Частина І

Забезпечення захисту інформації в інформаційно-комунікаційних системах

Розділ 1
Базові поняття

- ✦ Термінологія сфери захисту інформації в інформаційно-комунікаційних системах
- ✦ Основні загрози безпеці інформації
- ✦ Класифікація загроз
- ✦ Порушники

1.1. Термінологія

У сфері захисту інформації, як і в будь-якій іншій сфері діяльності, існує специфічна термінологія (професійна і жаргонна), що відображає концептуальні підходи до розв'язання конкретних проблем. Відтак ми розпочнемо саме з неї. У цьому розділі буде розглянуто основні терміни та наведено їх тлумачення.

1.1.1. Системи, в яких здійснюється захист інформації

Останнім часом спеціалісти використовують кілька понять для визначення безпеки інформації в інформаційних системах. Такими поняттями є *захист інформації в комп'ютерних системах*, *захист інформації в комп'ютерних системах і мережах*, *захист інформації в автоматизованих системах*, *захист інформації в інформаційно-телекомунікаційних системах*. Згадані поняття часто використовують як синоніми, але слід зазначити, що в останні роки вони зазнали певної еволюції. Ще кілька років тому більш поширеним було поняття *захист інформації в комп'ютерних системах і мережах*, а в офіційних документах перевагу надавали поняттю *захист інформації в автоматизованих системах*. Зараз загальноприйнятим в Україні є поняття *захист інформації в інформаційно-телекомунікаційних системах*, саме його переважно використовують у законодавчих і нормативних документах [1].

Розгляд термінології доцільно почати з визначення систем, в яких здійснюється захист інформації.

Інформаційно-телекомунікаційна система

Інформаційно-телекомунікаційною системою (ІТС) називають організаційно-технічну систему, яка виконує функції інформаційної системи, тобто такої організаційно-технічної системи, що реалізує певну технологію (або сукупність технологій) оброблення інформації, та (або) телекомунікаційної системи — технічної

системи, що реалізує певну технологію (або сукупність технологій) передавання даних шляхом їх кодування у формі фізичних сигналів.

Назва цього підручника відповідає сучасному терміну «інформаційно-комунікаційна система» (ІКС), який широко використовують у світовій практиці, а також у напряму підготовки фахівців у вищих навчальних закладах України за освітньо-кваліфікаційним рівнем бакалавра 6.170101 — «Безпека інформаційних і комунікаційних систем».

Комп'ютерна система

Термін «комп'ютерна система» (КС) часто використовують як узагальнюючий, його виносять у заголовки статей, книжок і навіть нормативних документів. Але у вітчизняних нормативних документах тлумачення цього терміну досить специфічне. Згідно з НД ТЗІ 1.1-003-99 «Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу» [2], *комп'ютерна система* — це сукупність програмно-апаратних засобів, яку подають на оцінювання. Під оцінюванням тут розуміють експертне оцінювання захищеності інформації в системі, яке є складовою експертизи або сертифікації на відповідність чинним нормативним документам і стандартам. Таке оцінювання ще називають кваліфікаційним аналізом (рос. — квалификационный анализ, англ. — evaluation). Докладніше про специфіку і процедури експертизи та сертифікації йтиметься в розділі 21. Еквівалентом терміну «комп'ютерна система» (у тому значенні, в якому його було тут подано) є: рос. — компьютерная система, объект оценки, англ. — target of evaluation. Термін «комп'ютерна система» у НД ТЗІ вживають до об'єктів оцінювання різних класів як узагальнення термінів «обчислювальна система» та «автоматизована система».

Обчислювальна система

Під *обчислювальною системою* (рос. — вычислительная система, англ. — computer system) розуміють сукупність програмних і апаратних засобів, призначених для оброблення інформації. Обчислювальна система поєднує в собі технічні засоби оброблення і передавання даних (засоби обчислювальної техніки і зв'язку), а також методи і алгоритми оброблення даних, реалізовані у вигляді відповідного програмного забезпечення (ПЗ).

Позаяк в українській мові стандартна абревіатура для обчислювальної системи (ОС) збігається з більш поширеною абревіатурою для операційної системи — найважливішого програмного компонента будь-якої обчислювальної системи (зокрема, в контексті захисту інформації), ми уникатимемо використання цієї абревіатури для обчислювальних систем, вживаючи її до операційних систем, яким присвячено розділи 11–14 цієї книжки.

Автоматизована система

Термін «автоматизована система» (рос. — автоматизированная система, англ. — automated system) вживають до систем автоматизованого оброблення інформації, побудованих на основі обчислювальної техніки. Його використовують не лише

в контексті захисту оброблюваної інформації, але й в численних стандартах, наприклад ГОСТ серії 34 (Інформаційна технологія. Комплекс стандартів на автоматизовані системи) [3–6].

Є різні тлумачення терміну «автоматизована система». Ми дотримуватимемося визначення з НД ТЗІ 1.1-003-99 [2]: *автоматизована система* (АС) — це організаційно-технічна система (рис. 1.1), що реалізує інформаційну технологію і поєднує у собі:

- обчислювальну систему;
- фізичне середовище;
- персонал;
- інформацію, яка обробляється.

