищені так само, як дані. Диски повинні мати маркування, включаючи при необхідності відповідну мітку класифікації. Вони повинні зберігатися в певному порядку, так щоб можна було помітити відсутній диск. Слід подумати щодо замкнутих кабінетів і висувних полиць для безпечного зберігання дисків, що не використовуються.

Ряд важливих вимог з контролю за ІБ включають наступне.

1. *Для виконання виробничих завдань слід використовувати тільки ті ПК і такі пакети програм, які отримали схвалення інформаційного керівництва підприємства*. ПК підприємства можуть використовуватися тільки для виробничих цілей підприємства. Якщо співробітник має власний ПК, то в керівних вказівках слід зазначити, можливо чи ні його використання для виробничих цілей, і якщо так, то як повинна контролюватися інформація. Спільне використання ПК працюючим співробітником і членами його сім'ї не є правильною ідеєю.

2. *Класифікована інформація не повинна бути отримана або введена з віддаленого терміналу*. Для комп'ютера шлях повідомлення або файлу, який

отримує аутентіфікований користувач не має значення, проте цей шлях дуже важливий з точки зору безпеки.

3. *Класифікована інформація не повинна оброблятися в присутності сторонніх осіб в приміщенні*. Це є більш загальним правилом, яке застосовується також при роботі всередині підприємства. Воно може бути застосовано в кожному випадку.

4. *Кожен співробітник несе персональну відповідальність за захист класифікованої інформації і за належне використання спеціальних заходів безпеки*. Індивідуальне розуміння і бажання використовувати надійні інструкції з безпеки є головними вимогами при експлуатації мереж. Співробітники повинні бути забезпечені заходами безпеки.

5. *Кожен користувач повинен отримати унікальний ідентифікатор і аутентифікатор перед тим, як увійти в мережу*. Повноваження не повинні використовуватися спільно; паролі або інші маркери повинні оберігатися самим користувачем.

6. *Паролі повинні зберігатися в таємниці і періодично змінюватися відповідно до стандартів підприємства*.

7. З'єднані ПК повинні бути відключені від мережі або переведені в пасивний стан, якщо пристрій залишився без нагляду. Мережа самостійно може встановити тайм-аут, якщо відсутність активності не викликає сумнівів.

8. Періодично керівництво повинно заново розглядати підтвердження для роботи кожного співробітника на ПК. Володіння і використання ПК на роботі має бути регулярним пунктом ревізій на підприємстві. Хорошим способом перевірки використання ПК поза підприємства, можливо, служать періодичні обстеження доступів "за викликом" в системних протоколах.

Практичні заходи безпеки для ПК

Як було сказано раніше, слід розділяти заходи безпеки, що необхідні різним рівням елементів безпеки, на фізичні, логічні і процедурні заходи безпеки. Розглянемо ці рівні детальніше.

Фізичні заходи

Приміщення, в яких перебувають ПК, повинні мати безпеку відповідно до ступеня секретності оброблюваної інформації. За винятком інформації

вищого значення, яка може зажадати спеціальних зусиль, ПК, встановлені у відділі, зазвичай забезпечуються середнім ступенем захисту.

Обладнання повинно мати кріплення безпеки для закріплення пристрою на столі або на підлозі. Відсутність його допускається в разі, коли приміщення вважається безпечним при відсутності людей в приміщенні. Для стрічок і дисків слід передбачити безпечне сховище. Це сховище повинне мати той же рівень захисту, як і для документів, що мають цю класифікацію. У більшості випадків, інформація вищого значення має зберігатися в сейфі або замикається кабінеті. ПЗ є дорогим і зберігається аналогічно важливих даних.

Носії, які були використані для секретної інформації, не повинні повертатися виробникові або продаватися як утиль. Незалежно від того, які дії були виконані по стиранню інформації на дисках, можуть бути знайдені технічні способи її витягнення. Більшість команд тільки викреслює заголовки файлів і входи в таблиці посилань, а самі дані залишаються на диску.

У деяких випадках потрібно блокування апаратури (наприклад, відключення блоку живлення). Перевага елементів безпеки різних рівнів в тому, що можна розробити просте економічне рішення. Простий замок на ПК може служити таким рішенням, особливо в приміщеннях, що охороняються.

Програмно-апаратні заходи

Ряд операційних систем ПК (наприклад, Windows) були розроблені для зручності користувача, а не для безпеки інформації. Більшість ПК (за винятком останніх, потужних моделей) не має системної організації, яка ефективно пристосована для розміщення механізмів безпеки. Можна сказати, що більша частина засобів контролю ПК просто не є надійною і не призначена для безпечного управління системними ресурсами або даними. Наприклад, дискова операційна система ПК має покажчики статусу файлів, такі як “тільки читання” або “прихований”. Вони забезпечують деякий вид контролю (залежить від особистого розсуду), але, маючи мінімальні технічні навички, можна легко маніпулювати прапорцями операційної системи, які контролюють ці стани. Файли на ПК, щойно отриманих від виробників, слід вважати доступними для будь-якого, хто має фізичний доступ до машини.

Щоб контроль доступу був ефективним, необхідно забезпечити засоби аутентифікації кожного користувача. Звичайно, в разі, коли тільки одна особа використовує ПК і контролює доступ до нього, можна обійтися без цього.

Пакети програм з безпеки мають широкий спектр додатків. Адміністратор ПК може встановити і контролювати різні рівні привілеїв. Директорії з секретними файлами можуть бути приховані, так що випадковий користувач не зможе побачити імена файлів. Як опція, пропонується шифрування файлів. У табл. 6.1 проводиться порівняння деяких операційних систем ПК і пропонованих послуг.

Таблиця 6.1

Порівняння операціних систем ПК і пропонованих послуг

ОС	Переваги	Недоліки та коментарі
MS-DOS	*Велика база ПЗ, деревоподібна структура директорій, розумні повідомлення про помилку, можливість управління завданнями*	*Немає контролю доступу, але може бути підключений. Служить й досі для цілей освіти*
UNIX	*Розрахована на багато користувачів, багатозадачна, реалізується у великих/міні/мікро варіантах, ПК, захист файлів, контроль доступу, підтримка реляційних баз даних*	*Не дуже дружня до користувача оболонка, вимагає значних ресурсів ПК. Недостатній обсяг ПЗ для сфери бізнесу, немає блокування рівня запису*
Windows, OS/2	*Розрахована на багато користувачів, багатозадачна, захист файлів, контроль доступу, СУБД з мовою SQL, блокування записів*	*Потребує значних ресурсів ПК*

Системи шифрування, переважно, використовують аутентифікацію повідомлень, є важливими у випадках, коли ПК використовується для комунікацій стратегічного характеру або для обробки виробничої інформації з високим рівнем цінності. Шифрування є вищим ступенем захисту, відомої на даний час, але воно вимагає суворого управління ключами шифрування. При втраті ключів одночасно втрачається й інформація.

Організаційні заходи

Всі користувачі ПК, а також власники, повинні бути ідентифіковані з метою керівного контролю. Користувачі повинні підписати заявку на апа-

ратні та програмні засоби і заяву про відповідальність. Серійний номер і місце розташування кожного ПК повинні бути записані і періодично перевірятися.

Мережеві засоби контролю і засоби контролю центрального комп'ютера повинні коректуватися згідно з поточними призначень співробітників. Повинен діяти процес, який гарантує зміну або скасування повноважень при звільненні працівника або переведення його на іншу роботу.

Повинні бути розроблені і ретельно перевірені плани на випадок форс-мажорних обставин для відновлення необхідної виробничої інформації в разі, якщо пожежа або інше лихо виведуть з ладу засоби ПК. Від користувачів необхідно вимагати зберігання резервних дисків, процедур, програм і т.п. для гарантії відновлення.

Локально розроблені програми (наприклад, прикладні програми, розроблені користувачем для виконання виробничого завдання) повинні пройти перевірку на якість до початку застосування. Таке локальне ПО зазвичай не має переваг формальної сертифікації, прийнятої в професійних групах програмістів і розробників систем. Текст може містити серйозні помилки, як випадкові, так і навмисні. До схвалення керівництвом використання даних у виробничих цілях, слід провести об'єктивну перевірку і випробування цих програм, можливо комісією вищестоящої організації.

Кожен користувач ПК повинен знати вимоги з безпеки, отримані при персональній підготовці або ж викладені в брошурі або листівці.

Безпека і з'єднання

Насамкінець розділу розглянемо проблему безпеки при роботі в глобальній мережі, такий як Інтернет. *Фактично мережа Інтернет з'єднує корпоративну мережу з усім світом, тому проблему безпеки важко переоцінити.*

Безпека мережі Інтернет забезпечує інформаційні систем підприємств від несанкціонованого доступу. Наприклад, міжмережеві екрани здатні встановити різницю між дозволеним трафіком, скажімо до веб-сторінок або електронної пошти, і забороненим, таким, як запити на читання файлів корпоративних файл-серверів або ПК клієнтів робочих груп.

Ще раз зазначимо, що *ПК та інші мікрокомп'ютерні пристрої забезпечують величезне зростання обробки інформації і виробничих комунікацій. В свою чергу, в разі з'єднання з мережами (в т.ч. Інтернет), ці пристрої створюють серйозну загрозу для безпеки інформації. Необхідна ретельна увага керівництва, щоб встановити вимоги безпеки і контролю над зовнішніми мережами, переконати співробітників діяти, як вимагають посадові інструкції і нормативні документи*.

Контрольні запитання

1. Які дії виконує користувач ПК і як можна зменшити негативні наслідки (ризик ІБ) від цих дій?
2. Назвіть найбільш вразливі місця користувача при роботі на ПК в мережі.
3. В чому суть мережевого захисту ПК?
4. Що має входити до рішення керівництва в якості попередньої умови прийняття стандартів з ІБ?
5. Назвіть слабкі сторони програмного забезпечення ПК.
6. Назвіть важливі вимоги для зменшення ризику небезпеки при роботі на ПК.
7. В чому суть фізичних заходів для для посилення ІБ підприємства?
8. В чому суть програмно-апаратних заходів посилення ІБ (зменшення ризику небезпеки)?
9. В чому суть організаційних заходів для зменшення ризику інформаційної небезпеки?
10. Яким чином можна зменшити інформаційний ризик при користуванні мережею Інтернет?

7. ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1. Загальні відомості

Засоби захисту інформації – це сукупність інженерно-технічних, електричних, електронних, оптичних та інших пристроїв і пристосувань, приладів та технічних систем, які використовуються для вирішення різних завдань із захисту інформації, в тому числі попередження витоку і забезпечення безпеки захищаємої інформації.

В цілому кошти забезпечення захисту інформації в частині запобігання навмисних дій в залежності від способу реалізації можна розділити на групи: технічні (апаратні), програмні, змішані апаратно - програмні, організаційні.

Технічні (апаратні) засоби – це різні за типом пристрої (механічні, електромеханічні, електронні та інші), які апаратними засобами вирішують завдання захисту інформації. Вони перешкоджають фізичному проникненню, або, якщо проникнення все ж відбулося, перешкоджають доступу до інформації, в тому числі за допомогою її маскування. Першу частину завдання вирішують замки, грати на вікнах, захисна сигналізація та ін. Другу – генератори шуму, мережеві фільтри, скануючі радіоприймачі і безліч інших пристроїв, які “перекривають” потенційні канали витоку інформації або дозволяють їх виявити. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб’єктивних факторів, високу стійкість до модифікації.

До теперішнього часу розроблено значну кількість технічних (апаратних) засобів різного призначення, проте найбільшого поширення набули наступні:

- спеціальні регістри для зберігання реквізитів захисту: паролі, що ідентифікують коди, грифи або рівні секретності;
- пристрої вимірювання індивідуальних характеристик людини (голоси, відбитки пальців і т.д.) з метою її ідентифікації;
- схеми переривання передачі інформації в лінії зв’язку з метою періодичних перевірок адреси видачі даних;
- пристрої для шифрування інформації (криптографічні методи).

Слабкі сторони апаратних засобів захисту – недостатня гнучкість, відносно великі обсяг і маса, висока вартість.

Програмні засоби включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін. Переваги програмних засобів – універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку. Недоліки – обмежена функціональність мережі, використання частини ресурсів файл-сервера і робочих станцій, висока чутливість до випадкових або навмисним змін, можлива залежність від типів комп'ютерів (їх апаратних засобів).

Змішані апаратно-програмні засоби реалізують ті ж функції, що апаратні і програмні засоби окремо, і мають проміжні властивості.

Організаційні засоби складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу до неї та ін.) і організаційно-правових (національні законодавства і правила роботи, що встановлюються керівництвом конкретного підприємства). Переваги організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають необмежені можливості модифікації і розвитку. Недоліки – висока залежність від суб'єктивних чинників, в тому числі від загальної організації роботи в конкретному підрозділі.

За ступенем поширення і доступності виділяються програмні засоби. Інші засоби застосовуються в тих випадках, коли потрібно забезпечити додатковий рівень захисту інформації.

7.2. Принципи інженерно-техничного захисту інформації

Загальновідомо, що відділам безпеки, які займаються захистом інформації, протистоять різні організації і зловмисники, як правило, оснащені апаратними засобами доступу до інформації. Виходячи з цього, основу захисту інформації повинні складати принципи, аналогічні принципам отримання інформації, а саме:

- безперервність захисту інформації. Характеризується постійною готовністю системи захисту до відбиття загроз інформаційній безпеці в будь-який час;

- активність, яка передбачає прогнозування дій зловмисника, розробку і реалізацію випереджаючих захисних заходів;

- скритність, що виключає ознайомлення сторонніх осіб із засобами і технологією захисту інформації;

- цілеспрямованість, яка передбачає зосередження зусиль щодо запобігання загроз найбільш цінної інформації

- комплексне використання різних способів і засобів захисту інформації, що дозволяє компенсувати недоліки одних перевагами інших.

Ці принципи хоча і не містять конкретних рекомендацій, проте визначають загальні вимоги до способів і засобів захисту інформації.

Наступна група принципів характеризує основні професійні підходи до організації захисту інформації, забезпечує раціональний рівень її захисту і дозволяє: скоротити витрати на відповідність рівня захисту цінності інформації, включаючи гнучкість захисту (можливість модифікації); багатозональність захисту, що передбачає розміщення джерел інформації в зонах з контрольованим рівнем її безпеки; багаторубіжність захисту інформації на шляху руху зловмисника або поширення носія.

При побудові системи захисту інформації потрібно враховувати також наступні принципи:

- мінімізація додаткових завдань і вимог до співробітників організації, викликаних заходами щодо захисту інформації;

- надійність в роботі технічних засобів системи, що виключає як нереагування на погрози (пропуски загроз) інформаційної безпеки, так і помилкові реакції при їх відсутності;

- обмежений і контрольований доступ до елементів системи забезпечення інформаційної безпеки;

- безперервність роботи системи в будь-яких умовах функціонування об’єкта захисту, в тому числі, наприклад, короткочасному відключенні електроенергії;

- адаптованість (пристосовність) системи до змін навколишнього середовища.

Сенс зазначених принципів очевидний, але слід зупинитися докладніше на останньому. Справа в тому, що закрита інформація про способи і засоби захисту інформації в конкретній організації з часом набуває розголосу все

більшої кількості людей, в результаті чого збільшується ймовірність попадання цієї інформації до зловмисника. Тому доцільно проводити зміни в структурі системи захисту інформації періодично або при появі досить реальної можливості витоку інформації про систему захисту, наприклад, при раптовому звільнення інформованого співробітника служби безпеки.

7.3. Методи захисту інформації технічними засобами

У загальному випадку захист інформації технічними засобами забезпечується в наступних просторово-часових рамках і умовах:

- джерело і носій інформації локалізовані в межах об'єкта захисту, забезпечена механічна перешкода від контакту з ними зловмисника або дистанційного впливу на них полів технічного характеру;

- співвідношення енергії носія і перешкод на виході приймача каналу витоку таке, що зловмиснику не вдається зняти інформацію з носія з необхідною для її використання якістю;

- зловмисник не може виявити джерело або носій інформації;

- замість правдивої інформації зловмисник отримує неправдиву, яку він приймає як справжню.

Цей перелік реалізують такі методи захисту, як перешкоджання безпосередньому проникненню зловмисника до джерела інформації за допомогою інженерних конструкцій, технічних засобів охорони, а також приховування достовірної інформації.

