В.А. Лужецький, Л.І. Северин, Ю.П. Гульчак,
А.Д. Кожухівський

О С Н О В И
ОРГАНІЗАЦІЙНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Міністерство освіти і науки України
Вінницький національний технічний університет

В. А. Лужецький, Л. І. Северин, Ю. П. Гульчак,
А.Д. Кожухівський

О с н о в и
організаційного захисту
інформації

Затверджено Вченою радою Вінницького національного технічного університету як навчальний посібник для студентів напряму підготовки 1601 – "Інформаційна безпека". Протокол № 7 від 24 лютого 2005р.

Вінниця ВНТУ 2005

УДК 681.3.067
Л 83

Р е ц е н з е н т и :

О.Д. Азаров, доктор технічних наук, професор
А.М. Пєтух, доктор технічних наук, професор
О.Ф. Мельничук, кандидат технічних наук, доцент

Рекомендовано до видання Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України

Лужецький В.А., Северин Л.І., Гульчак Ю.П., А.Д. Кожухівський
Л 83 Основи організаційного захисту інформації. Навчальний посібник. - Вінниця: ВНТУ, 2005. - 148 с.

У посібнику розглянуто організаційні, організаційно-правові і організаційно-технічні заходи, які грають значну роль у створенні надійного механізму захисту інформації, оскільки можливості несанкціонованого використання конфіденційних відомостей значною мірою обумовлюються не технічними аспектами, а зловмисними діями, необережністю і халатністю користувачів або персоналу захисту.

Посібник розрахований на студентів закладів освіти, що спеціалізуються за фахом "Інформаційна безпека. Захист інформації в комп'ютерних системах і мережах." Може бути корисним для працівників підприємств, організацій та громадян, які користуються комп'ютерною технікою.

УДК 681.3.067

Зміст

Передмова

Останнім часом в Україні відбуваються якісні зміни у процесах управління на всіх рівнях, які зумовлені інтенсивним впровадженням новітніх інформаційних технологій (НІТ). Виконання службових завдань, прийняття управлінських рішень зараз ґрунтується на індустрії НІТ, яка має сприймати колосальні інформаційні потоки, грамотно зберігати їх, забезпечувати швидкий і безпечний доступ до даних, реалізовувати їх обмін усіма наявними каналами та обробляти відповідно до певних алгоритмів і надавати споживачам.

Швидке вдосконалення інформатизації, проникнення її в усі сфери життєво важливих інтересів зумовило, крім безперечних переваг, і появу низки стратегічних проблем. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем, саме тому в Україні все більше уваги приділяється проблемам захисту інформації.

Для вирішення задачі забезпечення безпеки в інформаційних систем необхідно:

- захистити інформацію при її зберіганні, обробці та передачі мережами системи;
- підтвердити істинність об'єктів даних і користувачів (автентифікація сторін, що встановлюють зв'язок);
- виявити і запобігти порушенню цілісності об'єктів даних;
- захистити технічні пристрої та приміщення;
- захистити конфіденційну інформацію від витоку та впроваджених електронних пристроїв зняття інформації;
- захистити програмні продукти від впровадження програмних закладок і вірусів;
- захистити від несанкціонованого доступу до інформаційних ресурсів і технічних засобів мережі, в тому числі і до засобів управління, щоб запобігти зниженню рівня захищеності інформації та самої мережі в цілому;
- організувати необхідні заходи, направлені на забезпечення цілісності конфіденційних даних.

Ефективна реалізація загальних принципів забезпечення інформаційної безпеки можлива тільки при наявності процесу захисту інформаційних ресурсів. Причому в цьому мають брати участь професійні фахівці, адміністрація, співробітники і користувачі, що і визначає підвищену значимість організаційної сторони питання.

Організаційні заходи відіграють значну роль у створенні надійного механізму захисту інформації, оскільки можливості несанкціонованого використання конфіденційних відомостей значною мірою обумовлюються не технічними аспектами, а зловмисними діями, необережністю і халатністю користувачів або персоналу захисту.