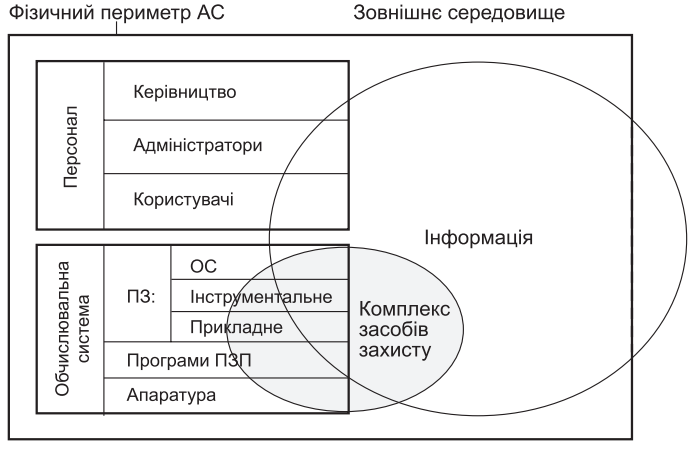

Рис. 1.1. Структура автоматизованої системи

Отже, обчислювальна система, персонал, інформація з технологією її оброблення та фізичне середовище є складовими АС. Також ці компоненти часто називають середовищем функціонування системи.

Надалі в цій книжці ми будемо використовувати термін «комп'ютерна система» в усіх випадках, коли не наводитиметься його звичне тлумачення, тобто як синонім терміну «обчислювальна система», а терміни «інформаційно-комунікаційна система», «інформаційно-телекомунікаційна система» та «інформаційна система» вживатимуться як синоніми терміну «автоматизована система».

1.1.2. Завдання захисту інформації

Далі ми зосередимо увагу на термінах, безпосередньо пов'язаних із питаннями захисту інформації в ІКС, при цьому будемо дотримуватися термінології згідно з НД ТЗІ 1.1-003-99 [2] та ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення» [7]. Перше питання, яке постає, — що саме ми захищаємо, і яка мета цього захисту. Навіть побіжно розглядаючи цю тему, можна переконатися, що захист інформації як такої, без чіткого визначення завдань захисту не має сенсу.

Наведемо приклад неадекватного застосування заходів щодо захисту інформації. Уявіть собі веб-сайт, який містить загальнодоступну інформацію рекламного характеру. Для доступу на цей сайт користувачі мусять проходити попередню процедуру реєстрації з отриманням персонального пароля, який необхідно змінювати щонайменше щотижня. Під час навігації по сайту користувачі отримуватимуть попередження про реєстрацію всіх їхніх дій. Чи буде такий сайт популярним (адже саме це потрібно його власникам)? Усі ці заходи були б цілком прийнятні та навіть необхідні, якби сайт містив, наприклад, конфіденційну корпоративну інформацію.

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, оброблення, зберігання, пошуку та надання користувачам. Ці технології мають ураховувати особливості інформації, які й роблять її цінною, а також давати змогу користувачам різних категорій працювати з інформаційними ресурсами (створювати, знаходити, копіювати, узагальнювати, порівнювати, модифікувати, перетворювати, знищувати тощо).

Передусім слід усвідомлювати, що не реалізація інформаційно-комунікаційної системи дає можливість користувачам різних категорій звертатися до певних інформаційних ресурсів, а зовнішні чинники, до яких насамперед належать Закони України (або іншої держави, відповідно до того правового поля, в якому функціонуватиме система). З усього цього випливає найважливіше для визначення мети захисту інформації поняття — політика безпеки.

Політика безпеки [інформації] (рос. — политика безопасности [информации], англ. — [information] security policy) — це сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок оброблення інформації в ІКС. Таким чином, саме політика безпеки інформації обумовлює вживання тих чи інших заходів захисту, які дають змогу підтримувати безпеку інформації.

Безпека інформації (рос. — безопасность информации, англ. — information security) — це стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації. Багаторічний досвід захисту інформації в ІКС дозволив визначити головні властивості інформації, збереження яких дає змогу гарантувати збереження цінності інформаційних ресурсів. Це конфіденційність, цілісність і доступність інформації.

Конфіденційність (рос. — конфиденциальность, англ. — confidentiality) — властивість інформації, завдяки якій лише вповноважені користувачі мають змогу її отримувати (тобто ознайомлюватися з інформацію).

Цілісність (рос. — целостность, англ. — integrity) — властивість інформації, яка дає можливість лише вповноваженим користувачам її модифікувати.

Доступність (рос. — доступность, англ. — availability) — властивість інформації, завдяки якій уповноважені користувачі можуть використовувати її згідно з правилами, встановленими політикою безпеки, не очікуючи довше заданого (невеликого) проміжку часу. Тобто інформаційний ресурс має необхідний користувачу вигляд, знаходиться в тому місці, де це потрібно користувачу, і тоді, коли це йому потрібно.

Термін *доступність* вживають не лише, коли йдеться про інформаційні ресурси, але й до ІКС у цілому, до її компонентів або окремих ресурсів. Наприклад, коректно говорити про доступність сервера, сегмента мережі, служби електронної пошти тощо.

1.1.3. Загрози і вразливості

Тепер визначимо, що може спричинити порушення безпеки інформації та проти чого, власне, застосовують заходи захисту інформації.

Несприятливий вплив (рос. — неблагоприятное воздействие, англ. — undesired event) — вплив, що призводить до зменшення цінності інформаційних ресурсів.

Загроза (рос. — угроза, англ. — threat) — будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та (або) нанесення збитку ІКС. Тобто загроза — це будь-який потенційно можливий несприятливий вплив.

Атака (рос. — атака, англ. — attack) — це спроба реалізації загрози. Якщо атака є успішною (здійснено подолання засобів захисту), це називають *проникненням* (рос. — проникновение, англ. — penetration). Наслідком успішної атаки є порушення безпеки інформації в системі, яке називають *компрометацією* (рос. — компрометация, англ. — compromise).

Слід звернути увагу на те, що за комплексного підходу до захисту інформації ми маємо розглядати не лише впливи, спрямовані на інформаційні ресурси, але й будь-які впливи, що можуть завдати шкоди ІКС. Ми вже узагальнили це твердженням про необхідність захисту не самої інформації, а насамперед технології її оброблення.