Приховування інформації передбачає такі зміни структури і енергії носіїв, при яких зловмисник не може безпосередньо або за допомогою технічних засобів виділити інформацію з якістю, достатньою для використання її у власних інтересах. Розрізняють інформаційне та енергетичне приховування.

Інформаційне приховування досягається зміною або створенням помилкового інформаційного портрета семантичного повідомлення, фізичного об'єкта або сигналу. Інформаційним портретом можна назвати сукупність елементів і зв'язків між ними, що відображають зміст повідомлення (мовного або даних), ознаки об'єкта або сигналу.

Зміна інформаційного портрета об'єкта викликає зміну зображення його зовнішнього вигляду (видових демаскируючих ознак), характеристік випро-

мінюваних їм полів або електричних сигналів (ознак сигналів), структури і властивостей речовин. Ці зміни спрямовані на зближення ознакових структур об'єкта і навколишнього його фону, в результаті чого знижується контрастність зображення об'єкта по відношенню до фону і погіршуються можливості його виявлення і розпізнавання.

Однак при зміні інформаційного портрета інформація не сприймається не тільки зловмисником, а й її санкціонованим одержувачем. Отже, для нього інформаційний портрет повинен бути відновлений шляхом додаткової передачі йому віддалених елементів і зв'язків або алгоритму (ключа) цих змін.

Інформаційне приховування дозволяє: істотно зменшити обсяг інформації, що захищається і тим самим спростити проблему захисту інформації; використовувати в рекламі нової продукції відомості про неї, не побоюючись розголошення. Наприклад, замість захисту інформації, що міститься в сотнях і тисячах аркушів технічної документації, яка розробляється для виробництва нової продукції, захисту підлягають лише кілька десятків листів з інформаційними вузлами.

Інший метод інформаційного приховування полягає в трансформації вихідного інформаційного портрета в новий, з помилковою семантичною інформацією або помилковою ознаковою структурою, і "нав'язуванні" нового портрета органу розвідки або зловмиснику. Такий метод захисту називається *дезінформуванням*.

Принципова відмінність інформаційного приховування шляхом змін інформаційного портрета від дезінформування полягає в тому, що перший метод спрямований на утруднення виявлення об'єкта з інформацією серед інших об'єктів (фону), а другий – на створенні на цьому фоні ознак помилкового об'єкта.

Дезінформування відноситься до числа найбільш ефективних способів захисту інформації, однак цей метод захисту практично складно реалізувати. Основна проблема полягає в забезпеченні достовірності помилкового інформаційного портрета. Дезінформування тільки в тому випадку досягне мети, коли у розвідки (зловмисника) не виникне сумніву в істинності неправдивої інформації, яку йому підсовують. В іншому випадку може бути отриманий протилежний ефект, так як при розкритті розвідкою факту дезінформування отримана помилкова інформація звузить область пошуку правдивої

інформації. Тому до організації дезінформування необхідно ставитися дуже серйозно, з урахуванням того, що споживачі інформації чітко уявляють збиток від дезінформації і при найменших сумнівах будуть перевіряти інформацію з використанням інших джерел.

Іншим ефективним методом приховування інформації є енертичне приховування. Воно полягає в застосуванні способів і засобів захисту інформації, що виключають або ускладнюють реалізацію енергетичного розвідувального контакту.

Енергетичне приховування досягається зменшенням відносини енергії (потужності) сигналів, тобто носіїв з інформацією (електромагнітного або акустичного полів і електричного струму) і перешкод. Зменшення відносини сигнал / перешкода можливо двома методами: зниженням потужності сигналу або збільшенням потужності перешкоди на вході приймача. Вплив перешкод призводить до зміни інформаційних параметрів носіїв: амплітуди, частоти, фази. Якщо носієм інформації є амплітудно-модульована електромагнітна хвиля, а в середовищі поширення каналу присутня перешкода у вигляді електромагнітної хвилі, що має однакову з носієм частоту, але випадкову амплітуду і фазу, то відбувається інтерференція цих хвиль. В результаті цього амплітуда сумарного сигналу випадковим чином змінюються, тобто інформація спотворюється.

Найбільш жорсткі вимоги до якості інформації пред’являються при передачі даних (міжмашинного обміну): ймовірність помилки символу по плановим завданням, завданням статистичного і бухгалтерського обліку оцінюється порядку 10^{-5} - 10^{-6}, по грошовим даними 10^{-8}-10^{-9}. Для порівняння, в телефонних каналах хороша складова розбірливість мови забезпечується при 60-80%, тобто вимоги до якості інформації, що приймається істотно менш жорсткі. Ця різниця зумовлена надмірністю мови, яка дозволяє при пропуску окремих звуків і навіть складів відновлювати мовне повідомлення. Ймовірність помилки знака 10^{-5} досягається при його передачі двійковим амплітудно-модульованим (АМ) сигналом і відношенням потужності сигналу до потужності флуктуаційного шуму на вході приймача приблизно 20 дБ, при передачі ЧМ сигналом – близько 10 дБ. Для забезпечення розбірливості мови близько 85% перевищення амплітуди сигналу над шумом має становити бли-

зько 10 дБ, для отримання задовільної якості факсимільного зображення – приблизно 35 дБ, якісного телевізійного зображення – більш 40 дБ.

У загальному випадку при зменшенні відносини сигнал / шум до одиниці і менше якість інформації настільки погіршується, що вона не може практично використовуватися. Для конкретних видів інформації і модуляції сигналу існують граничні значення відносини сигнал / перешкода, нижче яких забезпечується енергетичне приховування інформації.

7.4. Канали витоку інформації

Можливі канали витоку інформації можна розбити на чотири групи.

1-а група – канали, зв'язані з доступом до елементів системи обробки даних, але не потребують зміни компонентів системи. До цієї групи належать канали: дистанційного прихованого відеонагляду або фотографування; застосування підслуховуючих пристроїв; перехоплення електромагнітних випромінювань та наведень і т.д.

2-а група – канали, зв'язані з доступом до елементів системи і змінами структури її компонентів. До другої групи належать: спостереження за інформацією з метою її запам'ятовування в процесі обробки; розкрадання носіїв інформації; збір виробничих відходів, що містять оброблювану інформацію; навмисне зчитування даних з файлів інших користувачів; читання залишкової інформації, тобто даних, що залишаються на магнітних носіях після виконання завдань; копіювання носіїв інформації; навмисне використання для доступу до інформації терміналів зареєстрованих користувачів; маскування під зареєстрованого користувача шляхом викрадення паролів та інших реквізитів розмежування доступу до цінної інформації; використання для доступу до інформації так званих "лазійок", тобто можливостей обходу механізму розмежування доступу, що виникають внаслідок недосконалості загальносистемних компонентів програмного забезпечення (операційних систем, систем управління базами даних та ін.) і неоднозначність мов програмування, які застосовуються в автоматизованих системах обробки даних.

до 3-ої групи належать: незаконне підключення спеціальної реєструючої апаратури до пристроїв системи або ліній зв'язку (перехоплення модемного і факсимільного зв'язку); *зловмисна зміна програм таким чином, щоб ці програми поряд з основними функціями обробки інформації здійснювали та-*

кож несанкціонований збір і реєстрацію інформації, що захищається; зловмисне виведення з ладу механізмів захисту.

до 4-ої групи належить несанкціоноване отримання інформації шляхом підкупу чи шантажу посадових осіб відповідних служб, співробітників, їх знайомих, обслуговуючого персоналу або родичів, які знають про рід діяльності.

7.5. Засоби забезпечення ІБ в комп'ютерних системах

Пристрій для швидкого знищення інформації на жорстких магнітних дисках "Стек-Н"

Призначений для швидкого стирання інформації, записаної на жорстких магнітных дисках, як для таких, що експлуатуються, так і не експлуатуються в момент стирання (рис. 7.1). Основні особливості пристроїв цієї серії:

Рис. 7.1.

- гранично можлива швидкість знищення Інформації, відсутність рухомих частин;
- здатність перебувати в режимі "Готовності" як завгодно довго без погіршення характеристик;
- можливість застосування в дистанційно керованих системах з автономним електроживленням;

Стирання інформації, записаної на магнітному носії, відбувається без його фізічного руйнування, але подальше використання диска стає проблематичним. Для порівняння надамо основні характеристики пристрою Стек-НС1:

максимальна тривалість переходу в режим "Готовність" - 7 ... 10 с .;
тривалість стирання інформації на одному диску - 300 мс .;
електроживлення виробу - 220 В, 50 Гц, габарити - 235х215х105 мм;
максимальна відведена теплова потужність - 8 Вт;
тривалість безперервної роботи в циклі "Заряд» / Стирання"- не менш 0,5 г.

Прилади для виявлення підключень до локальної мережі

Заходи протидії в комп'ютерних мережах – дуже специфічна задача, котра потребує навичов спостереження і роботи у фоновому режимі. У цьо-

му виді сервісу застосовуються кілька приладів: ручний осцилограф; кабельний сканер; рефлектометр часових інтервалів; аналізатор мережевого трафіка/протокольний аналізатор; комп'ютер зі спеціальным пакетом виявлення программного забезпечення; портативний спектральний аналізатор та ін. Можливості кабельного сканера, рефлектометра и аналізатора трафіка поєднує прилад FLUKE (рис.7.2).

Рис.7.2

Для аналізу фактів порушень функціонування локальної мережі, вторжень хакерів і реєстрації наявності замаскированих пристроїв спостереження використовується ЛАНметр. Цей прилад також використовується при проведенні мережевих аудитів і перевірок.

Під час проведення інспекцій осцилограф, що підключається для загальної оцінки стану мережі, зазвичай дозволяє спостерігати за формою сигналів та їх наявністю. У разі наявності в мережі пристроїв несанкціонованого спостереження з розподіленим спектром осцилограф забезпечить швидке визначення цього факту, а також індикацію напруги, наявності радіочастотного шуму і обмеженої інформації щодо перехідних зв'язків.

Портативний спектральний аналізатор використовується для оперативного перегляду радіочастотного спектру мережі. Спостереження повинно здійснюватися за будь-якими сигналами, що не відповідають типовому вигляду в тестованій мережі.

Коли все комбінації з'єднань мережі ретельно перевірені на присутність сторонніх сигналів (використовуючи осцилограф і спектральний аналізатор), для моніторингу будь-якої активності на кожному специфічному сегменті використовується мережевий аналізатор трафіку. Аналізатор зазвичай оцінює тільки заголовки пакетів і може надати користувачеві кілька базових мережевих функцій, таких як передача даних з однієї програми в іншу (PING), відстеження шляху (Trace Route), перегляд DNS і забезпечення списків знайдених або активних мережевих адрес. З цієї точки зору спеціаліст протидії отримає список всіх мережевих об'єктів, який потім може бути звірений з фізичним списком.

Система захисту інформації Secret Net

Система призначена для забезпечення інформаційної безпеки в ЛОМ, робочі станції і сервери якої працюють під управлінням операційних систем Windows всіх модифікацій і UNIX MP-RAS версії 3.02.00 (рис. 7.3, 7.4, 7.5).

Основними сферами застосування системи Secret Net є захист інформаційних ресурсів, централізоване управління інформаційної безпекою, контроль стану інформаційної безпеки.

Рис. 7.3.

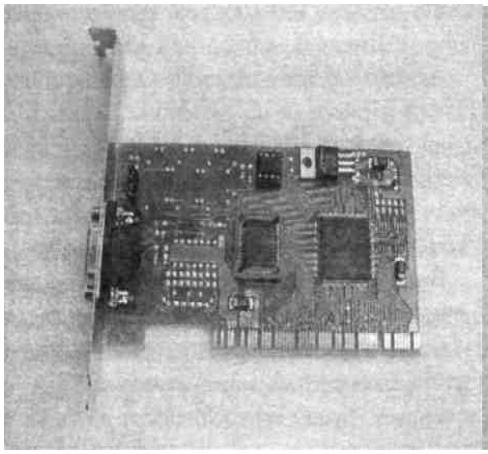


Рис. 7.4.

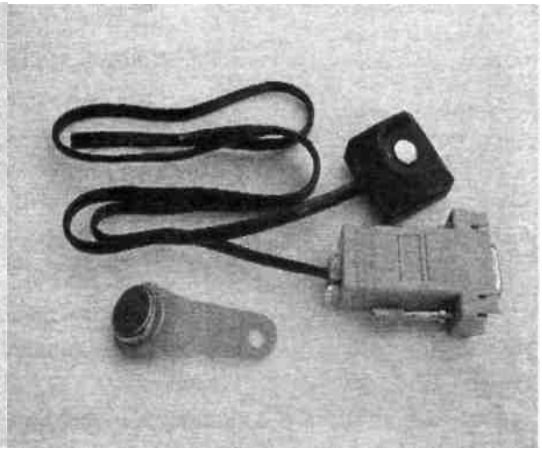


Рис. 7.5.

Адміністратору безпеки надається єдиний засіб управління всіма захисними механізмами, що дозволяє централізовано керувати і контролювати виконання вимог політики безпеки.

Вся інформація про події в інформаційній системі, що мають відношення до безпеки, реєструється в єдиному журналі реєстрації. Про

спроби скоєння користувачами неправомірних дій адміністратор безпеки дізнається негайно.

Система Secret Net складається з трьох компонентов: клієнтської частини, сервера безпеки і підсистеми управління.

Особливістю системи Secret Net є клієнт-серверна архітектура, при якій серверная частина забезпечує централізоване зберігання і обробку даних системи захисту, а клієнтська частина – захист ресурсів робочої станції або сервера і зберігання керуючої інформації у власній базі даних.

Клієнтська частина системи захисту (як автономний варіант, так і мережевий) встановлюється на комп'ютер, що містить важливу інформацію, будь то робоча станція в мережі або сервер (в тому числі і сервер безпеки). Клієнти Secret Net оснащуються засобами апаратної підтримки (для ідентифікації користувачів за електронними ідентифікаторами та управління завантаженням із зовнішніх носіїв).

Сервер безпеки встановлюється на виділений комп'ютер або контролер домену і забезпечує вирішення наступних завдань:

- ведення центральної бази даних (ЦБД) системи захисту, яка функціонує під управлінням СУБД Oracle 8.0 Personal Edition і містить інформацію, необхідну для роботи системи захисту;

- збір інформації про події, що відбуваються з усіма клієнтами Secret Net в єдиний журнал реєстрації та передача обробленої інформації підсистемі управління;

- взаємодія з підсистемою управління та передача керуючих команд адміністратору на клієнтську частину системи захисту.

Підсистема управління Secret Net встановлюється на робочому місці адміністратора безпеки.

Схема управління, реалізована в Secret Net, дозволяє управляти інформаційної безпекою в термінах реальної предметної області і в повній мірі забезпечити жорсткий розподіл повноважень адміністратора мережі і адміністратора безпеки.

Система захисту інформації Secret Net випускається в автономному та мережевому варіантах. *Автономний варіант* складається тільки з клієнтської частини і призначений для забезпечення захисту автономних комп'ютерів або робочих станцій і серверів мережі, що містять важливу інформацію. *Ме-*

режевий варіант складається з повного комплекту (клієнтської частини, підсистеми управління, сервера безпеки) і дозволяє реалізувати захист як усіх комп'ютерів мережі, так і тільки тих робочих станцій і серверів, які зберігають і обробляють важливу інформацію. Причому в мережевому варіанті, завдяки наявності сервера безпеки і підсистеми управління, буде забезпечено централізоване управління і контроль роботи всіх комп'ютерів, на яких встановлені клієнти Secret Net.

Сімейство засобів захисту інформації Secret Net можна застосовувати для захисту інформації, що містить державну таємницю.

Електронний замок «Соболь-PCI»

Призначений для захисту ресурсів комп'ютера від несанкціонованого доступу. Електронний замок "Соболь-PCI" може застосовуватися як пристрій, що забезпечує захист автономного комп'ютера, а також робочої станції або сервера, що входять до складу локальної обчислювальної мережі. При цьому використовуються наступні механізми захисту: ідентифікація і аутентифікація користувачів; реєстрація спроб доступу до ПЕОМ; заборона завантаження ОС зі знімних носіїв; контроль цілісності програмного середовища.