Впливу цих аспектів практично неможливо уникнути за допомогою технічних засобів. Для цього потрібна сукупність організаційно-правових і організаційно-технічних заходів, які б виключали або зводили до мінімуму можливість виникнення небезпеки щодо конфіденційної інформації.

Організаційний захист забезпечує:

- організацію режиму й охорони;
- організацію роботи із співробітниками (підбір, розстановка і навчання персоналу);
- організацію роботи з документацією та документованою інформацією;
- організацію використання технічних засобів збирання, оброблення, зберігання та передавання конфіденційної інформації;
- організацію роботи з аналізу внутрішніх і зовнішніх загроз конфіденційній інформації та розробки заходів щодо забезпечення її захисту;
- організацію ефективного контролю за функціонуванням системи інформаційної безпеки.

Очевидно, що організаційні заходи повинні чітко плануватися, спрямовуватися і здійснюватися певною організаційною структурою (структурним підрозділом), спеціально створюваною для таких цілей і укомплектованою відповідними фахівцями з безпеки підприємницької діяльності та захисту інформації. Часто таким структурним підрозділом є служба безпеки підприємства (фірми , установи).

Ретельний розгляд усіх перерахованих аспектів організаційного захисту інформації і є основною задачею навчального посібника.

Автори висловлюють подяку доктору технічних наук, професору Азарову О. Д., доктору технічних наук, професору Пєтуху А. М., кандидату технічних наук, доценту Кузьмічову О. І. за цінні зауваження і рекомендації та студентам Каменєвій Т., Шевчуку О. і Давидюку В. за надання допомоги у підготовці посібника до видання.

Глава 1. СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1. Основні поняття та уявлення

Проблема безпеки інформації в період загальної інформатизації, широкого впровадження новітніх технологій – одне з найгостріших питань сьогодення. Напевне, необхідність у захисті інформації з'явилась одночасно з самою інформацією. Можливі методи захисту інформації майже завжди визначалися формою її подання та передбачуваними способами використання.

Умовно виділяють **три періоди розвитку систем захисту інформації**:

перший – відноситься до того часу, коли опрацювання інформації здійснювалося за традиційними (ручними, паперовими) технологіями;

другий – коли для опрацювання інформації на регулярній основі застосовувалися засоби електронно-обчислювальної техніки перших поколінь;

третій – коли використання інформаційної техніки прийняло масовий характер.

Перед початком розгляду питань захисту інформації доцільно більш-менш формально визначити, що ховається за термінами "інформаційна безпека" і "захист інформації". Перш за все, обидва ці словосполучення є перекладом на українську мову англійського терміну "information security". Словосполучення "інформаційна безпека" має скоріше наукове, теоретичне поняття, а "захист інформації" звичайно використовується при описанні практичних заходів. Проте у цілому вони є синонімами і в подальшому між ними не буде робитися якої-небудь різниці.

На формування поняття захисту інформації впливає велика кількість різнопланових факторів, основними з яких є:

- вплив інформації на ефективність прийнятих рішень;
- концепція побудови і використання захищених інформаційних систем;
- технічне оснащення інформаційних систем;
- характеристики інформаційних систем і їх компонентів з точки зору загроз збереження інформації;
- потенційні можливості зовнішньої дії на інформацію, її отримання та використання;
- наявність методів та засобів захисту інформації.

Розвиток підходів до захисту інформації проходить під дією перелічених факторів.

Генеральним напрямком пошуку шляхів захисту інформації є неухильне підвищення системності підходу до самої проблеми захисту інформації. Поняття системності інтерпретується перш за все в тому розумінні, що захист інформації полягає не тільки у створенні відповідних

механізмів, а є регулярним процесом, здійснюваним на всіх етапах життєвого циклу систем опрацювання даних при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи і заходи, що використовуються для захисту інформації неодмінно і найбільш раціонально об'єднуються в єдиний цілісний механізм – систему захисту, яка повинна забезпечувати, кажучи мовою військових, глибокоешеловану оборону, причому не тільки від зловмисників, але й від некомпетентних чи недостатньо підготовлених користувачів і персоналу.