Уразливість системи (рос. — уязвимость системы, англ. — system vulnerability) — нездатність системи протистояти реалізації певної загрози або ж сукупності загроз.

Вади захисту (рос. — изъяны защиты, бреши, англ. — security flaw) — сукупність причин, умов і обставин, наявність яких може призвести до порушення нормального функціонування системи або політики безпеки інформації. Здебільшого під вадами захисту розуміють особливості побудови програмних (а іноді й апаратних) засобів захисту, що за певних обставин спричиняють їхню нездатність протистояти загрозам і виконувати свої функції. Тобто вади захисту є окремим випадком уразливості системи.

У літературі іноді використовують інше тлумачення цих термінів, що, як на наш погляд, не є коректним. Наприклад, часто замість терміну *загроза* вживають термін *атака*. Однак потрібно розрізняти атаку, яка є дією, тобто спробою реалізувати певну загрозу, та загрозу, яка робить потенційно можливим здійснення несприятливого впливу. Атака — це здебільшого цілеспрямований вплив, як правило, умисний. Загрози можуть бути випадковими, хоча втрати від цього не стають меншими. Тому захищати інформацію потрібно також від загроз, а не лише від атак.

Порушник (рос. — нарушитель, англ. — user violator) — фізична особа (необов'язково користувач системи), яка порушує політику безпеки системи. Іноді

використовують термін *зловмисник* (рос. — злоумышленник, англ. — intruder), чим наголошують умисність здійсненого ним порушення, тоді як порушник може здійснювати порушення ненавмисно (наприклад, через необережність або недостатню обізнаність).

Часто вживаний термін *хакер* (рос. — хакер, англ. — hacker) є доволі неоднозначним, тому ми не використовуватимемо його як синонім терміну *порушник*.

Модель [політики] безпеки (рос. — модель [политики] безопасности, англ. — security policy model) — абстрактний формалізований чи неформалізований опис політики безпеки. Модель безпеки використовують під час проектування системи для визначення механізмів і алгоритмів захисту, а також під час аналізу захищеності системи для перевірки й доведення коректності та достатності реалізованих механізмів.

Модель загроз (рос. — модель угроз, англ. — model of threats) — абстрактний формалізований чи неформалізований опис методів і засобів здійснення загроз.

Модель порушника (рос. — модель нарушителя, англ. — user violator model) — абстрактний формалізований чи неформалізований опис порушника. Моделі загроз і порушника є вихідною інформацією для розроблення політики безпеки і проектування будь-яких систем захисту.

Захищена комп'ютерна система (рос. — защищенная компьютерная система, англ. — trusted computer system) — комп'ютерна система, що здатна забезпечувати захист оброблюваної інформації від визначених загроз. Цей термін частіше вживають до обчислювальних систем або їхніх складових (програмних продуктів, окремих програмно-апаратних пристроїв). Іноді його застосовують до ІКС, але слід розуміти, що будь-яка сучасна ІКС має бути захищеною (навіть домашній комп'ютер із одним користувачем). Інакше її використання дуже швидко призведе до втрат інформації.

Спостережність (рос. — наблюдаемость, англ. — accountability) — властивість ІКС, що дає змогу фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів із метою запобігання порушенню політики безпеки і (або) забезпеченню відповідальності за певні дії. Це дуже важлива властивість обчислювальних систем та ІКС, яка досягається реалізацією засобів *реєстрації,* або *аудита* (англ. — audit, auditing).

1.1.4. Комплексна система захисту інформації

Під *захистом інформації в ІКС* (рос. — защита информации в ИКС, англ. – information protection, information security, computer system security) розуміють діяльність, спрямовану на забезпечення безпеки оброблюваної в ІКС інформації й ІКС у цілому, що дає змогу запобігти реалізації загроз або унеможливити її, та зменшити ймовірність завдання збитків від реалізації загроз.

Захист інформації в ІКС полягає у створенні системи технічних (інженерних, програмно-апаратних) і нетехнічних (правових, організаційних) заходів та в підтримці її роботоздатного стану.

Систему таких заходів називають комплексною системою захисту інформації. Відтак *комплексна система захисту інформації* (КСЗІ) (рос. — комплексная система защиты информации) — це сукупність організаційних, інженерних і програмно-апаратних засобів, що забезпечують захист інформації в ІКС.

Отже, захист інформації в ІКС формально зводиться до створення і супроводу КСЗІ. Слід зазначити, що навіть домашній комп'ютер з одним користувачем має якусь КСЗІ, щоправда, недокументовану. Нічого дивного, адже операційна система обов'язково має засоби контролю цілісності компонентів самої ОС і файлової системи. Швидше за все, користувач установив антивірусний засіб і хоча б зрідка оновлює його бази даних (або просто видаляє застарілу програму і встановлює нову). Час від часу він робить резервні копії своїх найцінніших файлів. Зрештою, якщо користувач має вихід в Інтернет, він мусить вживати додаткових заходів безпеки.

Потрібно добре знати про те, що підключення до Інтернету є найкритичнішим із міркувань безпеки системи. Якщо без такого підключення користувач може працювати роками, не застосовуючи специфічних заходів безпеки, то з виходом в Інтернет йому, фактично, необхідно створити КСЗІ. Крім антивірусного ПЗ до складу цієї системи мають входити настроєні певним чином засоби міжмережної фільтрації (наприклад, персональний брандмауер), реєстрації подій, а, можливо, і виявлення вторгнень. Потрібно також періодично вживати заходів, на кшталт оновлення програмного забезпечення, встановлення виправлень, оновлення антивірусних баз тощо.

Що стосується ІКС, які використовують у державних органах і установах, підприємствах різної форми власності, то для них створення КСЗІ є життєво необхідним. У багатьох випадках обов'язковість створення КСЗІ визначається чинним законодавством.