Можливості щодо ідентифікації і аутентифікації користувачів, а також реєстрація спроб доступу до ПЕОМ не залежать від типу використовуємої ОС. Дія полягає в перевірці персонального ідентифікатора і пароля користувача при спробі входу в систему. У разі спроби входу в систему незареєстрованого користувача електронний замок реєструє цю спробу і здійснює апаратне блокування до 4 пристроїв (наприклад: CD-RW, ZIP, LPT і USB-порти).

В електронному замку використовуються ідентифікатори Touch Memory фірми Dallas Semiconductor. Завантаження операційної системи з жорсткого диска здійснюється тільки після пред'явлення зареєстрованого ідентифікатора. Службова інформація про реєстрацію користувача (ім'я, номер присвоєного ідентифікатора і т.д.) зберігається в незалежній пам'яті електронного замка. Цей замок здійснює ведення системного журналу, записи якого зберігаються також в незалежній пам'яті. "Соболь" надає інформацію адміністратору безпеки про всі спроби доступу до ПЕОМ.

Електронний замок може застосовуватися в складі системи захисту інформації Secret Net для генерації ключів шифрування і електронно-

цифрового підпису. Крім того, при використанні “Соболя” в складі Secret Net забезпечується єдине централізоване управління його можливостями. За допомогою підсистеми управління Secret Net адміністратор безпеки може керувати статусом персональних ідентифікаторів співробітників (наприклад, присвоювати електронні ідентифікатори, тимчасово робити їх недійсними), що дозволяє управляти доступом співробітників до комп’ютерів автоматизованої системи організації.

У базовий комплект електронного замка “Соболь-PCI” (рис. 7.6, 7.7) входить : контролер “Соболь-PCI”; зчитувач; два ідентифікатора DS-1992; інтерфейс для блокування завантаження з FDD та CD; програмне забезпечення формування списків контрольованих програм; документація.

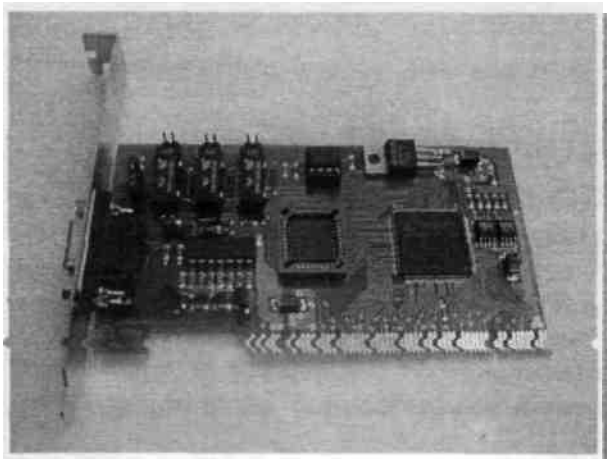


Рис. 7.6.

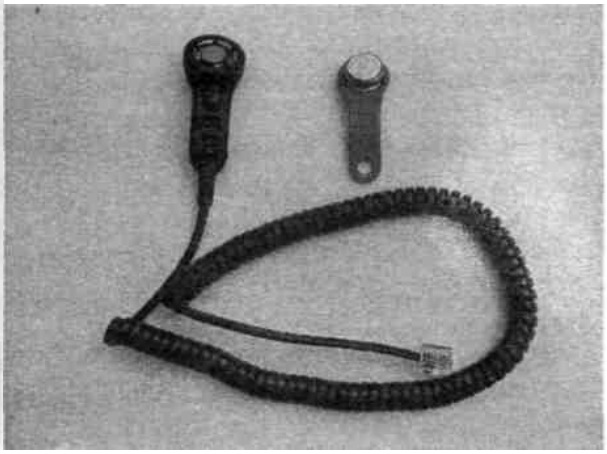


Рис. 7.7.

Система захисту корпоративної інформації Secret Disk Server

Призначена для захисту конфіденційної інформації, корпоративних баз даних. Система призначена для роботи в Windows NT 4.0 Server / Workstation, підтримує роботу з усіма дисками, в т.ч. RAID-масивами. Система не тільки надійно захищає конфіденційні дані, але й приховує їх наявність. Захист інформації здійснюється шляхом “прозорого” (на льоту) шифрування змісту розділів жорсткого диска.

При установці Secret Disk Server вибрані логічні диски зашіфровуються. Права доступу до них для користувачів мережі встановлюються засобами Windows NT. Шифрування здійснюється програмним драйвером ядра (kernel-mode driver).

Крім вбудованого алгоритму перетворення даних з довжиною ключа 128 біт, Secret Disk Server дозволяє підключати зовнішні модулі криптографічного захисту, наприклад емулятор плати “Криптон з довжиною ключа 256 біт (розробка РФ). Швидкість шифрування дуже висока, тому мало хто зможе помітити невелике уповільнення при роботі.

Ключі шифрування вводяться в драйвер Secret Disk Server перед початком роботи з захищеними розділами (або при завантаженні сервера). Для цього використовуються мікропроцесорні картки (смарткарти), захищені PIN-кодом. Не знаючи код, скористатися карткою можна, але три спроби введення неправильного коду заблокують карту. При роботі сервера смарткарта не потрібна, її можна заховати в надійне місце.

Генерація PIN-коду і ключів шифрування проводиться самим користувачем. При генерації використовується послідовність випадкових чисел, формуємої по траєкторії руху миші і тимчасовим характеристикам натискання довільних клавіш.

Secret Disk Server має відкритий інтерфейс для подачі сигналу "тривога" і дозволяє підключати різні датчики і пристрої контролю доступу в приміщення (датчики відкривання дверей, вікон, руху, кодові замки та ін.).

При підключенні захищених дисків можливий автоматичний запуск необхідних програм і сервісів, заявлених у файлі конфігурації.

Після перезавантаження сервера без пред’яви смарткарти або спроби читання дисків на іншому комп’ютері, захищені розділи будуть виглядати як неформатовані області, прочитати які не можна. При виникненні небезпеки можна миттєво знищити інформацію, зробивши захищені розділи “невидимими”. В поставку входить інсталяційний CD, універсальний пристрій для роботи зі смарт-картами (зовнішній), комплект кабелів, спеціальна плата Hardlock, документація, 3 смарткарти.

Система захисту конфіденційної інформації Secret Disk

Secret Disk - спрощена версія попередньої системи захисту конфіденційної інформації для широкого кола користувачів комп’ютерів: керівників, менеджерів, бухгалтерів, аудиторів, адвокатів та ін.

При установці системи в комп’ютері з'являється новий віртуальний логічний диск (один або кілька). Все, що на нього записується, автоматично

шифрується, а при читанні розшифровується. Зміст цього логічного диска знаходиться в спеціальному контейнері (зашифрованому файлі). Файл секретного диска може перебувати на жорсткому диску комп'ютера, на сервері, на змінних носіях типу ZIP, CD або магнітооптиці.

Secret Disk забезпечує захист даних навіть у разі вилучення такого диска або самого комп'ютера. Використання секретного диска рівносильно автоматичному запуску шифрування усіх додатків. Підключення секретного диска і робота із зашифрованими даними можливі тільки після апаратної аутентифікації користувача і введення правильного пароля. Для аутентіфікаціі використовується електронний ідентифікатор – смарткарта, електронний ключ або брелок.

Після підключення секретного диска він стає видимим операційній системі Windows як ще один жорсткий диск, а записані на ньому файли доступні будь-яким програмам. Не маючи електронного ідентифікатора і не знаючи пароля, підключити секретний диск не можна – для сторонніх він залишиться просто зашифрованим файлом з довільним ім'ям (наприклад, game.exe або girl.tif).

Як будь-який фізичний диск, захищений диск може бути наданий для спільного використання в локальній мережі. Після відключення диска всі записані на ньому файли і програми стануть недоступними.

Перелік основних характеристик системи наведений далі.

1. Захист конфіденційних даних за допомогою професійних алгоритмів шіфрування (можливість підключення зовнішніх криптографічних бібліотек).

2. Генерація ключів шифрування самим користувачем.

3. Апаратна аутентифікація користувача за допомогою електронних брелоків, смарт-карт або електронних ключів.

4. Подвійний захист. Кожен секретний диск захищений особистим електронним ідентіфікатором користувача і паролем доступу до цього диску.

5. Робота із зашифрованими архівами. Інформацію можна стиснути і зашифрувати як для себе (з використанням електронного ідентифікатора), так і для захищеного обміну з колегами (з паролем).

6. Блокування комп'ютера Secret Disk дозволяє гасити екран і блокувати клавіатуру при відключенні електронного ідентифікатора, при натисканні

заданої комбінації клавіш або тривалу неактивність користувача. При блокуванні системи секретні диски не відключаються, запущені додатки, що використовують захищене відео, продовжують нормально працювати, робота інших користувачів з доступом до секретного диска в мережі, не порушується.

7. Режим роботи під примусом. У критичній ситуації можна ввести спеціальний аварійний пароль. При цьому система на деякий час підключить диск, знищивши особистий ключ шифрування в електронному ідентифікаторі (що унеможливить доступ до диску в майбутньому), а потім зімітує одну з відомих помилок Windows.

8. Можливість відновлення даних при втраті (або навмисному псуванні) електронного ідентифікатора або втрати пароля.

9. Простий і зручний інтерфейс користувача.

10. Відмінності по алгоритмам шифрування (в залежності від потреб може використовуватися один з вбудованих алгоритмів): алгоритм кодування з довжиною ключа 128 біт; криптографічний алгоритм RC4 з довжиною ключа 40 біт та ін.

Версія з апаратном захистом, починаючи від початкового завантаження комп'ютера, поставляється за окремими угодами.

Програмно-апаратный комплекс засобів захисту "Акорд-АМДЗ"

Призначений для застосування на IBM-сумісних ПЕОМ (робочих станціях ЛОМ) з метою їх захисту від НД. Комплекс являє собою сукупність технічних і програмних засобів, що забезпечують виконання основних функцій захисту від НД на основі: персональних ідентифікаторів користувачів; парольного механізму; блокування завантаження ОС зі змінних носіїв інформації; контролю цілісності технічних засобів і програмних засобів (файлів загального, прикладного ПЗ і даних) ПЕОМ; забезпечення режиму довіреного завантаження в ПЕОМ операційних систем.

Програмна частина комплексу, включаючи засоби ідентифікації і аутентифікації, засоби контролю цілісності технічних і пропрограмних засобів ПЕОМ, засоби реєстрації дій користувача, а також засоби адміністрування і аудиту (роботи з реєстраційним журналом) розміщується в енергонезалежній пам'яті контролера при виготовленні комплексу. Доступ до засобів адміністрування та аудиту надається тільки адміністратору.

Ідентифікація та аутентифікація користувачів, контроль цілісності технічних і програмних засобів ПЕОМ виконуються контролером комплексу перед завантаженням ОС, встановленої в ПЕОМ. Комплекс забезпечує виконання основних функцій захисту від НД як в складі окремої ПЕОМ, так і на робочих станціях ЛОМ, в тому числі налаштування, контроль функціонування і управління комплексом.

Апаратно-програмный комплекс IP Safe-PRO

Призначений для побудови захищених віртуальних частин IP-мереж, що створюються на базі мереж загального користування (в тому числі й Інтернет). Виконаний основі на IBM PC-сумісного комп'ютера з двома Ethernet-інтерфейсами (базова конфігурація) з операційною системою FreeBSD (рис. 7.8). Додаткові можливості: маршрутизація і функції міжмережевого екрану; можливість підтримки різних інтерфейсів (наприклад, G.703, G. 704, V.35, RS-232 та ін.); система "гарячого" резервування.

Рис. 7.8

Апаратно-програмный комплекс "КОНТИНЕНТ-К"

Призначений для побудови віртуальної приватної мережі (VPN) на основі глобальних мереж загального користування, що використовують протокол обміну TCP/IP (рис. 7.9.). У якості складових частин VPN, побудованої на базі комплексу, можуть виступати корпоративні ЛОМ, їх сегменти і окремі ПК (в т. ч. домашні комп'ютери співробітників). .

Рис. 7.9

АПК "Континент-К" забезпечує: захист внутрішніх сегментів мережі від несанкціонованого доступу з боку мереж загального користування; статичну маршрутизацію IP-пакетів; фільтрацію IP-пакетів відповідно до заданих правил; криптографічний захист даних, що передаються по каналах зв'язку мереж загального користування між складовими частинами VPN; безпечний доступ користувачів VPN до ресурсів мереж загального користування; централізоване налаштування VPN-пристроїв; віддалений доступ до ресурсів VPN по виділених і комутованих каналах зв'язку.

Основним елементом комплексу є криптографічний шлюз, який являє собою спеціалізований апаратно-програмний пристрій, що функціонує на платформі Intel під керуванням спрощеної версії ОС FreeBSD. Криптографічний шлюз оснащується мережевими інтерфейсами стандарту Ethernet, а також платою ЕЗ "Соболь", що забезпечує локальну ідентифікацію та аутентифікацію адміністратора КШ і контроль цілісності програмного забезпечення.

У мережі "Континент-К" можливо встановити до 5000 криптошлюзів. Додавання нових і зміна налаштувань вже встановлених компонентів виробляються без втручання в процес функціонування системи. Технічні характеристики: довжина ключа шифрування – 256 біт; кількість мережевих інтерфейсів – до 16; пропускна здатність (шифрування, імітозахист) – до 80 Мбіт / с; пропускна здатність абонентського пункту - до 14 Мбіт / с; збільшення довжини IP-пакета - до 36 байт; підтримка режиму “гарячого” резервування.

Кейс для транспортування ноутбуків «ТІНЬ К1»

“ТІНЬ К1” призначений для транспортування ноутбуків або окремих накопичувачів на жорстких дисках, стримерних картриджів, ZIP дисків з можливістю негайного знищення інформації при спробі НСД (рис. 7.10).

Конструктивно комплекс монтується в пило-, волого-, вибухозахищеному кейсі, в якому ноутбук транспортується. Інформація, що підлягає захисту, розміщується на додатковому жорсткому диску, який знаходиться в кейсі окремо від ноутбука в спеціальному відсіку і з’єднаний з ним зовнішнім інтерфейсним кабелем. Екстрене знищення інформації проводиться:

Рис. 7.10

- автоматично при НД до кейса (або розкритті);
- автоматично при несанкціонованому розкритті відсіку, де знаходится жорсткий диск;
- автоматично, по закінченню 24 годин автономної роботи;
- дистанційно за командою користувача. Процес знищення не впливає на працездатність ноутбука і не залежить від того, чи працював він. Можливий варіант виготовлення комплекса для транспортування одночасно жорстких дисків, дискет, аудіо-, відео- і стримерних касет.

Комплекс може перебувати в двох режимах: режим очікування (РО) і режим охорони (Р1). У режимі РО відбувається тестування всіх основних вузлів, блоків і датчиків. Здійснюється вільний доступ до ноутбука або магнітних носіїв. У режимі Р1 автоматично відбувається знищення інформації при спробі несанкціонованого доступу або користувачем в будь-який момент часу по радіоканалу (дальність до 100 метрів). Постановка в режим охорони здійснюється за допомогою безконтактної електронної Proximity карти.

Комплекс Тінь має автономне джерело живлення, що забезпечує безперебійну роботу до 24 годин. Додаткові можливості: знищення інформації по команді користувача з будь-якого стільникового телефону по GSM каналу; повний захист корпусу, що виключає некоректне розтин і висвердлювання; повне протоколювання роботи в реальному часі, що фіксує в незалежній пам'яті останні кілька десятків подій з докладним описом.

Комплекс Тінь має автономне джерело живлення до 24 годин.

Додаткові можливості: знищення інформації по команді користувача з будь-якого стільникового телефону; захист корпусу, що виключає некоректний доступ; протоколювання роботи в реальному часі, що фіксує в незалежній пам’яті останні кілька десятків подій з докладним описом.

Апаратно-програмна система криптозахисту повідомлень “SX-1”

Апаратно-програмна система SX-1 призначена для криптографічного захисту даних, які передаються по каналам зв’язку між різними ПЕВМ, або для зберігання повідомлень в пам’яті окремой ПЕВМ (рис. 7.11).