1.1.5. Об'єкти захисту та їхні властивості

До цього ми розглядали систему як ціле, хоча й згадували окремі її складові та ресурси. Далі ми розглядатимемо окремі підсистеми і об'єкти системи, а також їх взаємодію.

Комплекс засобів захисту (КЗЗ) (рос. — комплекс средств защиты, англ. — trusted computing base) — сукупність програмно-апаратних засобів, що забезпечують реалізацію політики безпеки інформації. Тобто КЗЗ є складовою обчислювальної системи (див. рис. 1.1). КЗЗ може бути локалізованим у системі у вигляді одного чи кількох апаратних і програмних компонентів, а може бути розпорошеним по різноманітних програмних засобах. Безперечно, перший варіант має суттєві переваги, проте другий — також іноді використовують у достатньо надійних, перевірених часом рішеннях (наприклад, саме такий вигляд має архітектура КЗЗ ОС UNIX).

Об'єкт системи — це елемент ресурсів обчислювальної системи, який знаходиться під керуванням КЗЗ і характеризується визначеними атрибутами й поводженням.

Розрізняють такі види об'єктів:

- пасивні об'єкти;
- об'єкти-користувачі;
- об'єкти-процеси.

Об'єкти-користувачі й об'єкти-процеси є активними об'єктами. Активні об'єкти можуть виконувати дії над пасивними об'єктами.

У більшості зарубіжних стандартів, зокрема й у сучасному міжнародному стандарті ISO 15408 [8–10], пасивні об'єкти називають *об'єктами* (рос. — объект, англ. — object), а активні об'єкти — *суб'єктами* (рос. — субъект, англ. — subject). Потрібно розуміти, що, як правило, суб'єкт — це об'єкт-процес, який діє від імені певного об'єкта-користувача.

Об'єкт-користувач (рос. — объект-пользователь, англ. — user object) — це подання фізичного користувача в обчислювальній системі, яке утворюється під час його входження в систему і характеризується своїм контекстом (обліковий запис, псевдонім, ідентифікаційний код, повноваження тощо).

Об'єкт-процес (рос. — объект-процесс, англ. — process object) — задача, процес, потік, що виконується в поточний момент (абстракція програми, що виконується) і повністю характеризується своїм контекстом (стан регістрів, адресний простір, повноваження тощо).

З міркувань безпеки інформації в ІКС виняткове значення має спроможність об'єктів взаємодіяти. Для цього використовують поняття доступу.

Доступ (рос. — доступ, англ. — access) — це взаємодія двох об'єктів обчислювальної системи, коли один із них (той, що здійснює доступ) виконує дії над іншим (тим, до якого здійснюється доступ). Результатом такого доступу є змінення стану системи (наприклад, запуск програми на виконання) і (або) утворення інформаційного потоку від одного об'єкта до іншого (наприклад, читання або записування інформації). У випадку, коли утворюється інформаційний потік, кажуть, що здійснюється *доступ до інформації*. Для забезпечення захисту інформації доступ до об'єктів, які містять інформацію, що підлягає захисту, слід здійснювати з дотриманням визначених правил.

Правила розмежування доступу (ПРД) (рос. — правила разграничения доступа, англ. — access mediation rules) — складова політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об'єктів.

Несанкціонований доступ (НСД) (рос. — несанкционированный доступ, англ. — unauthorized access) — доступ, який здійснюють з порушенням політики безпеки, тобто з порушенням ПРД. Цей термін є найбільш уживаним, переважно до систем, в яких обробляють таємну інформацію, тому його винесено в назви деяких нормативних документів системи технічного захисту інформації (НД ТЗІ) [2, 11–13]. Разом із тим навіть у цих документах зазначено, що захист інформації не обмежується захистом від НСД.

Щоб можна було реалізувати розмежування доступу, система має розпізнавати об'єкти.

Ідентифікація (рос. — идентификация, англ. — identification) — процес розпізнавання об'єктів системи за їхніми мітками, або ідентифікаторами.

Ідентифікатор (рос. — идентификатор, англ. — identifier) — це унікальний атрибут об'єкта, який дає змогу вирізнити об'єкт з-поміж інших. Ідентифікацією називають процедуру присвоєння ідентифікаторів об'єктам. Стосовно ідентифікації користувачів системи процедура може полягати у введенні унікального ідентифікатора користувача, наприклад його кодового імені. Є також застаріле визначення ідентифікатора як послідовності латинських літер і цифр, яка починається з літери.

Автентифікація (рос. — аутентификация, англ. — authentication) — перевірка запропонованого ідентифікатора на відповідність об'єкту, пересвідчення в його справжності. Стосовно автентифікації користувачів системи процедура передбачає введення додаткової інформації, яка дає змогу системі пересвідчитися, що користувач справді є тим, за кого себе видає. Наприклад, у найпростішому і найпоширенішому випадку це введення таємного кодового слова — пароля. Вважається, що якщо користувач знає пароль, то він справді той, за кого себе видає.

Авторизація (рос. — авторизация, англ. — authorization) — це процедура надання користувачу визначених повноважень у системі. У захищених системах авторизації користувача обов'язково передують його ідентифікація й автентифікація. Наприклад, в операційних системах авторизація полягає у створенні програмного середовища, яке дає змогу користувачу виконувати дозволені йому функції, зокрема запускати в системі процеси від свого імені. Іноді ідентифікацію і автентифікацію розглядають як складові процесу авторизації. Також для повідомлення (пасивного об'єкта) авторизацією називають процедуру визначення його джерела (користувача або процесу, тобто активного об'єкта).

Відмова від авторства (рос. — отказ от авторства, англ. — repudiation of origin) — це заперечення причетності до створення або передавання якого-небудь документа чи повідомлення.