Рис. 7.11

В системі SX-1 вперше у вітчизняній і зарубіжній криптографічній практиці реалізован “хаотичний” поточний шифр. Система забезпечує: криптографічне перетворення повідомлень, оформлених у вигляді файлів, та їх запис на будь-які диски; високу стійкість ключових даних до їх компрометації при будь-яких діях зловмисників і обслуговуючого апаратно-програмні засоби персоналу; гарантоване виконання заданих функцій не менш 2 років без зміни системного ключа.

Система SX-1 включає: плату з однокристальної ЕОМ, що встановлюється в слот ISA ПЕОМ IBM PC/AT (або розміщується в окремому контейнері розміром 140x110x35 мм) і підключається до ПЕОМ за допомогою роз'єму COM; спеціальне програмне забезпечення, яке встановлюється в ПЕОМ з ОС Windows.

Перелічимо основні характеристики системи: ймовірність вгадати системний ключ з k-ої спроби не більше $k \cdot 2^{-240}$; швидкість криптографічного перетворення – не менше 190 кбіт / с; використання для шифрування даних криптостійких алгоритмів шифрування з довжиною ключа від 128 біт; можливість підключення сертифікованого криптографічного модуля або плати "Криптон" виробництва фірми "Анкад"; формування унікальних ключів шифрування на основі послідовності випадкових чисел.

Міжмережевий екран і шифратор IP-протоколів

Призначений для міжмережевого екранування і криптографічного захисту даних при створенні віртуальних приватних мереж (Virtual Private Network) в мережах загального доступу (рис. 7.12).

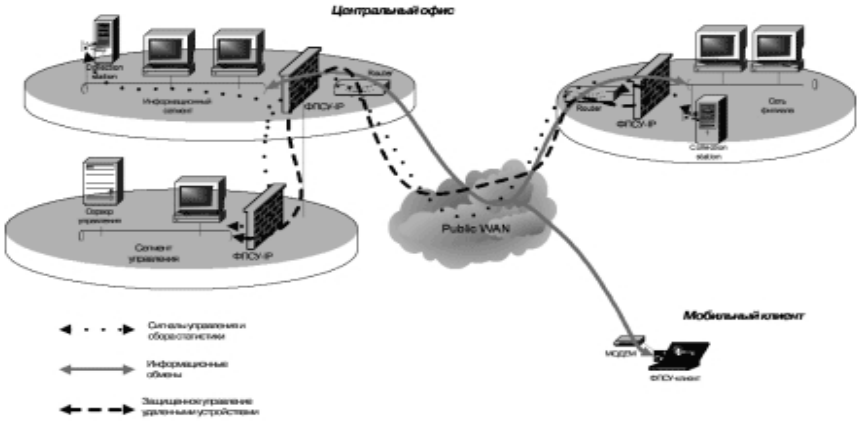


Рис. 7.12. Типова схема застосування комплексу

За рахунок стиснення інформації комплекс забезпечує помітне підвищення швидкості передачі даних, має можливість одночасної підтримки до 1024 криптографічно захищених з'єднань при швидкості шифрування сумарного IP-потоку "на проході" до 90 Мбіт/с. У комплексі використовуються тільки власні реалізації всіх протокольних стеків TCP / IP, алгоритмів авто-

матизованого управління комплексами і закладеними в них засобами криптографічного захисту.

Перелічимо основні характеристики пристрою.

1. Продуктивність – комплекс забезпечує швидкість передачі IP-потоків від 65 Мбіт/с і вище при включенні всіх режимів захисту (фільтрація + стиск + шифрування).

2. Ключова система – симетрична.

3. ОС/стек протоколів – 32 розрядна DOS-подібна система власної розробки.

4. Оброблювані рівні протоколу обміну – мережевий + транспортний, сеансовий і прикладний (вибірково).

5. Тип і кількість інтерфейсів – 2; 10 / 100Ethernet, FDDI.

6. VPN-протокол / надмірність / стиснення даних – власний / не більше 22 байт на пакет / за рахунок прохідного стиснення даних досягається ефект прискорення інформаційних взаємодій.

7. Ефективне протистояння активним і пасивним інформаційним впливам розвідувального характеру.

8. Можливість каскадного включення комплексів – забезпечує виділення окремих сегментів мереж в ізольовані зони підвищеної захищеності.

Контрольні запитання

1. Дайте визначення поняттям “засоби захисту інформації” і “технічні засоби захисту”. Назвіть переваги і недоліки технічних ЗЗІ.
2. Які елементи відноситься до програмних та організаційних ЗЗІ? Назвіть їх переваги і недоліки.
3. Назвіть та поясніть принципи інженерно-технічного захисту інформаціїї.
4. Назвіть та поясніть методи захисту технічними засобами?
5. Що таке інформаційне приховування (ІП)? Які способи ІП ви знаєте?
6. Яких результатів дозволяє досягти інформаційне приховування?
7. Поясніть суть 4-ох груп каналів витоку інформації?
8. Назвіть найбільш ефективні технічні засоби ІБ в комп’ютерних мережах?

8. ЗАГАЛЬНА ХАРАКТЕРИСТИКА КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЇ

8.1. Загальні відомості. Задачі КЗІ

Комплексний захист інформації (КЗІ) – сукупність людей, процедур і обладнання, захищаючих інформацію від несанкціонованого доступу, модифікації або відмови доступу.

Розглянемо задачі КЗІ.

1. Регламентація дій користувача з метою захисту інформації.
2. Навчання і встановлення юридичної відповідальності за виконання правил інформаційної безпеки (ІБ).
3. Явний і прихований контроль за порядком інформаційного обміну.
4. Блокування всіх можливих каналів витоку.
5. Виявлення закладних пристроїв в технічних засобах (ТЗ) і програмному забезпеченні (ПЗ).
6. Виявлення зондувань, нав’язувань і випромінювань.
7. Забезпечення санкціонованого доступу в фізичний та інформаційний простір.
8. Виявлення вторгнень в фізичний та інформаційний простір.
9. Виявлення загорянь, затоплень і інших надзвичайних ситуацій (НС).
10. Забезпечення резервування важливої інформації.
11. Організація обороту фізичних носіїв інформації, що захищаються.
12. Забезпечення достовірності електронного документообігу.
13. Шифрування інформації на будь-яких етапах обробки.
14. Відновлення ключових структур при компрометації.
15. Генерація, розподіл і зберігання ключів і паролів.
16. Реєстрація подій і виявлення порушень.
17. Розслідування у взаємодії з правоохоронними органами порушень політики безпеки.
18. Безперервний контроль і управління криптографічного захисту.

8.2. Стратегії комплексного захисту інформації

Усвідомлення необхідності стратегічного підходу в організації безпечного інформаційного середовища формується у керівників в міру усвідомлення важливості, багатоаспектності та проблеми захисту інформації.

Стратегія – загальна спрямованість діяльності організації з урахуванням її об'єктивних потреб, можливих умов здійснення і можливостей. Розрізняють три види стратегій: оборонна, наступальна і випереджуюча стратегії. Основні характеристики стратегій КЗІ наведені в табл. 8.1.

Таблиця 8.1

Основні характеристики стратегій комплексного захисту інформації

Назва характеристики	**Стратегії комплексного захисту інформації**		
	оборони	**наступу**	**упередження**
Можливий рівень захисту	Достатньо високий, але тільки стосовно відомих загроз	Дуже високий, але тільки в межах існуючих уявлень стосовно природи загроз і можливостей їх проявлень	Рівень захисту гарантовано дуже високий
Необхідні умови реалізації	Наявність методів і засобів реалізації	1. Наявність переліку і характеристик повної множини потенціальних загроз. 2. Наявність розвинутого арсенала методів і засобів захисту. 3. Наявність можливостей впливати на архітектуру ІС і технологію обробки інформації	Наявність захисту інформаційних технологій
Ресурсоемність	Незначна порівняно з іншими стратегіями	Значна (з ростом вимог із захисту зростає по експоненті)	1. Висока по капітальним витратам. 2. Незначна в кожному конкретному випадку при наявності уніфіковано захищеної інформаційної технології
Рекомендації щодо застосування	Невисокий ступінь секретності інформації і не дуже великі очікувані втрати	Достатньо високий ступінь секретності інформації і можливість значних втрат при порушенні захисту	Перспективна

Оборонна стратегія захисту – захист від вже відомих загроз, що здійснюється автономно, без впливу на існуючу інформаційну систему.

Наступальна стратегія захисту – захист від усієї множини потенційних загроз. Архітектура інформаційної системи і технологія її функціонування зобов'язані враховувати потреби захисту.

Упереджувальна стратегія захисту – створення спочатку такого інформаційного середовища, в якому загрози не мали б умов для виникнення.

8.3. Етапи побудови КЗІ для різних стратегій

Основні етапи побудови стратегій КЗІ надані в табл. 8.2. Основні принципи побудови КЗІ надані далі.

Таблиця 8.2

Основні етапи побудови стратегій КЗІ

Назви етапів побудови	**Стратегії комплексного захисту інформації**		
	оборонна	*наступальна*	*упереджувальна*
Формування середовища захисту	Відсутнє	1. Структурована архітектура ІС. 2. Структурована технологія обработки інформації, що захищається. 3. Чітка організація робіт із захисту	Захищена інформаційна технологія в уніфікованому виготовленні
Аналіз засобів захисту	1. Подання організаційної структури ІС у вигляді графа, вузли якого – типові структурні компоненти, а дуги – взаємозв'язки між компонентами. 2. Подання технології обробоки захищаємої інформації у вигляді строго визначеної схеми. 3. Визначення параметрів захищаємої інформації та умов її обробки		Відсутній
Оцінювання вразливості інформації	1. Визначення рівня ймовірності порушення захисту інформації в умовах її обробки. 2. Оцінювання розмірів можливого збитку при порушенні захисту		Відсутнє
Визначення вимог до захисту	Визначення ймовірності порушення захисту інформації, котра має бути забезпечена при обробці, інформації, яка захищається		
Побудова системи комплексного захисту	Визначення технічних засобів, які мають бути використані при обробці ЗІ	Вибір типового варіанту (профіля) або проектування індивідуальної системи КЗІ	Визначення механізмів захисту, які мають бути задіяні при створенні КЗІ
Вимоги до середовища захисту	Відсутні	Визначається в залежності від вимог до захисту інформації	Реалізується на базі уніфікованої ІТ, яка захищається

Простота механізму захисту. Механізм має бути інтуїтивно зрозумілий і простий у використанні. Застосування механізму захисту не повинно вима-

гати знання мов і бути трудомістким.

Сталість захисту. Механізм захисту повинен бути постійно захищений від несанкціонованих змін. Жодна корпоративна ІС не є безпечною, якщо механізм захисту може стати об'єктом модифікації і зміни.

Повнота контролю. Перевірка повноважень будь-якого звернення до будь-якого об'єкта – це основа комплексного захисту інформації. Структурно КЗІ повинна охоплювати всі рівні контролю: інформацію, документи, режими роботи об'єкта захисту, програмне забезпечення, апаратуру, інженерно-технічні споруди, персонал.

Відкритість проектування. КЗІ повинна ефективно функціонувати і підтримуватися незалежно від досвіду противника. При цьому знання алгоритму захисту не повинно сприяти подоланню захисту навіть автору.

Ідентифікація. Кожен об'єкт ІС повинен бути однозначно ідентіфіцірован. Користувач → повноваження, файл → рівень доступу.

Поділ повноважень. Застосуванням декількох ключів захисту, що дозволяє вирішити доступ тільки при виконанні ряду умов.

Надійність. Повинен бути механізм постійної оцінки надійності (справності) функціонування КЗІ.

Максимальна відособленість захисту. Захист повинний бути відділений від функцій управління даними та ІС.

Безперервність. КЗІ – це не разовий захід і не сукупність заходів щодо захисту, це неперервний цілеспрямований процес.

Неминучість покарання порушень. Найпростіший і найдієвіший спосіб покарання порушень – відмова в доступі.

Економічність. Розумне поєднання ціни та якості захисту інформації в умовах експлуатації.

8.4. Безпека цінних інформаційних ресурсів

Безпека цінних інформаційних ресурсів завжди виступає необхідною умовою успіху в справі, отримання прибутку, збереження цілісності підприємства та підтримки його ефективного функціонування.

Метою ІБ є безпека інформаційних ресурсів в будь-який момент часу в будь-якій обстановці, а також гарантована в конкретній ситуації захищеність інформації в часі і просторі від будь-яких об'єктивних і суб'єктивних загроз.

Спочатку завжди необхідно вирішити наступні питання: навіщо і що захищати? від кого захищати? як захищати?

Проблеми ІБ з часом стають більш складними і значними, оскільки зростає перехід до безпаперових технологій в управлінні, документообіг стає все більш електронним. Якщо раніше головними небезпеками були втрата конфіденційного документа, розголошення конфіденційних відомостей або витік технічними каналами, то в даний час все частіше доводиться стикатися з незаконним таємним оперуванням електронними документами без крадіжки з БД і незаконним використанням інформаційних ресурсів.

Поточні і перспективні завдання забезпечення ІБ та ЗІ формуються в рамках програми інформаційної безпеки підприємства. Основа рішення – принцип персональної відповідальності керівництва всіх рівнів, служби безпеки та співробітників за використання інформації відповідно до законодавства та функціональних обов'язків.

Завдання захисту реалізуються системою захисту інформації. Головна небезпека – це несанкціонований доступ (несанкціоноване ознайомлення). Крадіжка, копіювання, розголошення, знищення, фальсифікація, спотворення, модифікація і підміна інформаційних ресурсів є наслідками головної небезпеки.

Архітектура систем захисту інформації (СЗІ) зобов'язана охоплювати: електронні інформаційні системи; весь комплекс управління підприємством в єдності його функціональних і структурних систем; традиційні документаційні процеси.

Як вже було сказано в попередніх розділах конспекту лекцій комплексность СЗІ забезпечується включенням таких обов'язкових елементів, як: правові; організаційні; інженерно-технічні; програмно-апаратні; криптографічні.

8.5. Критерії цінності інформації

Документовані інформаційні ресурси – це інтелектуальна власність. Інтелектуальна власність складається з елементів – інформаційних продуктів (комерційно цінних ідей), реалізованих в інформаційному вигляді. Інформаційний продукт (ІП) є результатом творчої праці підприємця (колективу підприємства), що має конкретну цінність для власника.

Цінність ІП можна визначити через: вартість (розмір прибутку при використанні, розмір збитків при втраті; правове значення для фірми (установчі документи, програми та плани, договори з партнерами); перспективно наукове значення; техніко-технологічне значення.

Існують наступні види цінної інформації.

1. *Технічна та технологічна*: хімічна формула; рецепт; результат випробувань; дані контролю якості; методи виготовлення продукції; програмне забезпечення; виробничі показники.

2. *Ділова*: управлінські рішення; методи реалізації функцій; вартісні показники; результати дослідження ринку; списки клієнтів; економічні прогнози і т.д.

Основні напрямки формування цінної інформації (ЦІ) представлені в табл. 9.1.

Таблиця 9.1

Основні напрямки формування цінної інформації

№	Область діяльності	Напрямки формування цінної інформації
1.	Управління підприємством	застосування нетрадиційних методів управління, порядок підготовки та прийняття рішення в областях діяльності
2.	Прогнозування і плануванння	розширення або згорнення виробництва, очікуваний обсяг досліджень, програми розвитку, програми взаємодії з інофірмами, плани інвестицій, продаж, покупки
3.	Фінансова діяльність	баланс, відомості про стан банківських рахунків, відомості про рівень прибутковості продукції, інформація про отримання кредитів, про колообіг фінансів, про виробничі операції, про боргові зобов'язання
4.	Виробнича діяльність	виробничі потужності, тип обладнання, запаси сировини, матеріалів, комплектуючих, запаси готової продукції
5.	Торговельна діяльність	інформація про ринкові стратегії, методи здійснення продажу, інформація про результати дослідження ринку, інформация про ефективність комерційної діяльності.
6.	Переговори і наради за напрямками діяльності	інформація щодо підготовки, змісту і результатів переговорів з посередниками і партнерами, про наради з персоналом

№	Область діяльності	Напрямки формування цінної інформації
7.	Формування цінової політики	структура ціни, очікувані ціни, методи оцінювання, розміри знижок
8.	Формування складу клієнтів, компаньйонів, посередників, постачальників	відомості про зарубіжних і внутрішніх замовників, постачальників і користувачів
9.	Вивчення напрямків інтересів конкурентів	методи аналітичної роботи, способи боротьби за ринок, результати маркетинговых досліджень
10.	Участь в торгах і аукціонах	стратегічна інформація, інформація про підготовку до торгів і результати торгівлі
11.	Наукова і дослідницька діяльність по створенню нової техніки	відомості щодо програм перспективних досліджень і результатах
12.	Використання нових технологій	інформація про їх зміст, специфіку застосування і отриманий ефект
13.	Управління персоналом	персональні відомості про співробітників, методи ки добіра, тестування кандидатів на посаду, результати поточної роботи з персоналом
14	Організація безпеки підприємства	відомості щодо функціонування служби безпеки, змісту СЗІ, системи фізичного захисту

До особливо цінної інформації прийнято відносити: відомості про виробництво і про продукцію; відомості про ринок і наукові розробки; матеріально-технічне забезпечення; умови контрактів і переговорів; відомості про персонал; відомості про систему безпеки; динаміка збуту продукції; ефективність послуг.

Для України характерно віднесення до особливо цінної інформації відомостей про фінансову діяльність та систему безпеки підприємств. Завжди цінною інформацією є "чужа" інформація, тобто інформація від підприємств, установ, організацій, партнерів і клієнтів, які співпрацюють з об'єктом захисту.

8.6. Вияв і документування конфіденційних відомостей

Процес виявлення і регламентації реального складу конфіденціальної інформації – базова частина системи КЗІ. Комплексний захист – дорога технологія, тому визначення складу конфіденціальних відомостей має базуватися на економічній доцільності. Існують два критерія аналізу

інформаційних ресурсів: ступінь зацікавленості конкурентів; ступінь цінності інформації у вартісному і правовому аспектах.

Інформація про реальних і потенційних конкурентів є основою визначення інформації, яку необхідно захищати.

У процесі аналізу виділяють головні елементи, що відображають фірмовий секрет, який дозволяє здешевити систему комплексного захисту інформації, зробити її максимально цілеспрямованої, динамічною та ефективною. Захист за всі нововведення, включаючи загальновідомі складові, як правило, бажаного результату, не дає. Система захисту стає громіздкою, зростає складність контролю великого обсягу конфіденційної інформації. Масовість засекречування веде лише до зростання штатної чисельності служби безпеки і в кінцевому підсумку до зниження ефективності захисту і втрати інформації.

Найбільша безпека конфіденційної інформації забезпечується при відсутності її фіксації на будь-якому носії.

Загрози конфіденційних документів виникають в момент появи думки про необхідність документування. *Існують наступні загрози конфіденційних документів:*

- документування на випадковому носії поза сферою контролю системи безпеки;

- підготовка до видання документа, який не обгрунтований діловою необхідністю;

- включення в документ надлишкової інформації (рівнозначно розголошенню);

- випадкове (умисне) заниження грифу конфіденційності;

- виготовлення документа в умовах, які не гарантують збереження носія, конфіденційність оброблюваної інформації;

- втрата оригіналу, чернетки, варіанти або редакції документа, його частини, додатки;

- замовчування такого факту або спроба підміни втраченого матеріалу;

- повідомлення змісту проекту документа сторонній особі;

- несанкціоноване копіювання, у т. ч. на неврахованому носії;

- витік інформації по технічним каналам;

- *помилкові дії користувачів, особливо в частині дозволеної системи доступу*.

8.7. Носії конфіденційних відомостей

Носій ще до прийому конфіденційної інформації повинен бути врахований із закріпленням рівня конфіденційності. Безпека інформації, контроль її збереження забезпечується не тільки в оригіналі, а й в усіх чернетках, варіантах, редакціях, записах.

Всі носії конфіденційних відомостей умовно можна класифікувати на такі види: носії традиційні текстові, носії креслярсько-графічні, машинозчитувані документи, аудіо та відео документи і фотодокументи.

До традиційних текстових носіїв відносяться: блокнот з відривнимі листами і корінцем для ведення обліку листів, цілей їх використування, виконавців і дат; робочий зошит для документів великого обсягу; окремі пронумеровані листи; друкарські форми і бланки.

Носії креслярсько-графічні представляють собою пронумеровані листи кальки, ватману, координатної паперу.

Машинозчитувані документи – це марковані і пронумеровані диски, дискети, магнітні стрічки, карти та інші носії, які візуально не читаються.

Аудіо та відео документи являють собою марковані і пронумеровані лазерні диски, касети, магнітні стрічки, карти, кіноплівки.

Фотодокументи – марковані і пронумеровані касети з фотоплівкою, слайди, фотопапір.

Конфіденційний документ – це необхідним чином оформлений носій документованої інформації, що містить відомості обмеженого доступу або використання, які становлять інтелектуальну власність юридичної (фізичної) особи.

Конфіденційність є відображенням обмеження на доступ, яке накладає власник інформації. Називати конфіденційні документи секретними або ставити на них гриф секретності не допускається.

До складу конфіденційних документів в державних структурах входять документи, проекти документів і супутні матеріали для службового користування. Вони містять відомості, віднесені до службової таємниці, мають робочий характер і не підлягають опублікуванню у відкритій пресі.

До складу конфіденційних документів в підприємницьких структурах входять документи, що містять відомості, які власник має право віднести до комерційної таємниці, до таємниці фірми або майстерності.

Незалежно від приналежності до складу конфіденційних входять документи, що фіксують будь-які персональні дані, а також технічні та технологічні нововведення до їх патентування.

При розгляді термінів конфіденційності необхідно пам'ятати, що цінність інформації, як правило, не довговічна. Потрібно оцінювати час, необхідний конкуренту для вироблення такої ж ідеї, для викрадення ідеї, для відтворення ідеї і для її опублікування, тобто її переходу в загальнодоступну. Важливим моментом є те, що захист цінної інформації коштує дорого. Це пов'язано з постійною небезпекою втратити її в результаті дії конкурентів.

За термінами обмеження вільного доступу конфіденційність має значний розкид від декількох годин до декількох років. Основна маса конфіденційних документів відразу ж після роботи і виконання втрачає свою цінність і конфіденційність. Наприклад, листування до укладення контракту конфіденційна, а після підписання і дозволу першого керівника гриф конфіденційності знімається.

Контрольні запитання

1. Що таке комплексний захист інформації? Назвіть основні задачі КЗІ.
2. Назвіть та поясніть суть характеристик основних стратегій КЗІ.
3. Поясніть суть етапів побудови КЗІ для різних стратегій.
4. Розкажіть про принципи побудови КЗІ.
5. Як формується безпека цінних інформаційних ресурсів?
6. Коли виникають загрози конфіденційних документів? Назвіть ці загрози.
7. Як здійснюється захист носіїв з конфіденційними відомостями?
8. Чому не можна називати конфіденційні документи секретними?

9. РЕЖИМНИЙ ХАРАКТЕР РОБОТИ ОРГАНІЗАЦІЇ ЯК ОСНОВА КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЇ

9.1. Розробка Політики безпеки

Автоматизація процесів діяльності (бізнес-процесів) практично будь-якого сучасного підприємства сприяє росту продуктивності праці та поліпшенню управління за рахунок функціонування корпоративної інформаційної системы (КІС). З іншої сторони, одночасно з цим збільшується рівень інформаційних ризиків.

Аналіз світового та вітчизняного досвіду щодо ІБ диктує необхідність створення системи забезпечення безпеки інформації (СЗБІ) – взаємопов'язані різноманітні організаційні та технічні заходи захисту, що використовують сучасні методи прогнозування, аналізу і моделювання.

Створення повномасштабної СЗБІ вимагає значних фінансових витрат. Покрити необхідні витрати відразу, як правило, не представляється можливим. Це призводить до необхідності поетапної побудови системи (розгортання її окремих елементів з затримкою в часі). Очевидно, що для цілісного об'єднання цих елементів, що розробляються або закуповуються в різний час, необхідний єдиний архітектурний задум СЗБІ. Іншими словами, організація повинна сформувати свою Політику безпеки інформації.

Політика безпеки інформації – це сукупність нормативних документів, які встановлюють порядок забезпечення безпеки інформації на конкретному підприємстві, а також висуваючих вимоги з підтримки цього порядку. Важливо підкреслити, що документи, які розробляються при формуванні Політики безпеки, повинні мати офіційний юридичний статус (підпис першої особи).

Розробка Політики безпеки інформації є основоположним етапом при розробці та подальшому впровадженні СЗБІ. Якщо вимоги, висунуті на початку розробки не повні або помилкові, то, СЗБІ в ряді випадків не зможе повністю відповідати своєму призначенню.

Очевидно, що розробити Політику безпеки інформації, тобто побудувати повну систему правил і вимог з безпеки інформації, можливо тільки в тому випадку, якщо проаналізовані всі інформаційні ризики і визначена нормативна база, що регулює питання захисту інформації. Тому попереднім етапом

для розробки Політики безпеки повинно бути Комплексне обстеження захищеності КІС організації.

Як говорилося вище, під Політикою безпеки інформації розуміється узгоджений по цілям захисту інформації пакет нормативно, організаційно-розпорядчих та експлуатаційних документів, що регламентують всі питання організації, управління і контролю безпеки, а також експлуатації засобів захисту. Структура даного пакета документів подається у вигляді трьох ієрархічних рівнів.

Перший рівень Політики безпеки інформації містить головний документ "Концепція інформаційної безпеки", яка визначає цілі і завдання захисту інформації в КІС, корпоративні вимоги і практичні правила управління інформаційною безпекою, склад інших документів, що регламентують питання безпеки інформації. За своєю суттю це стратегія вирішення питань захисту інформації.

Даний документ є системоутворюючим, який інтегрує всі документи Політики безпеки за поставленими цілями і завданнями інформаційної безпеки.

Другий рівень, як правило, містить два документа: "Регламент забезпечення безпеки інформації" та "Профіль захисту", які є нормативними або організаційно-розпорядчими документами.

"Регламент забезпечення безпеки інформації" розробляється на підставі "Концепції безпеки інформації" і в директивної формі викладає порядок поводження із захищаємою інформацією, основні правила дій співробітників і їх відповідальність у забезпеченні безпеки інформації в будь-яких ситуаціях і на всіх стадіях життєвого циклу КІС підприємства.

"Профіль захисту" містить технічні вимоги до програмно-апаратних засобів захисту, в тому числі і вбудованим в загальносистемне програмне забезпечення на основі відповідних державних і галузевих стандартів.

Після розробки документів першого і другого рівнів проводиться наступний етап робіт – *третій рівень* – розробка виконавчої документації, що включає в себе різні посадові положення та інструкції, доцільність яких визначається за результатами першого та другого етапів. Крім того, даний рівень містить експлуатаційні документи засобів захисту інформації. Третій рівень політики безпеки спирається на експлуатаційну документацію вико-

ристовуваних програмно-технічних засобів захисту, загальносистемного та прикладного програмного забезпечення, а також на стратегію і тактику захисту, що забезпечується технічними і програмними засобами СЗБІ і КІС.

9.2. Система фізичного захисту – типові задачі та способ її реалізації. Основні характеристики системи фізичного захисту

Система фізичного захисту (СФЗ) – сукупність людей, процедур і обладнання, які захищають майно (об'єкти) від розкрадання, диверсій та інших неправомірних дій. Кінцева мета СФЗ – запобігання успішного виконання кваліфікованим порушником відкритих або таємних зловмисних акцій.

Типові завдання СФЗ: запобігання диверсій, спрямованих на виведення з ладу обладнання; запобігання розкрадань матеріальних засобів, майна або інформації; захист співробітників об'єкта. Основними характеристики СФЗ є: надійність (ешелонування, рівні захисту); мінімізація наслідків відмов; збалансованість. *Існує два способи організації ефективної СФЗ: стримування; виявлення, затримка і реагування*.

Стримування

Стримування – реалізація заходів, які сприймаються потенційним порушником як важкоподолане, страхітливе і перетворюють об'єкт в непривабливу мету. Результат стримування – порушник припиняє напад, або взагалі його не робить.

Приклад: охорона з відповідною формою; достатнє освітлення; попереджувальні знаки; грати на вікнах; бетонний паркан, колючий дріт; наявність сигналізації та систем відеоспостереження; опечатування.

Стримування безсиле, якщо порушник вирішується на напад, незважаючи на перешкоди. Покладатися на стримування як безальтернативний захист вкрай ризиковано. До того ж якість захисту способом стримування важко виміряти і оцінити. Навіть якщо не було нападів, це не означає, що система фізичного захисту способом стримування ефективна.

Виявлення

Виявлення – візуальна реєстрація прихованої або відкритої акції порушника щодо проникнення в простір об'єкта. У виявленні особливо

виділяються точки санкціонованого доступу, тобто виявлення при контролі входу і виходу осіб, яким не дозволено проносити матеріальні цінності та інформацію.

Показниками ефективності контролю на вході є: пропускна здатність; кількість персоналу, яка в одиницю часу має право проходу; частота помилкових проходів – частота, з якою дозволяється прохід за підробленими документами або невірно впізнаним; частота помилкових відмов - частота відмов у доступі особам, яким прохід дозволений.

Виявлення закінчується тільки за умови проведення оцінки вторгнення. *Цілями оцінки є відповіді на питання Що? Хто? Де? Яка кількість?*

Затримка

Затримка – уповільнення просування порушника до мети. Шляхами (способами) затримки є: фізичні бар'єри, перешкоди; замки; персонал охорони (в режимі постійної готовності, або в режимі очікування).

Показник ефективності затримки – загальний час подолання кожного елемента затримки після виявлення.

Затримка до виявлення при визначенні ефективності не враховується. Це є також стримуванням. Причина полягає, в тому, що час втрачено для реакції на дії порушника.

Реагування

Реагування – дія сил захисту щодо перешкод успіху порушника, переривання його дій. Для успішного переривання необхідна кількісна перевага охорони в очікуваній точці зупинки порушника, час на повне розгортання і точна інформація про порушника.

Завдання Виявлення та Затримки вирішуються, як правило, інженерно-технічними засобами та (або) силами охорони. В даний час ведуться відповідні розробки щодо створення засобів автоматичного Реагування.

9.3. Кількісний та якісний аналіз СФЗ

Метою аналізу є встановлення ефективності такого захисту.

Кількісний аналіз СФЗ застосовується у випадках, коли втрата неприпустима навіть при малій ймовірності нападу: АЕС, військові об'єкти, в'язниці, музеї, об'єкти енергетики, зв'язку.

Якісний аналіз СФЗ застосовується для об'єктів, що вимагають низького рівня захисту.

Аналіз виконується для: визначення стану СФЗ; підготовки до модернізації із застосуванням нових розробок; пристосування СФЗ до нових виробничих процесів, до появи нових цінних об'єктів; підвищення рівня захисту при зростанні загроз.

Нижче представлені деякі складові аналізу СФЗ на підприємствах і організаціях з внутрішньовідомчою охороною.

Шлях порушника

Шлях порушника – упорядкована послідовність дій проти об'єкта нападу, яка завершується диверсією, розкраданням або терористичним актом.

Приклади дій і шляхи порушника наведені відповідно в табл. 9.1 і на рис 9.1.

Таблиця 9.1

Приклад дій порушника

Шлях	***Елемент затримки***	***Елемент виявлення***
Подолати паркан або стіну	*Матеріал паркану або міцність стіни*	*Датчик на паркані, шум при проломі*
Пройти двері	*Міцність дверей*	*Датчик на двері*
Скопіювати файл	*Час копіювання*	*Вхід в КІС*

Рис. 9.1. Можливі шляхи порушника

Загальні обов’язки робітника охорони об’єкта з низьким рівнем захисту

Працівник охорони в будь-яких умовах повинен бути ввічливим і тактичним з громадянами, звертатися до них на “Ви”, свої вимоги і зауваження викладати в переконливій і зрозумілій формі, не допускати суперечок і дій, що ображають їх честь і гідність.

При звертанні до громадянина працівник охорони повинен назвати свою посаду і прізвище, після чого коротко повідомити причину і мету звернення. У разі звернення громадян працівник охорони, виконавши ті ж вимоги, зобов'язаний уважно вислухати і роз'яснити, куди слід звернутися для вирішення поставленого питання.