Відмова від одержання (рос. — отказ от получения, англ. — repudiation of receipt) — це заперечення причетності до отримання якого-небудь документа чи повідомлення.

1.1.6. Розроблення й оцінювання захищених систем

Зупинимося на деяких термінах, які найчастіше вживають під час оцінювання захищених систем.

Кваліфікаційний аналіз (рос. — квалификационный анализ, англ. — evaluation) — це аналіз ІКС (чи обчислювальної системи) з метою визначення рівня її захищеності та відповідності вимогам безпеки на основі критеріїв стандарту безпеки.

Гарантії (рос. — гарантии, англ. — assurance) — міра впевненості в тому, що ІКС коректно реалізує політику безпеки.

У перекладах зарубіжних стандартів російською мовою замість терміну «гарантії» зазвичай вживають термін «адекватність».

Адекватність (рос. — адекватность, англ. — assurance) — це показник реально гарантованого рівня безпеки, що відображає ступінь ефективності та надійності реалізованих засобів захисту та їхніх відповідностей поставленим задачам.

1.2. Загрози безпеці інформації

1.2.1. Класифікація загроз

До можливих загроз безпеці інформації належать:

- стихійні лиха й аварії;
- збої та відмови устаткування;
- наслідки помилок проектування і розроблення компонентів АС;
- помилки персоналу під час експлуатації;
- навмисні дії зловмисників і порушників.

Для побудови моделі загроз використовують різні класифікації загроз безпеці інформації [14–18]. Наведемо узагальнюючу класифікацію загроз (табл. 1.1).

Таблиця 1.1. Класифікація загроз

Ознака класифікації загроз	Причини, спрямованість, характеристики загроз
Природа виникнення	Природні загрози (загрози, які виникають через впливи на АС та її компоненти об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від людини). Штучні загрози (загрози, викликані діяльністю людини)
Принцип НСД	Фізичний доступ: ✦ подолання рубежів територіального захисту і доступ до незахищених інформаційних ресурсів; ✦ розкрадання документів і носіїв інформації; ✦ візуальне перехоплення інформації, виведеної на екрани моніторів і принтери; ✦ підслуховування; ✦ перехоплення електромагнітних випромінювань. Логічний доступ (доступ із використанням засобів комп'ютерної системи)
Мета НСД	Порушення конфіденційності (розкриття інформації). Порушення цілісності (повне або часткове знищення інформації, її спотворення, фальсифікація, викривлення). Порушення доступності (наслідок — відмова в обслуговуванні)
Причини появи вразливостей різних типів	Недоліки політики безпеки. Помилки адміністративного керування. Недоліки алгоритмів захисту. Помилки реалізації алгоритмів захисту
Об'єкт безпосередньої атаки	Політика безпеки АС. Компоненти системи захисту АС. Протоколи взаємодії. Функціональні компоненти АС
Стан кінцевого об'єкта атаки	Зберігання (об'єкт знаходиться на зовнішніх носіях). Оброблення (об'єкт знаходиться в оперативній пам'яті). Передавання (об'єкт просувається через лінію зв'язку)

Таблиця 1.1 (*закінчення*)

Ознака класифікації загроз	Причини, спрямованість, характеристики загроз
Спосіб впливу на об'єкт атаки	Безпосередній вплив. Вплив на систему дозволу «Маскарад». Використання наосліп
Спрямованість НСД	Безпосереднє стандартне використання: ✦ слабкостей політики безпеки; ✦ недоліків адміністративного керування. Приховане нестандартне використання: ✦ недокументованих особливостей системи; ✦ прихованих каналів
Характер впливу	Активний (внесення змін в АС). Пасивний (спостереження)
Режим НСД	За постійної участі людини (в інтерактивному режимі) можливе застосування стандартного ПЗ. Без особистої участі людини (у пакетному режимі) найчастіше для цього застосовують спеціалізоване ПЗ
Умова початку здійснення впливу	У відповідь на запит від об'єкта, який атакують. Після визначеної події на об'єкті. Безумовна атака
Місцезнаходження джерела НСД	Внутрішньосегментне (джерело знаходиться в локальній мережі). У цьому випадку, як правило, ініціатор атаки — санкціонований користувач. Міжсегментне: ✦ несанкціоноване вторгнення з відкритої мережі в закриту; ✦ порушення обмежень доступу з одного сегмента закритої мережі в інший
Наявність зворотного зв'язку	Зі зворотним зв'язком (атакуючий отримує відповідь системи на його вплив) Без зворотного зв'язку (атакуючий не отримує відповіді)
Рівень моделі взаємодії відкритих систем (Open Systems Interconnection, OSI)	Вплив може бути здійснено на таких рівнях: фізичному, канальному, мережному, транспортному, сеансовому, представницькому, прикладному

Таку класифікацію використовують, наприклад, коли потрібно детально проаналізувати загрози, спричинені типовими атаками [15]. Для побудови моделі загроз вона надто громіздка і непрактична. Частіше з цієї класифікації беруть лише перші три характеристики.

1.2.2. Перелік типових загроз безпеці

Розглянемо зручнішу класифікацію, що виглядає, як перелік найтиповіших загроз безпеці. На жаль, це не повний перелік загроз.

1. Природні загрози.
2. Штучні загрози.