У розмові з громадянами працівники охорони зобов'язані виявляти спокій і витримку, не повинні вступати в суперечки, втрачати самовладання, відповідати грубістю на грубість і в своїх діях керуватися особистими неприязними почуттями.

Якщо порушник на зроблені йому зауваження реагує збудливо, потрібно дати йому час заспокоїтися, після чого роз'яснити неправильність його поведінки з посиланням на відповідні закони або інші правові акти. Після цього прийняти рішення про виклик начальника охорони або його помічника.

Зауваження порушникам, які мають при собі дітей, слід, по можливості, робити так, щоб діти цього не чули.

З підлітками працівник охорони повинен поводитися так само ввічливо, як і з дорослими. Зауваження дітям робляться з урахуванням їх віку та рівня розвитку.

З документами громадян при перевірці необхідно поводитися акуратно, не робити в них будь-які позначки. Якщо в документ вкладені гроші та інші цінні папери, необхідно запропонувати власнику самому взяти їх.

На місці вчинення правопорушення постової зобов'язаний:

- вжити заходів до припинення правопорушення;

- по можливості організувати затримання правопорушника;

- надати допомогу потерпілим, при необхідності викликати швидку допомогу;

- по можливості встановити свідків (очевидців);

- доповісти про те, що сталося, начальнику охорони і діяти відповідно до його вказівок.

Переслідування правопорушників ведеться тільки на території об'єкту, що охороняється.

Пропускний режим

У випадку пропускного режиму порядок забезпечується сукупністю заходів і правил, що виключають можливість безконтрольного входу-виходу осіб, в'їзду-виїзду транспортних засобів, вносу-виносу і ввезенню-вивезенню майна на об'єкти і з об'єктів, які охороняються.

Пропускний режим повинен передбачати такі основні заходи:

- встановлення та обладнання певних місць (КПП) для проходу (проїзду) на територію об'єкта;

- порядок допуску на об'єкти робочих змін, входу і виходу персоналу і відвідувачів;

- контроль за ввезенням (вивезенням), вносом (виносом) за межі охороняємого об'єкта матеріальних цінностей і т.д.;

Робочим органом по здійсненню пропускного режиму на об'єктах, що охороняються, є бюро перепусток, працівники яких входять до складу підрозділів відомчої охорони.

9.4. Інженерно-технічні засоби охорони

Для обладнання об'єктів охорони повинні використовуватися інженерно-технічні засоби охорони (ІТЗО), що мають державний сертифікат відповідності. Тип, кількість, місця установки і обсяг функцій, виконуваних інженерно-технічними засобами охорони, визначаються при проектуванні відповідно до технічного завдання на розробку, узгодженими та затвердженими з компетентними органами в галузі забезпечення фізичної безпеки в установленому порядку.

Вимоги до ІТЗО об'єкта та їх елементів

Основним призначенням ІТЗО в поєднанні з організаційними заходами є своєчасне виявлення і протидія спробам вчинення актів незаконного втручання (в тому числі терористичних акцій) щодо майна, інформації, обладнання та фізичних осіб на об'єкті.

ІТЗО повинні забезпечувати: передачу сигналу тривоги на пульт чергового (начальника охорони); охорону і телеспостереження периметра і території; контрольно-пропускний режим на території об’єкта; управління доступом на об’єкт в цілому, а також в зони обмеженого доступу і окремі приміщення, ведення протоколу доступу; протипожежний контроль.

До складу ІТЗО входять: система збору, обробки і відображення інформації; технічні засоби охорони, що включають системи охоронної сигналізації (периметра, будівель і споруд), зв’язку та оповіщення, телевізійного спостереження, контролю та управління доступом, охоронного освітлення, гарантованого електропостачання.

Система збору та обробки інформації

Система збору, обробки і відображення інформації (СЗОВІ) – це сукупність пристроїв, призначених для передачі, прийому, збору, обробки, реєстрації та подання оператору інформації від засобів виявлення, а також для дистанційного керування пристроями технічних засобів охорони, контролю працездатності сповіщувачів та каналів передачі інформації. Структурно СЗОВІ повинна складатися з:

- центрального пульта управління на базі персонального комп’ютера і сертифікованих контрольних панелей, інтегрованих в єдину систему і забезпечених спеціалізованим програмним забезпеченням;

- сервера зберігання баз даних;

- апаратури локальної мережі, що розгортається на об’єктах охорони;

- станцій управління окремими системами технічних засобів охорони (ТЗО), виконаних на базі ПК або сертифікованих контрольних панелей серійного виробництва.

СЗОВІ повинна забезпечувати:

- надання за запитом уповноваженої особи інформації про стан будь-якого об'єкта та (або) технічного засобу, що входить до складу ІТЗО. Інформація надається відповідно до прав доступу користувача;

- підключення необмеженого числа користувачів, об’єктів і ТЗО в розрахунку на можливі зміни в структурі об’єкта охорони;

- відображення сигналів, які надходять на центральний пульт управління та інформації у візуальному, світловому та звуковому режимах, причому кожен сигнал повинен відображатися не менше ніж в двох режимах;

- реєстрацію сигналів та інформації, а також запитів уповноважених осіб;

- перешкоджання використанню СЗОВІ неуповноваженими особами.

Інженерні засоби охорони

До інженерних засобів охорони відносяться: огорожа периметра об'єкта охорони і внутрішніх зон обмеженого доступу; КПП з відповідним дооглядовим обладнанням; в'їзні ворота, хвіртки, шлагбауми.

Огорожа повинна виключати випадковий прохід людей (тварин), в'їзд транспорту або ускладнювати проникнення порушників на охороняєму територію, минаючи КПП. До огородження не повинні примикати будь-які прибудови, крім будівель, які є продовженням периметра. Вікна перших поверхів цих будівель, що виходять на територію без охорони, повинні бути обладнані металевими ґратами, а при необхідності й металевими сітками.

Периметри об'єкта охорони і зон обмеженого доступу, а також окремі об'єкти охорони там, де встановлений пропускний режим або планується його введення, повинні бути обладнані КПП для проходу людей і проїзду транспорту (автомобільного, залізничного).

КПП повинен забезпечувати необхідну пропускну здатність проходу людей і проїзду транспорту. Територія КПП обладнується сигнальними огорожами, шлагбаумом і механізованими воротами.

У складі КПП рекомендується передбачити: коридор; приміщення для розміщення бюро перепусток; кімнату огляду; приміщення для співробітників охорони і розміщення технічних засобів охорони. Для виключення можливості несанкціонованого проходу на територію осіб, які не мають встановленої форми пропуску, КПП обладнуються системами контролю і управління доступом.

Для спостереження за обстановкою на території перед КПП із зовнішньої сторони периметра можливе використання вікон з однобічною видимістю, оглядових віконець дверей (воріт) і (або) систем охоронного телеспостереження.

На КПП для пропуску людей повинні бути встановлені стаціонарні металодетектори.

Електроживлення обладнання комплексної систем безпеки

Для аварійного електропостачання об’єктів охорони повинен бути передбачений аварійний дизель-генератор. Для аварійного електропостачання ТЗО можуть використовуватися джерела безперебійного електроживлення (ДБЖ). Потужність ДБЖ повинна бути достатньою для електропостачання протягом не менше 24 годин наступних систем: охоронної та пожежної сигналізації; телевізійного спостереження.

Перехід ТСО на роботу від резервного джерела електроживлення і назад повинен здійснюватися автоматично без видачі сигналів тривоги.

Контрольні запитання

1. Що таке політика інформаційної безпеки?
2. Розкажіть про три ієрархічні рівні політики безпеки.
3. В чому суть системи фізичного захисту? Що таке стримування?
4. Розкажіть про такі складові СФЗ, як виявлення, затримка і реагування.
5. Поясніть загальні обов’язки робітника внутрішньовідомчої охорони.
6. Охарактеризуйте основні заходи пропускного режиму.
7. В чому суть системи збору та обробки інформації?
8. Що відноситься до інженерних засобів охорони?

10. МІЖНАРОДНИЙ СТАНДАРТ БЕЗПЕКИ ISO/IEC 17799

10.1. Загальні відомості

Міжнародний стандарт безпеки ISO/IEC 17799:2005 є практичним керівництвом із захисту інформації. Основними цілями та задачами стандарту ISO 17799 є: формування в світі єдиного підходу до систем управління ІБ на рівні корпорацій; структура загальних вимог ІБ; впровадження принципів ІБ в організаційну структуру компаній; розробка і впровадження ефективної політики безпеки.

Переваги ISO 17799: міжнародне визнання; позитивне сприйняття бізнес-партнерами; поліпшення захищенності інформаційної системи; ефективна політика інформаційної безпеки.

Зміст стандарту

1. Політика безпеки
2. Організаційні заходи щодо забезпечення безпеки
3. Класифікація і управління ресурсами
4. Безпека персоналу
5. Фізична безпека
6. Управління комунікаціями і процесами
7. Контроль доступу
8. Розробка і технічна підтримка обчислювальних систем
9. Управління інцидентами інформаційної безпеки
10. Управління неперервністю бізнесу;
11. Відповідність системи основним вимогам

10.2. Стисла суть розділів стандарту

Нижченаведений матеріал представлений, переважно, заголовками тем кажного з розділів.

10.2.1. Основні напрямки політики забезпечення ІБ

1. Визначення інформаційної безпеки, перелік її складових.
2. Положення про цілі управління – підтримка цілей і принципів інформаційної безпеки.

3. Стисле роз’яснення політики безпеки, принципів її побудови і стандартів в цій сфері. Відповідність політики вимогам з особливим значенням для організації, наприклад: положення політики мають відповідати як державному, так і міжнародному законодавству; розуміння про наслідки порушення політики безпеки; нерерервність виявлення і блокування вірусів та інших шкідливих програм.

4. Включення в посадові обов’язки керівників відповідальності стосовно забезпечення інформаційної безпеки, а також складання звітів про інциденти.

5. Докладний перелік документів, котрі мають бути видані разом з політикою безпеки (інструкції, регламенти і т.п.).

10.2.2. Організаційні заходи щодо забезпечення безпеки

1. Завдання керівництва організації щодо забезпечення інформаційної безпеки.
2. Координація питань, пов'язаних з інформаційною безпекою.
3. Розподіл відповідальності щодо забезпечення безпеки.
4. Процес прийняття нової інформаційної системи.

Завдання керівництва організації

Керівництву організації слід брати участь в процесі забезпечення інформаційної безпеки:

- визначити цілі інформаційної безпеки;
- визначити обов'язки і відповідальність співробітників по забезпеченню інформаційної безпеки;
- організувати взаємодію між структурними підрозділами організації з питань забезпечення інформаційної безпеки.

Координація питань, зв’язаних с ІБ

1. Вироблення угод про розмежування відповідальності за забезпечення інформаційної безпеки всередині організації.

2. Вироблення спеціальних методик і політик, пов'язаних з інформаційною безпекою: аналіз ризиків, класифікація систем та захисту інформації за рівнями безпеки.

3. Підтримка в організації “атмосфери” інформаційної безпеки, зокрема, регулярне інформування персоналу з цих питань.

4. Забезпечення обов’язковості врахування питань інформаційної безпеки при стратегічному та оперативному плануванні.

5. Забезпечення зворотного зв’язку (оцінка адекватності вжитих заходів безпеки в існуючих системах) і координація впровадження засобів забезпечення; інформаційної безпеки в нові системи або сервіси.

6. Аналіз інцидентів в області інформаційної безпеки, вироблення рекомендацій.

Розподіл відповідальності стосовно забезпечення безпеки

1. Визначення ресурсів, що мають відношення до інформаційної безпеки по кожній системі.

2. Для кожного ресурсу (процесу) повинен бути призначений відповідальний співробітник з числа керівників. Розмежування відповідальності повинно бути закріплено документально.

3. Для кожного ресурсу повинен бути визначений та закріплений документально список прав доступу (матриця доступу).

Процес прийняття нової інформаційної системи

1. Нова інформаційна система повинна відповідати існуючій політиці управління користувачами, в якій описані цілі і завдання користувачів, а також в обов’язковому порядку узгоджуватися з керівником, відповідальним за забезпечення безпеки даної системи.

2. Усі компоненти системи, що впроваджується мають бути перевірені на сумісність з існуючими частинами системи.

10.2.3. Класифікація та управління інформаційними ресурсами

Мета класифікації інформаційних ресурсів – гарантувати, що рівень захисту інформаційних ресурсів відповідає їх критичності.

Критерії класифікації інформаційних ресурсів: вартість ресурсу; вимоги законодавства; критичність ресурсу для інформаційної системи.

Кожному ресурсу слід привласнити категорію критичності і визначити правила: обробки; зберігання; передачі; зняття категорії критичності; знищення; реєстрації інцидентів, пов'язаних з ресурсом.

10.2.4. Безпека персоналу

Необхідно включити завдання забезпечення безпеки в службові обов'язки всіх співробітників. Перевірка персоналу при прийомі на роботу складається з: перевірки рекомендацій; перевірки даних з резюме; підтвердження наукових ступенів і освіти; ідентифікації особистості.

Необхідно укласти угоди про дотримання режиму інформаційної безпеки з усіма співробітниками.

Безпека в процесі роботи співробітника

Керівництву організації потрібно зобов'язати співробітників, підрядників і третіх осіб виконувати вимоги до забезпечення інформаційної безпеки відповідно до затверджених в організації інструкціями і процедурами.

Всі співробітники і, при необхідності, підрядники та треті особи повинні проходити навчання з питань інформаційної безпеки, а також отримувати оновлені версії політик і процедур забезпечення інформаційної безпеки відповідно до їх посадових обов'язків.

Слід затвердити формальну процедуру накладання дисциплінарних стягнень на співробітників, які порушили прийняті в організації вимоги до інформаційної безпеки.

Правила звільнення або зміни посади співробітника

Повернення матеріальних цінностей: при звільненні, закінчення терміну контракту або договору всі співробітники, підрядники та треті особи повинні здійснити повернення матеріальних цінностей організації, які перебували в їх користуванні під час роботи (дії договору).

Відгук наданих прав доступу: при звільненні, закінчення терміну договору або контракту всі права доступу співробітників, клієнтів або третіх осіб до інформації або засобам її обробки повинні бути відкликані, а відомі їм аутентифікаційні дані змінені.

10.2.5. Фізична безпека

1. Безпека обладнання.
2. Безпека кабельної системи.
3. Безпека знищення обладнання при списуванні.
4. Безпека робочого місця.

10.2.6. Управління комунікаціями і процесами

1. Службові інструкції і відповідальність.
2. Захист від шкідливого ПЗ (вірусів, троянських коней та ін.).
3. Управління внутрішніми ресурсами.
4. Управління мережами.
5. Безпека носіїв даних.
6. Безпека при передачі інформації і ПЗ.

Захист від шкідливого ПЗ (вірусів, троянських коней та ін.)

Для захисту від шкідливого ПЗ мають бути прийняті наступні заходи:

- обов'язковість застосування тільки ліцензійного програмного забезпечення і заборона використання незатвердженого ПЗ мають бути закріплені документально;

- з метою зниження ризиків, зв'язаних з отриманням ПЗ через мережі загального користування або на носіях, цей процес має бути формалізований у вигляді належного документа;

- усі системи мають бути забезпечені антивірусними програмами, які повинні своєчасно оновлюватися. Сканування всіх систем повинно проводитися регулярно;

- цілісність програмного забезпечення, що займається обробкою критичних даних (і самих даних) повинна перевірятися регулярно. За фактом відхилення від еталонних значень має проводитися службове розслідування;

- всі вузли, через які в систему надходить інформація у вигляді файлів, повідомлень і т.п. повинні забезпечувати антивірусний контроль вхідної інформації;

- в організації повинен бути розроблений і задокументований механізм відновлення після вірусних атак, зокрема, визначено процедури резервного копіювання ПЗ і даних;

- моніторинг всієї інформації, що стосується шкідливого ПЗ, зокрема, аналіз всіх публікованих бюлетенів і попереджень по цій темі.

Управління внутрішніми ресурсами

1. Резервні копії разом з інструкціями відновлення мають зберігатися в місці, територіально віддаленому від основної копії інформації. Для особливо важливої інформації треба зберігати три останніх копії.

2. До резервних копій має бути застосований адекватний ряд фізичних і організаційних заходів захисту, які відповідають стандартам для використовуваних носіїв.