2.1. Ненавмисні загрози.
- 2.1.1. Ненавмисні дії, що призводять до відмови системи.
- 2.1.2. Неправомірне відключення устаткування чи зміна режимів роботи пристроїв і програм.
- 2.1.3. Ненавмисне псування носіїв інформації.
- 2.1.4. Запуск технологічних програм, здатних за некомпетентного використання викликати втрату роботоздатності системи чи незворотні зміни в ній.
- 2.1.5. Нелегальне впровадження і використання неврахованих програм.
- 2.1.6. Ненавмисне зараження вірусом.
- 2.1.7. Необережні дії, що призводять до розголошення конфіденційної інформації.
- 2.1.8. Розголошення, втрата атрибутів розмежування доступу.
- 2.1.9. Проектування архітектури системи з можливостями, що становлять небезпеку для самої системи.
- 2.1.10. Ігнорування організаційних обмежень.
- 2.1.11. Входження у систему в обхід засобів захисту.
- 2.1.12. Некомпетентне використання, настроювання і неправомірне відключення засобів захисту.
- 2.1.13. Пересилання даних за адресою абонента, яка є хибною.
- 2.1.14. Введення помилкових даних.
- 2.1.15. Ненавмисне ушкодження каналів зв'язку.

2.2. Навмисні загрози.
- 2.2.1. Фізичне руйнування системи.
- 2.2.2. Вимкнення чи виведення з ладу підсистем забезпечення функціонування.
- 2.2.3. Дії з дезорганізації функціонування системи.
- 2.2.4. Вторгнення агентів у оточення персоналу системи.
- 2.2.5. Вербування персоналу чи окремих користувачів, що мають визначені повноваження.
- 2.2.6. Застосування пристроїв, що підслуховують, дистанційних фото- та відеозйомок.
- 2.2.7. Перехоплення побічних електромагнітних, акустичних та інших випромінювань і наведень від пристроїв і каналів зв'язку.
- 2.2.8. Перехоплення даних, переданих по каналах зв'язку.
- 2.2.9. Розкрадання носіїв інформації.
- 2.2.10. Несанкціоноване копіювання носіїв інформації.
- 2.2.11. Розкрадання і вивчення виробничих відходів.
- 2.2.12. Зчитування залишкової інформації з оперативної пам'яті та зовнішніх запам'ятовуючих пристроїв.

2.2.13. Незаконне заволодіння паролями.

2.2.14. Несанкціоноване використання терміналів користувачів.

2.2.15. Розкриття шифрів криптографічно захищеної інформації.

2.2.16. Впровадження програмно-апаратних закладок і вірусів.

2.2.17. Незаконне підключення до ліній зв'язку з метою роботи «між рядків».

2.2.18. Незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача шляхом його повного відключення.

1.2.3. Класифікація атак

Наведемо спрощену класифікацію, яка відображає найбільш типові атаки на розподілені автоматизовані системи [18]. Цю класифікацію було запропоновано Пітером Меллом (Peter Mell) [19].

- *Віддалене проникнення* (рос. — удаленное проникновение, англ. — remote penetration). Атаки, які дають змогу реалізувати віддалене керування комп'ютером через мережу. Приклади програм, що реалізують цей тип атак: NetBus, BackOrifice.
- *Локальне проникнення* (рос. — локальное проникновение, англ. — local penetration). Атаки, що призводять до отримання несанкціонованого доступу до вузлів, на яких вони ініційовані. Приклад програми, що реалізує цей тип атак: GetAdmin.
- *Віддалена відмова в обслуговуванні* (рос. — удаленный отказ в обслуживании, англ. — remote denial of service). Атаки, що дають можливість порушити функціонування системи або перенавантажити комп'ютер через мережу (зокрема, через Інтернет). Приклади атак цього типу: Teardrop, trin00.
- *Локальна відмова в обслуговуванні* (рос. — локальный отказ в обслуживании, англ. — local denial of service). Атаки, що дають змогу порушити функціонування системи або перенавантажити комп'ютер, на якому їх ініційовано. Приклади атак цього типу: аплет, який перенавантажує процесор (наприклад, відкривши багато вікон великого розміру), що унеможливлює оброблення запитів інших програм.
- *Сканування мережі* (рос. — сканирование сети, англ. — network scanning). Аналіз топології мережі та активних сервісів, доступних для атаки. Атака може бути здійснена за допомогою службового програмного забезпечення, наприклад за допомогою утиліти nmap.
- *Використання сканерів уразливостей* (рос. — использование сканеров уязвимостей, англ. — vulnerability scanning). Сканери вразливостей призначені для пошуку вразливостей на локальному або віддаленому комп'ютері. Такі сканери системні адміністратори застосовують як діагностичні інструменти, але їх також можна використовувати для розвідки та здійснення атаки. Найвідоміші з таких програмних засобів: SATAN, SystemScanner, Xspider, nessus.

- *Злам паролів* (рос. — взлом паролей, англ. — password cracking). Для цього використовують програмні засоби, що добирають паролі користувачів. Залежно від надійності системи зберігання паролів, застосовують методи зламу або підбору пароля за словником. Приклади програмних засобів: L0phtCrack для Windows і Crack для UNIX.
- *Пасивне прослуховування мережі* (рос. — пассивное прослушивание сети, англ. — sniffing). Пасивна атака, спрямована на розкриття конфіденційних даних, зокрема ідентифікаторів і паролів доступу. Приклади засобів: tcpdump, Microsoft Network Monitor, NetXRay, LanExplorer.

Перші чотири класи атак розрізняють переважно за кінцевим результатом (або метою реалізації), а решта — за способом їх здійснення.

1.2.4. Методика класифікації загроз STRIDE

Методика STRIDE розроблена, обґрунтована та активно пропагується фахівцями з корпорації Майкрософт [20]. Фактично, це ще один варіант класифікації загроз за їхніми наслідками. Методику використовують для побудови моделі загроз під час розроблення ПЗ. Назву методики утворено з перших літер назв категорій загроз.