3. Носії для резервного копіювання повинні регулярно перевірятися на працездатність.

4. Для персоналу має проводитись регулярна перевірка і практичний тренінг з метою відновлення даних в установленому порядку на протязі гарантованого проміжку часу.

Запис дій операторів

До обов'язкової реєстрації в системних журналах повинні підпадати: час старту і зупинки системи; системні помилки і дії щодо їх виправлення; підтвердження коректного поводження з вхідними і вихідними даними; ідентифікатор оператора, який виправив дію, що призвела до запису в журналі реєстрації.

Безпека носіїв даних

Така безпека забезпечується відповідним управлінням носіями. *Управління змінними носіями включає*: знищення в установленому порядку всіх носіїв, термін експлуатації яких закінчився; отримання спеціального дозволу для виносу носіїв за межі організації, причому факт винесення повинен бути зафіксований в спеціальному журналі (базі даних); всі носії повинні зберігатися в безпечному місці відповідно до вимог компанії-виробника.

Наступні носії та інформація вимагають підвищеної безпеки при зберіганні: паперові документи: записи на касетах, копіювальний папір, звіти, картриджі, магнітні стрічки, знімні диски або касети; оптичні носії, листинги програм, тестові дані; системна документація.

10.2.7. Управління доступом

Реєстрація користувача

1. Використання унікального ідентифікатора користувача, за яким його можна однозначно ідентифікувати. Застосування групових ідентифікаторів може бути дозволено тільки там, де це потрібно для виконання роботи.

2. Перевірка, що користувач авторизований відповідальним за систему для роботи з нею. Можливе отримання окремого дозволу для наділення правами користувача у керівництва.

3. Перевірка, що рівень доступу відповідає бізнес-завданням політики безпеки організації і не суперечить розподілу обов'язків (відповідальності).

4. Документальна фіксація призначених користувачеві прав доступу.

5. Ознайомлення користувача під розпис з наданими правами доступу і порядком його здійснення.

6. Всі сервіси повинні дозволяти доступ тільки аутентифікованим користувачам.

7. Забезпечення формального списку всіх осіб, зареєстрованих для роботи в системі.

8. Негайне виправлення (видалення) прав доступу при зміні посадових обов'язків (звільнення).

9. Періодичний контроль і видалення записів, що не використані.

10. Забезпечення недоступності запасних ідентифікаторів іншим користувачам.

Перевірка прав користувача

1. Перевірка прав користувачів повинна проводитися регулярно (кожні 6 місяців) або після кожної зміни в системі.

2. Перевірка прав користувачів, які мають особливі привілеї для доступу в систему повинна проводитися частіше - кожні 3 місяці.

3. Необхідно регулярно перевіряти адекватність призначених привілеїв, щоб уникнути отримання будь-ким з користувачів зайвих прав.

Усі користувачі повинні знати, що необхідно:

- зберігати паролі строго конфіденційно;
- уникати запису паролів на папері, якщо вони не зберігаються в безпечному місці;
- при компрометації (розголошення або підозрі на розголошення пароля) негайно міняти паролі;
- вибирати якісні паролі і знати що: пароль легко запам'ятовується, але не є легко ідентифікованою інформацією (ім'я користувача, дата народження і т.п.), пароль не містить слова, занесені в словники паролів, пароль не є по-

вторюваною послідовністю будь-яких символів (наприклад, "111111", “аааааа” і т .п.);

- змінювати паролі на регулярній основі (або через певний проміжок часу, або після певного числа використань), при цьому паролі привілейованих користувачів повинні змінюватися частіше. При зміні пароля неприпустимо вибирати паролі, які вже використовувалися раніше;

- змінювати заданий адміністратором тимчасовий пароль при першому ж вході в систему;

- не використовувати автоматичний вхід в систему, не застосовувати збереження пароля під функціональними клавішами;

- не повідомляти іншим користувачам особистий пароль, не реєструвати їх в системі під своїм паролем.

Контроль доступу в ОС. Використання системних утиліт

1. Застосовувати процес аутентифікації при використанні системних утиліт.
2. Окремо зберігати системні утиліти і додатки.
3. Обмежити використання системних утиліт мінімально можливого числа довірених авторизованих користувачів.
4. Спеціальна авторизація при використанні системних утиліт.
5. Обмеження доступності системних утиліт.
6. Протоколювання при використанні системних утиліт.
7. Визначення і документування способу авторизації для запуску системних утиліт.
8. Видалення всіх системних утиліт, використанні яких в даній системі не є необхідним.

Мобільні комп’ютери і користувачі

Віддалена робота. Вимоги безпеки.

1. Забезпечення фізичного захисту місця віддаленої роботи.
2. Забезпечення безпеки телекомунікацій, що враховує необхідність віддаленого доступу до внутрішніх ресурсів компанії; важливість інформації і систем, до яких буде здійснено віддалений доступ; проходження через канали зв’язку.

3. Облік можливої загрози несанкціонованого доступу до інформації або ресурсів, від близьких до віддаленому користувачеві людей, наприклад, сім'я, друзі.

Забезпечення безпеки.

1. Забезпечення необхідним обладнанням для віддаленого мобільного доступу.

2. Визначення дозволених видів робіт, дозволеного часу доступу, класифікація інформації, яка може оброблятися віддалено, визначення систем і сервісів, до яких цьому мобільному користувачеві дозволено віддалений доступ.

3. Забезпечення необхідним комунікаційним устаткуванням, включаючи засоби забезпечення безпеки.

4. Фізична безпека.

5. Правила доступу до обладнання та інформації для членів сім'ї і відвідувачів.

6. Забезпечення програмним забезпеченням та обладнанням.

7. Наявність процедур резервного копіювання та забезпечення безперервності ведення бізнесу.

8. Аудит і моніторинг безпеки.

9. Анулювання дозволу, прав доступу і повернення обладнання при скасуванні (завершенні) віддаленого мобільного доступу.

10.2.8. Розробка і технічна підтримка обчислювальних систем

1. Безпека додатків.
2. Криптографічний захист даних.
3. Безпека системних файлів.
4. Безпека процесів розробки і підтримки.

Безпека системних файлів. Захист даних, які використовуються в процесі тестування систем

1. Система розмежування доступу до тестової системи повинна відповідати доступу до звичайної системи.

2. Потрібно забезпечення різних авторизацій кожного разу, коли оперативна інформація копіюється в тестову систему.

3. Після завершення тестів робочу інформацію треба негайно вилучити з тестової системи.

4. Копіювання і використання робочої (оперативної) інформації повинно бути запротокольовано для подальшої можливості аудиту.

Процедури контролю змін

1. Документальне закріплення типових рівнів доступу.

2. Забезпечення того, що зміни зроблені авторизованими користувачами.

3. Ідентифікація всього програмного забезпечення, інформації, баз даних, апаратного забезпечення, яке вимагає змін.

4. Отримання формального дозволу для деталізації пропозицій до початку робіт.

5. Забезпечення того, що авторизовані користувачі приймають (перевіряють) зміни до їх впровадження.

6. Забезпечення безпечного впровадження змін без наслідків для бізнесу.

7. Забезпечення змін системної документації після кожної модифікації, а також архівація старої документації або її відхилення.

8. Забезпечення контролю версій для всіх оновлень програмного забезпечення.

9. Забезпечення протоколювання всіх запитів на зміну.

10. Забезпечення відповідних змін оперативної і призначеної для користувача документації.

11. Забезпечення того, що впровадження змін мало місце у відповідний час і не торкнулося залучені в роботу бізнес-процеси.

10.2.9. Управління інцидентами ІБ

Таке управління повинно передбачати всі можливі ситуації, включаючи: збої в інформаційних системах; відмови в обслуговуванні; помилки через неповні або неправильні вхідні дані; витік інформації.

У доповнення до оперативного плану процедури управління повинні також включати: аналіз і визначення причин інциденту; планування та впровадження заходів для запобігання повторенню (якщо необхідно); аналіз і

збереження відомостей про інцидент, які можна уявити як доказ (докази, свідчення і т.п.); визначення порядку взаємодії між постраждалими від інциденту і учасниками процесу відновлення; обов'язкове інформування відповідальних осіб.

По кожному інциденту має бути зібрано максимальну кількість інформації для: подальшого аналізу внутрішніх проблем; використання зібраних даних для притягнення винних до дисциплінарної, адміністративної або кримінальної відповідальності; використання при веденні переговорів про компенсації з постачальниками апаратного і програмного забезпечення.

Дії по відновленню після виявлення вразливостей в системі безпеки, виправлення помилок і ліквідації несправностей повинні бути уважно запротокольовані. Процедура повинна гарантувати що: тільки персонал, що пройшов процедури ідентифікації і аутентифікації може отримувати доступ до "ожилим" систем і даних; всі дії по виходу з нештатної ситуації зафіксовані у вигляді документа для подальшого використання; про всі проведені дії керівництво було проінформовано в установленому порядку; цілісність і працездатність системи підтверджена в мінімальні терміни.

10.2.10. Управління неперервністю бізнесу

Управління неперервністю базується на наступних принципах.

1. Процес управління безперервністю ведення бізнесу повинен бути регламентований.
2. Потрібно створити і впровадити план неперервного ведення бізнесу;
3. Основи планування неперервності бізнесу;
4. Тестування, забезпечення і переоцінка плану безперервного ведення бізнесу.

Розглянемо перелічені 4 пункти дещо докладніше.

Процес управління неперервним веденням бізнесу

1. Усвідомлення ризиків, їх ймовірностей, можливих наслідків, включаючи ідентифікацію і розстановку пріоритетів для критичних бізнес-процесів.
2. Усвідомлення шкоди в разі переривання бізнесу, створення бізнес-цілей для інформаційно-обробної системи компанії.

3. Вибір підходящої схеми страхування, яка може бути однією з форм підтримки безперервності ведення бізнесу.

4. Формалізація і документування стратегії ведення безперервного бізнесу, що містить узгоджені цілі бізнесу і пріоритети.

5. Регулярне тестування і обновлення планів та процесів.

6. Необхідно переконатися, що управління безперервним веденням бізнесу впроваджено в організаційні процеси і структуру компанії.

7. Відповідальність для координації управління безперервним веденням бізнесу повинна бути поширена за відповідними рівнями всередині організації, так званий форум з інформаційної безпеки.

Створення і впровадження плану неперервності бізнесу

1. Розподіл відповідальності і визначення всіх контраварійних процедур (порядок дій в аварійній ситуації).

2. Впровадження контраварійних процедур для відновлення систем у відведений період часу. Особлива увага приділяється оцінці залежності бізнесу від зовнішніх зв’язків.

3. Документування всіх процесів і процедур.

4. Відповідне навчання персоналу порядку дій в аварійних ситуаціях включаючи управління в кризових процесах.

5. Тестування і обновлення планів.

Основи планування неперервності бізнесу

1. Умови вступу в дію планів (як оцінити ситуацію, хто в неї втягнутий).

2. Контраварійні процедури, що описують дії в разі інцидентів, які становлять небезпеку для бізнес-операцій або/і людського життя. Процедури повинні включати в себе заходи щодо зв’язків з громадськістю та органами влади.

3. Процедури нейтралізації несправностей, в яких описуються дії по виведенню життєво важливих бізнес-потреб або служб підтримки у тимчасове альтернативне приміщення і повернення їх у відповідний період часу.

4. Процедури відновлення, в яких наведені дії щодо повернення до нормального процесу бізнес-операцій.

5. Розробка програми, в якій описано, як і коли план буде протестований і впроваджений.

6. Дії з інформування та навчання, які розробляються для розуміння персоналом процесу забезпечення безперервності бізнесу і гарантії, що цей процес продовжує бути ефективним.

7. Особиста відповідальність – хто саме відповідає за виконання кожного компонента плану із зазначенням дублюючих осіб.

Тестування планів забезпечення неперервності бізнесу

1. Базові тести різних сценаріїв (обговорення заходів по відновленню бізнесу в разі різних ситуацій).

2. Моделювання (практичний тренінг персоналу щодо дій у критичній ситуації).

3. Тестування технічних заходів по відновленню (для гарантії того, що інформаційна система буде ефективно відновлена).

4. Тестування технічних заходів по відновленню в альтернативному місці (запуск бізнес-процесів разом з відновлювальними заходами поза основним місцем розташування).

5. Тести систем і постачальників послуг (гарантія, що зовнішні надаються сервіси та продукти будуть відповідати контрактним зобов'язанням).

6. Комплексні навчання (тестування того, що компанія, персонал, обладнання, інформаційна система можуть впоратися з нештатної ситуацією).

10.2.11. Відповідність системи захисту основним вимогам

Суть відповідності складається в:

- розробці та впровадженні політики дотримання авторського права на програмне забезпечення, де визначається легальне використання ПЗ та інформаційних продуктів;

- випуску стандартів для процедур придбання програмного забезпечення;

- забезпеченні поінформованості користувачів про авторські права на програмне забезпечення, правила придбання програмного забезпечення та повідомлення користувачів, що в разі порушення будуть зроблені дисциплінарні дії;

- забезпеченні можливості доказати, що дане програмне забезпечення ліцензійно;

- контролі того, що максимальне число користувачів в ліцензії не перевищено;

- виконанні перевірок, що тільки дозволені і ліцензійні продукти інстальовані;

- розробці політики для забезпечення відповідних умов ліцензійної угоди;

- розробці політики щодо розміщення або передачі програмного забезпечення стороннім особам або компаніям;

- застосування відповідних засобів аудиту;

- дотримання умов для програмного забезпечення та інформації, отриманих з відкритих мереж.

Контрольні запитання

1. Що являє собою міжнародний стандарт безпеки ISO/IEC 17799 ?
2. Розкажіть стисло про суть розділів стандарту “ Політика безпеки” і “Класифікація та управління ресурсами”.
3. Розкажіть стисло про суть розділу стандарту “Організаційні заходи щодо забезпечення безпеки”.
4. Розкажіть про суть розділів стандарту “ Безпека персоналу” і “Фізична безпека”.
5. Розкажіть стисло про суть розділу стандарту “Управління комунікаціями і процесами”.
6. Розкажіть про суть розділу стандарту “Контроль доступу”.
7. Розкажіть про суть розділів стандарту “Розробка і технічна підтримка обчислювальних систем” і “Управління інцидентами”.
8. Розкажіть про суть розділу стандарту “Управління неперервністю бізнесу”.
9. Розкажіть про суть розділу стандарту “Відповідність системи основним вимогам”. Поясніть власними словами причини розповсюдженості ISO/IEC 17799 у світі.

11. АУДИТ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. АНАЛІЗ РИЗИКІВ КОРПОРАТИВНИХ ІС

11.1. Основні етапи аудиту ІБ

1. Технологічний аудит.
2. Аудит системи управління ІБ (за ISO 17799).
3. Аналіз інформаційних ризиків.

Технологічний аудит

Застосовувані методики: NSA Infosec, NIST, OSSTM.

Об'єкти аудиту: мережева інфраструктура, сервери, робочі станції.

Аудит системи управління інформаційною безпекою на основі ISO 17799

1. Організаційні заходи щодо забезпечення безпеки.
2. Класифікація та управління ресурсами.
3. Безпека персоналу.
4. Фізична безпека.
5. Управління комунікаціями і процесами.
6. Контроль доступу.
7. Розробка і технічна підтримка обчислювальних систем.
8. Управління неперервністю бізнесу.
9. Відповідність системи основним вимогам.

Аналіз інформаційних ризиків

Метою аналізу інформаційних ризиків є розробка економічно ефективної і обгрунтованої системи забезпечення інформаційної безпеки.

Завданнями аналізу є: комплексна оцінка захищеності ІС; оцінка вартості інформації (потенційного збитку); оцінка ризику (ймовірності шкоди); розробка комплексної системи забезпечення ІБ відповідно до оцінок інформаційних ризиків.

Аналіз інформаційних ризиків необхідний для: визначення можливої шкоди (ризику) за існуючими видами цінної інформації, співвідношення ри-

зику з витратами на забезпечення інформаційної безпеки, оцінки ефективності витрат на забезпечення інформаційної безпеки.

Інформаційний ризик – це величина, що залежить від рівня захищеності об'єкта і яка формулюється як:

РИЗИК = Р (ймовірність реалізації загрози) · Вартість збитку

В якості критеріїв оцінки захищеності інформаційних систем можуть застосовуватися як кількісні, так і якісні методи оцінки.