- *Підміна об'єктів* (рос. — подмена объектов, англ. — spoofing identity). Крім згаданих вище загроз, які виникають через недоліки мережних протоколів, до цього класу належить також загроза, викликана підміною особи користувача. Її здійснюють, скориставшись слабкістю системи автентифікації або здобувши автентифікаційні дані шляхом крадіжки чи шахрайства (так звана соціальна інженерія — докладніше в [15]).
- *Модифікація даних* (рос. — модификация данных, англ. — tampering with data). До цього класу належать загрози впливів (атак), мета яких — навмисне псування даних. Атаки можуть бути спрямовані на інформаційні об'єкти, що перебувають у стані зберігання (файли, бази даних), і такі, що передаються мережею.
- *Відмова від авторства* (рос. — отказ от авторства, англ. — repudiation of origin). Загрози цього класу дають змогу порушнику відмовитися від здійснених ним дій (або бездіяльності). Причиною існування такої загрози є відсутність або слабкість механізмів реєстрації подій і слабкі механізми автентифікації.
- *Розголошення інформації* (рос. — разглашение информации, англ. — information disclosure). Загрози цього класу не потребують коментарів.
- *Відмова в обслуговуванні* (рос. — отказ в обслуживании, англ. — denial of service). Ми вже обговорювали загрози цього класу. Атаки, що спричиняють відмову в обслуговуванні, порівняно легко здійснити в розподілених системах і дуже важко їм протидіяти. Особливо небезпечними є атаки *розподіленої відмови в обслуговуванні* (рос. — распределенный отказ в обслуживании, англ. — distributed denial of service), які здійснюють на один об'єкт одразу з кількох вузлів мережі.

- *Підвищення привілеїв* (рос. — повышение привилегий, англ. — elevation of privilege). До цього класу належать загрози, які дають можливість порушнику підвищити свої привілеї у системі. Наприклад, звичайний користувач отримує повноваження адміністратора, або порушник, що підключився без автентифікації до будь-якого мережного сервісу, виконує дії як авторизований користувач.

1.2.5. Модель загроз

Проаналізувавши наявні загрози, можна створити модель загроз — їх абстрактний структурований опис. У Додатку до НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» [21] (цей документ буде розглянуто у розділах 20, 22) рекомендовано таку структуру опису загрози.

- Властивості інформації або АС, на порушення яких спрямована загроза:
  - конфіденційність;
  - цілісність;
  - доступність інформації;
  - спостережність та керованість АС.
- Джерела виникнення загрози:
  - суб'єкти АС;
  - суб'єкти, зовнішні відносно АС (див. далі модель порушника).
- Способи реалізації загрози:
  - технічними каналами, до яких належать канали побічного електромагнітного випромінювання і наведень, а також акустичні, оптичні, радіотехнічні, хімічні та інші канали;
  - каналами спеціального впливу шляхом формування полів і сигналів із метою руйнування системи захисту або порушення цілісності інформації;
  - шляхом несанкціонованого доступу через підключення до засобів та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування програмно-апаратних закладок і впровадження комп'ютерних вірусів.

Загрози, реалізовані першими двома способами, — це загрози фізичного рівня, а останнім — логічного.

1.3. Порушники

1.3.1. Визначення терміну «хакер»

Про хакерів розповідають не лише в засобах масової інформації та Інтернеті, але й в літературі з питань захисту інформації. За своїм історичним походженням і дотепер термін «хакер» застосовують до тих, хто добре розуміється на принципах роботи обчислювальних систем, особливо ПЗ. Ці знання дають їм змогу ви-

являти вразливості систем. Тобто *хакер* — це той, хто знаходить уразливості системи і знає, як ними можна скористатися.

Є різні думки щодо застосування терміну «хакер». Деякі фахівці в галузі захисту інформації [15] вважають, що справжні хакери — це ті, хто діє виключно в інтересах безпеки інформації. Про виявлені вразливості ці хакери повідомляють лише тих, хто у змозі виправити помилки ПЗ, які й спричинили наявність уразливості. Такі хакери можуть тісно співпрацювати з розробниками ПЗ та експертами з комп'ютерної безпеки.

Однак є люди, які мають кваліфікацію хакерів, але використовують свої знання та вміння або задля власної користі, або взагалі з метою вандалізму. Згадані вище фахівці вважають, що називати таких зловмисників хакерами некоректно. До них пропонують застосовувати інші терміни, наприклад, *кракер* (англ. — cracker), що іноді перекладають як зломщик (рос. — взломщик). Але у масовій свідомості, яку формує аж ніяк не спеціальна література, а здебільшого кіно і телебачення, саме зі словом «хакер» пов'язані всі комп'ютерні зловмисники. До речі, значна частина зловмисників (у наш час таких переважна більшість) не мають високої кваліфікації. Для здійснення атаки достатньо знайти необхідний інструментарій та інструкції з його використання. Усе це легко можна знайти в Інтернеті.

Надалі ми не вдаватимемося до дискусій щодо хакерів і кракерів. Ми будемо вживати терміни «порушник» і «зловмисник» у тих значеннях, які було наведено в підрозділі «Термінологія», а термін «хакер» вживатимемо до тих, хто знайшов уразливість і використав її на власний розсуд або здатний це зробити.

1.3.2. Наслідки від дій порушників

На запитання: «Хто або що є джерелом найбільшої небезпеки в інформаційній системі?» різні категорії респондентів дають зовсім різні, а часом протилежні відповіді. Людина, яка цікавиться питаннями безпеки інформації в комп'ютерних системах, але професійно з цією сферою не пов'язана, швидше за все, відповість, що це хакери або віруси. Можливо, в деяких окремих випадках так воно і є. Але переважна більшість системних адміністраторів, тобто тих фахівців, які повсякденно підтримують нормальне функціонування системи, скажуть, що це користувачі.

Потенційні можливості легального користувача в ІКС набагато більші, ніж у будь-якого зовнішнього порушника. Користувач має в системі певні повноваження. Він володіє інформацією про систему, а іншу інформацію може порівняно легко отримати (когось спитати, дещо підслухати, з кимось «неформально» поспілкуватися, десь підібрати якісь записи — йому це легше зробити, ніж будь-якій сторонній особі). Користувач, як правило, не задоволений обмеженнями своїх прав у системі. Він цікавиться новими інформаційними технологіями і намагається перевірити все на практиці. Насправді ж користувач, який не має достатньої кваліфікації, діє за принципом спроб і помилок.

Серед користувачів є специфічна категорія — керівництво. Звичайно керівники вимагають собі підвищені привілеї в системі, а також не визнають щодо себе жодних обмежень. До того ж адміністратори системи формально підпорядковані керівництву, а не навпаки.

Легальні користувачі — найбільша проблема для адміністраторів, позаяк саме вони постійно створюють реальні загрози безпеці інформації. Та зрештою, не користувачі існують для того, щоб заважати адміністраторам, а адміністратори — для того, щоб обслуговувати користувачів. Єдиним виходом із цієї ситуації є взаємоповага і співпраця між ними. Проте на це не варто сподіватися без відповідного документування прав і обов'язків користувачів усіх категорій і адміністраторів. Особливості поведінки користувачів (зокрема, керівників) слід враховувати ще на етапі проектування КСЗІ в ІКС під час створення моделі порушника.

1.3.3. Модель порушника

Модель порушника — це всебічна структурована характеристика порушника, яку разом із моделлю загроз використовують під час розроблення політики безпеки інформації. Рекомендовано таку структуру моделі порушника [21].

- Категорії порушників:
  - внутрішні порушники;
  - користувачі;
  - інженерний склад;
  - співробітники відділів, що супроводжують ПЗ;
  - технічний персонал, який обслуговує будинок;
  - співробітники служби безпеки;
  - керівники;
  - зовнішні порушники.
- Мета порушника:
  - отримання необхідної інформації;
  - отримання можливості вносити зміни в інформаційні потоки відповідно до своїх намірів;
  - завдання збитків шляхом знищення матеріальних та інформаційних цінностей.
- Повноваження порушника в АС:
  - запуск фіксованого набору задач (програм);
  - створення і запуск власних програмних засобів;
  - керування функціонуванням і внесення змін у конфігурацію системи;
  - підключення чи змінення конфігурації апаратних засобів.
- Технічна оснащеність порушника:
  - апаратні засоби;
  - програмні засоби;
  - спеціальні засоби.
- Кваліфікація порушника:
  - під час проведення аналізу загроз завжди вважають, що порушник має високу кваліфікацію.

Висновки

1. Захисту інформації в ІКС властива специфічна термінологія, професійна та жаргонна. Термінологія відображає концептуальні підходи до вирішення проблеми. В Україні термінологію у цій сфері регламентує державний стандарт ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення» [7] і нормативний документ системи технічного захисту інформації (НД ТЗІ) 1.1-003-99 «Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу» [2].
2. До можливих загроз безпеці інформації належать:
   - стихійні лиха й аварії;
   - збої та відмови устаткування;
   - наслідки, спричинені помилками у проектуванні та розробленні компонентів АС;
   - помилки персоналу під час експлуатації;
   - навмисні дії зловмисників і порушників.
3. Для виявлення та аналізу можливих загроз безпеці інформації, а також для розроблення засобів протидії використовують різні класифікації загроз. Класифікації, які застосовують під час створення теоретичних моделей і проведення аналізу загроз, будують за численними ознаками загроз. Більш зручні класифікації мають вигляд переліку найтиповіших загроз безпеці. Деякі класифікації залучають порівняно невелику кількість ознак загроз (5–8). Такі класифікації використовують компанії-розробники програмного забезпечення. До них належить, наприклад, методика STRIDE, що розроблена, обґрунтована й активно пропагується фахівцями з корпорації Майкрософт.
4. Модель загроз — це абстрактний структурований опис загроз, притаманних певній системі. Рекомендовано таку структуру опису загрози:
   - властивості інформації або АС, на порушення яких спрямована загроза;
   - джерела виникнення загрози;
   - можливі способи здійснення загрози.
5. Порушники в комп'ютерних системах можуть бути зовнішніми (тобто такими, що не мають або не можуть мати повноважень у системі) і внутрішніми (користувачі, обслуговуючий персонал ІКС, технічний персонал, який обслуговує будинок, співробітники служби безпеки, керівники). Порушників розрізняють за рівнем їх повноважень у системі, технічною оснащеністю, кваліфікацією.
6. Модель порушника — це всебічна структурована характеристика порушника, яку разом із моделлю загроз використовують під час створення політики безпеки інформації. Рекомендовано таку структуру опису порушника:
   - категорія осіб, до якої може належати порушник;
   - мета порушника;
   - повноваження порушника в системі;
   - технічна оснащеність порушника;
   - кваліфікація порушника.

Контрольні запитання та завдання

1. Поясніть різницю між термінами «обчислювальна система», «комп'ютерна система», «автоматизована система», «інформаційно-комунікаційна система».
2. Як би ви назвали процес, коли вахтер порівнює ваше обличчя з фотографією у перепустці, — ідентифікацією чи автентифікацією?
3. На порушення яких властивостей інформації та системи спрямована загроза прослуховування трафіку?
4. Назвіть загрози, які розглядаються в моделі STRIDE.
5. Які з наявних способів реалізації загрози розглядаються в моделі загроз?
6. Хто, на вашу думку, є більш небезпечним порушником для корпоративної інформаційної системи — хакер, який має великий досвід і потужний комп'ютер, але не має жодних прав доступу до системи, чи користувач, який працює в компанії та має доступ до ресурсів системи, але права якого в системі обмежені? Обґрунтуйте свою відповідь.