Критерії проведення аудиту інформаційної безпеки встановлюються на основі загальноприйнятих міжнародних стандартів (наприклад, міжнароднийий ISO 17799, німецький BSI і ін.), внутрішніх стандартів аудиторських компаній і вітчизняних відомчих стандартів.

Як приклад в підрозділі 11.2 представлені заголовки основних тем стандарту BSI.

11.2. Німецький стандарт для вибору критерію аудиту BSI

Стандарт складається з двох основних частин : *методологія управління ІБ*; *компоненти інформаційних технологій*. Окрім того стандарт містить *каталоги загроз безпеки и контрзаходів* (близько 600 найменувань в кожному каталозі).

Методологія управління

1. Організація менеджменту у сфері ІБ.
2. Методологія керівництва.

Компоненти інформаційних технологій

1. Основні компоненти (організаційний рівень ІБ, процедурний рівень, організація захисту даних, планування дій у надзвичайних ситуаціях).
2. Інфраструктура (будівлі, приміщення, кабельні мережі, організація віддаленого доступу).
3. Клієнтські компоненти різних типів (DOS, Windows, UNIX, мобільні компоненти, інші типи).
4. Мережі різних типів (з'єднання "точка-точка", мережі Novell NetWare, мережі з ОС UNIX і Windows, різнорідні мережі).

5. Елементи систем передачі даних (електронна пошта, модеми, міжмережеві екрани і т.д.).

6. Телекомунікації (факси, автовідповідачі, інтегровані системи на базі ISDN, інші телекомунікаційні системи).

7. Стандартне ПЗ.

8. Бази даних.

Каталог загроз безпеки (загрози і контрзаходи) за класами

1. Форс-мажорні обставини;
2. Недоліки організаційних заходів;
3. Помилки людини;
4. Технічні несправності;
5. Умисні дії.
6. Поліпшення інфраструктури;
7. Адміністративні контрзаходи;
8. Процедурні контрзаходи;
9. Програмно-технічні контрзаходи;
10. Зменшення вразливості комунікацій;
11. Планування дій в надзвичайних ситуаціях.

11.3. Порівняння підходів за ISO 17799 і BSI

У міжнародному стандарті декларуються деякі загальні принципи, які пропонується конкретизувати стосовно до досліджуваних інформаційних технологій.

У другій частині основна увага приділена сертифікації інформаційної системи на відповідність стандарту, тобто формальної процедури, що дозволяє переконатися у реалізації декларованих принципів. Обсяг стандарту порівняно невеликий – менше 120 сторінок в обох частинах.

Недоліком стандарту є високі вимоги до кваліфікації фахівців, які здійснюють перевірку на відповідність вимогам стандарту. Крім того, в ньому недостатньо враховується специфіка сучасних розподілених систем.

У німецькому стандарті, навпаки, розглянуто багато “окремих випадків” – різних елементів інформаційних технологій. Обсяг документа дуже великий – кілька тисяч сторінок і, безсумнівно, він буде зростати.

Такий підхід має свої переваги і недоліки.

Перевагою BSI є врахування специфіки різних елементів. Зокрема, набагато краще, у порівнянні з британським стандартом, розглянуті особливості забезпечення ІБ в сучасних мережах. Іншою перевагою є використання гіпертекстової структури, що дозволяє оперативно вносити зміни і коригувати зв'язки між частинами стандарту.

Недолік – неможливість осягнути неосяжне. Безліч елементів сучасних інформаційних технологій викладено на однаковому рівні деталізації. Неминуче доводиться вводити розділ "інше", в якому в загальному вигляді розглядаються менш поширені елементи.

11.4. Міжнародний стандарт з управління СУІБ ISO 27001

Цей стандарт створений для надання моделі розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення системи управління інформаційною безпекою (СУІБ). Прийняття СУІБ повинне бути стратегічним рішенням для організації. Передбачається, що впровадження СУІБ буде масштабуватися відповідно до потреб організації, наприклад, проста ситуація потребує простого рішення для СУІБ.

Цей стандарт може бути використаний зацікавленими внутрішніми та зовнішніми сторонами для оцінки відповідності вимогам.

Стандарт складається з 5 основних розділів: *Система управління інформаційною безпекою (СУІБ)*; *Обов'язки керіввництва компании*; *Внутрішній аудит СУІБ*; *Перевірки СУІБ керівництвом компанії*; *Вдосконалення СУІБ.*

Процесний підхід до управління інформаційною безпекою, запропонований цим стандартом, заохочує його користувачів робити наголос на важливості: 1) розуміння вимог інформаційної безпеки організації і необхідності розроблення політики та цілей інформаційної безпеки; 2) впровадження контролів та їх функціонуванні для управління ризиками інформаційної безпеки організації в контексті загальних бізнес-ризиків організації; 3) моніторингу та перегляді продуктивності та ефективності СУІБ; 4) постійному вдосконаленні, основаному на об'єктивному вимірюванні.

Цей стандарт приймає модель "Плануй-Виконуй-Перевіряй-Дій" (Plan-Do-Check-Act – надалі PDCA), яку застосовують для структуризації всіх про-

цесів СУІБ. Стандарт узгоджено із стандартами ISO 9001 (стандарт з розробки системи якості) та ISO 14001 (стандарт з охорони навколишнього середовища) з метою підтримки послідовного і комплексного впровадження і функціонування системи якості організації.

Таким чином, одна відповідним чином запроектована система управління може задовольняти вимоги всіх трьох стандартів.

11.5. Оцінювання можливого збитку (втрат)

Оцінюючи наслідки збитку, потрібно розуміти, що виникають витрати:

- *безпосередні* на заміну обладнання, аналіз і дослідження причин подолання захисту, відновлення інформації і функціонування ІС;

- *непрямі*, зв'язані із зниженням банківської довіри, втратою клієнтури, послабленням репутації та позицій на ринку.

Для оцінювання втрат необхідно побудувати сценарій дій трьох сторін: порушника по використанню добутої інформації; служби інформаційної безпеки щодо запобігання наслідків і відновлення нормального функціонування системи; третьої сторони.

Мотивами злочинів є недосвідченість, корисливий інтерес, безвідповідальність (самоствердження). Основний принцип при обліку мотівів і причин порушень – принцип розумної достатності, а іноді і "золотої середини".

Оцінюючи наслідки втрати ресурсу потрібно враховувати вартість:

- ресурсу (витрати на виробництво), відновлення або створення (придбання) нового ресурсу;

- відновлення працездатності організації (при роботі зі спотвореним ресурсом, без нього, при дезінформації);

- вимушеного простою і упущеної вигоди (втрачений контракт);

- виплат за невиконання зобов'язань контракту;

- витрат на реабілітацію підмоченої репутації, престижу фірми;

- витрат на пошук нових клієнтів, на пошук (або відновлення) нових каналів зв'язку та інформаційних джерел.

Типи виникаючих конфліктів

1. Обмеженість ресурсів (обчислювальних, інформаційних).
2. Невідповідність цілей співробітників СІБ та інших відділів.

3. Вимоги режиму.
4. Психофізіологічні особливості співробітників СІБ та інших відділів.
5. Невідповідність очикувань реальності.
6. Конфлікти в особистому житті співробітників.
7. Ієрархічні конфлікти.
8. Конфлікт людина-машина.

Для усунення конфліктів та їх запобігання потрібно задіяти певні *стратегії управління ризиками, наприклад:* зміна характеру ризику; його зменшення; ухилення від ризику; прийняття ризику.

Рівні аналізу ризиків: базовий; повний.

Аналіз ризиків для базового рівня ІБ

Для того щоб забезпечити базовий рівень безпеки, достатньо буде перевірити виконання вимог відповідного стандарту (специфікації), наприклад ISO 17799. Програмні продукти, призначені для цієї мети, дозволяють сформувати список питань, що стосуються виконання цих вимог. На основі відповідей генерується звіт з рекомендаціями щодо усунення виявлених недоліків.

Прикладом програмного продукту цього класу є продукти КОНДОР і COBRA. Дані програмні засоби дозволяють істотно полегшити процес перевірки інформаційної системи на відповідність вимогам стандарту ISO 17799. Є кілька баз знань: загальні вимоги і спеціалізовані бази, орієнтовані на різні сфери застосування. Ще один приклад – програма RiskPAC фірми CSCI (Австралія). Область застосування – перевірка на відповідність вимогам базового рівня захищеності організації. Є можливість налаштування на різні сфери застосування шляхом додавання (виключення) додаткових запитань. Крім того, є калькулятор очікуваних середньорічних втрат, що дозволяє оцінити очікувані втрати за різними видами інформаційних ресурсів.

Повний аналіз ризиків

Програмні засоби, що дозволяють провести повний аналіз ризиків, будуються з використанням структурних методів системного аналізу і проектування (SSADM - Structured Systems Analysis and Design). Вони являють собою інструментарій для: побудови моделі ІС з точки зору ІБ; оцінки цінності

ресурсів; складання списку загроз і вразливостей, оцінки їх характеристик; вибору контрзаходів і аналізу їх ефективності; аналізу варіантів побудови захисту; документування (генерація звітів).

Прикладами програмних продуктів цього класу є CRAMM – розробник Logica (Великобританія), MARION – розробник CLUSIF (Франція), RiskWatch (Національний інститут стандартів і технологій США за участю МО США і Канади), ГРИФ – розробник Digital Security (Росія).

Обов'язковим елементом цих продуктів є база даних, яка містить інформацію по інцидентах в області ІБ, що дозволяє оцінити ризики і уразливості, ефективність різних варіантів контрзаходів.

Принципи, покладені в основу методик аналізу ризиків

Один з можливих підходів до розробки подібних методик – накопичення статистичних даних про реальні події, аналіз і класифікація їх причин, виявлення факторів ризику. На основі цієї інформації можна оцінити загрози та вразливості в інших інформаційних системах. Практичні складності в реалізації цього підходу такі: по-перше, повинен бути зібраний досить великий матеріал про події в цій галузі; по-друге, застосування цього підходу виправдано далеко не завжди.

Якщо інформаційна система досить велика (містить багато елементів, розташована на великій території), має давню історію, то подібний підхід, швидше за все, можна застосувати. Якщо система порівняно невелика, використовує тільки новітні елементи технології (для яких поки немає достовірної статистики), оцінки ризиків можуть виявитися недостовірними.

Альтернативою статистичного підходу є підхід, заснований на аналізі особливостей технології. Прикладом є згаданий Німецький стандарт BSI, великий каталог загроз і контрзаходів, який доступний в Інтернет. Втім, цей підхід також не універсальний: темпи технологічного прогресу в області IT такі, що наявні оцінки відносяться до вже застарілих технологій. Для новітніх технологій таких оцінок поки не існує.

Оцінка ефективності вкладених коштів

ROSI – Return of Security Investment – коефіцієнт окупності інвестицій в інформаційну безпеку. ROSI визначає ефективність кожної одиниці грошових коштів, вкладених в інформаційну безпеку.

В загальному випадку ROSI визначається як відношення прибутку до вкладених коштів. У сфері інформаційної безпеки прибуток – величина, на яку знизився інформаційний ризик після впровадження контрзаходів. Таким чином, отримаємо

$$ROSI = (R1-R2):C,$$

де *R1* – ризик до впровадження, *R2* – ризик після впровадження, *C* – витрати на впровадження контрзаходів.

11.6. Оцінювання ефективності існуючої системи захисту ІС з використанням спеціалізованих інструментаріїв

Оцінювання ефективності існуючої системи захисту ІС включає:

- визначення і фіксування на момент перевірки реальної конфігурації засобів захисту ІС;

- проведення випробувань програмних і програмно-апаратних засобів захисту, а також вбудованих механізмів захисту загальносистемного програмного забезпечення, що використовуються в ІС для захисту інформації при: тестових випробуваннях програмних засобів захисту; тестових випробуваннях захисту ІС від витоку за рахунок наведень і перешкод від електромагнітних випромінювань; тестових випробуваннях захисту інформації від витоку акустичним і віброакустичним каналу; проведенні випробувань функцій системи захисту інформації методом моделювання дій зловмисника і ін.

Насамкінець відзначимо, що в останні кілька років у зв’язку з багатьма хакерськими атаками не тільки в інформаційні системи підприємств, а й в ІС ключових державних структур, поняття “інформбезпека” розширилося до поняття “кібербезпека”.

Кібербезпека – це процес використання заходів безпеки для забезпечення конфіденційності, цілісності та доступності електронних даних організації при спробі свідомо завдати шкоди не тільки БД, а й одночасно операційній системі сервера з кількох сторін (мереж). Такі заходи стосуються не тільки корпоративних ІС, а й інфокомунікаційних мереж та середовища, в якому дані передаються (звідси термін – “кіберсереда”). Іншими словами, під захист беруться не тільки локальні мережі комп’ютерів і серверів, а й будівлі, персонал і середовище передачі інформації (кабелі, лінії зв'язку з відповід-

ним обладнанням, приймачі, передавальні станції тощо). Метою забезпечення кібербезпеки є найбільш повний захист даних (сервера) як в процесі передачі і/або обміну, так і в процесі їх зберігання.

Зараз в країнах Заходу планується навчання з кібербезпеки вже зі шкільної лави. Так, у Великобританії школярам запропонують уроки, на яких вони будуть навчатися навичкам, що дозволяють забезпечити безпеку британських компаній і організацій від мережевих атак хакерів. Навчальна програма розроблена Міністерством культури, ЗМІ і спорту Великобританії. Уроки плануються реалізувати як в онлайн-формі так і в формі позакласних занять, які будуть проходити чотири рази на тиждень і проводитися викладачами-експертами. Програма спрямована на учнів у віці від 14 до 18 років. Проведення перших пробних занять заплановано на вересень 2017 року.

Розгляд конкретних заходів щодо забезпечення кібербезпеки організацій України виходить за межі конспекту лекцій.

Контрольні запитання

1. Яким чином здійснюється оцінка можливого збитку (втрат)?
2. Розкажіть про основні етапи аудиту ІБ.
3. Що таке інформаційний ризик? Як можна оцінити його ефективність?
4. Поясніть суть німецького стандарт для вибору критерію аудиту BSI.
5. Порівняйте переваги і недоліки стандартів ISO 17799 і BSI
6. В чому суть вимог стандарту з управління системою ІБ ISO 27001?
7. Як можна провести оцінювання можливих втрат (збитків)?
8. В чому суть аналізу ризиків базового і повного рівня ІБ?
9. В чому суть коефіцієнта окупності інвестицій в інформаційну безпеку?
10. Поясніть суть поняття “кібербезпека”.

ЛІТЕРАТУРА

Основна

1. Белов Е.Б. Основы информационной безопасности / Е.Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов.. – М.: Горячая линия - Телеком, 2006. – 544 с.
2. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К.: МК-Прес, 2005. – 432 с.
3. Ємельянов С.Л. Основи інформаційної безпеки. – Одеса: Фенікс, 2014.– 357 с.
4. Емельянов С.Л. Проблема защиты информации от утечки и пути ее решения. – Одесса: Феникс, 2011.– 624 с.
5. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД “Гельветика”, 2017. – 168 с.
6. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В.Романец, П.А.Тимофеев, В.Ф.Шаньгин – М.: Радио и связь, 1999. – 328 с.

Додаткова

1. Бондарев В.В.. Введение в информационную безопасность автоматизированных систем. – М.: ГТУ им. Н.Э. Баумана, 2016. – 252 с.
2. Богуш В.М. Криптографічні застосування елементарної теорії чисел / В.М. Богуш, В.А. Мухачов. – К.: ДУІКТ, 2006. – 126 с.
3. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.
4. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / С.М. Головань, С.Б. Гордієнко, О.С. Петров, В.О. Хорошко, Л.М. Щербак; під ред. В.О. Хорошко. – Луганськ: Ноулідж, 2012. – 480 с.

Список Інтернет-ресурсів:

1. www.wired.com;
2. http://virusov-net.info;
3. www.bezpeka.com

Заплотинський Борис Андрійович

кандидат технічних наук, доцент

Основи інформаційної безпеки

конспект лекцій на 128 стор.

Електронний ресурс кафедри ІАтаІД КІІВіП НУ “ОЮА”