В цій системі повинно бути не менше *чотирьох захисних поясів:*

- *зовнішній,* що охоплює всю територію, на якій розміщені споруди;
- *пояс споруд*, приміщень чи пристроїв системи;
- *пояс компонентів системи* (технічних засобів, програмного забезпечення, елементів баз даних);
- *пояс технічних процесів опрацювання даних* (введення, виведення, внутрішнє оброблення тощо).

Основні правила, якими рекомендовано керуватися при організації робіт з захисту інформації, зводяться до таких.

1. Забезпечення безпеки інформації – це безперервний процес, що заключається в систематичному контролі захищеності, виявленні вузьких місць в системі захисту, обґрунтуванні і реалізації більш раціональних шляхів удосконалення і розвитку системи захисту.
2. Безпека інформації в системі опрацювання даних може бути забезпечена тільки при комплексному використанні всього арсеналу наявних засобів захисту.
3. Ніяка система захисту не забезпечить безпеку інформації без належної підготовки користувачів і дотримання ними всіх правил захисту.
4. Ніяку систему захисту не можна вважати абсолютно надійною. Слід виходити з того, що може знайтися такий умілий зловмисник, який знайде лазівку для доступу до інформації.

Основні труднощі реалізації систем захисту полягають в тому, що вони повинні задовольняти двом групам суперечних вимог. З однієї сторони, повинен бути забезпечений надійний захист наявної в системі інформації. Це більш конкретно можна сформулювати у вигляді двох узагальнених задач: виключення випадкового чи навмисного видання інформації стороннім особам і розмежування доступу до пристроїв і ресурсів системи всіх користувачів, адміністрації та обслуговуючого персоналу. З іншої сторони, системи захисту не повинні створювати помітних незручностей при роботі з використанням ресурсів системи.

Зокрема *повинні бути гарантовані*:

- повна свобода доступу кожного користувача і незалежність його роботи в межах наданих йому прав і повноважень;
- зручність роботи з інформацією для груп взаємопов'язаних

користувачів;
- можливість користувачам допускати один одного до своєї інформації.

Існують різні уявлення про системи захисту інформації (СЗІ) з точки зору їх призначення, складу і виконуваних функцій. Для формування повного уявлення про СЗІ розглянемо їх основні складові, а саме:
- законодавча, нормативно-методична і наукова база;
- структура і задачі органів (підрозділів), що здійснюють комплексний захист інформації;
- організаційно-технічні та режимні заходи;
- програмно-технічні методи і засоби захисту інформації.

Однією з основних складових СЗІ є нормативно-методологічна база, у документах якої розкриваються такі групи питань.

Основи:
- структура і задачі органів (підрозділів), що забезпечують захист інформації;
- організаційно-технічні та режимні заходи і методи (політика інформаційної безпеки);
- програмно-технічні способи і засоби.

Напрями:
- захист об'єктів корпоративних систем;
- захист процесів, процедур і програм оброблення інформації;
- захист каналів зв'язку;
- заглушення побічних електромагнітних випромінювань;
- управління системою захисту.

Етапи:
- визначення інформаційних і технічних ресурсів, що підлягають захисту;
- виявлення потенційно можливих загроз і каналів витоку інформації;
- проведення оцінки уразливості та ризиків інформації при наявних загрозах і каналах витоку;
- визначення вимог до системи захисту;
- здійснення вибору засобів захисту інформації та їх характеристик;
- впровадження і організація використання обраних заходів, способів і засобів захисту;
- здійснення контролю цілісності та управління системою захисту;

Морально-етичні норми – це усталені моральні норми і правила, підтримання яких сприяє захисту інформації, а порушення їх прирівнюється до не підтримання правил поведінки у суспільстві.

Головними властивостями системи захисту інформації є (рис. 1):
- адаптивність її при зміні структури технологічних схем чи умов функціонування ІС;
- мінімізація витрат, максимальне використання серійних засобів;

- комплексне використання засобів захисту, оптимізація архітектури;

Рис.1. Властивості системи захисту інформації

- забезпечення рішень необхідної сукупності задач захисту;
- зручність для персоналу;
- простота експлуатації.

Система захисту інформації, як правило, будується у вигляді взаємозв'язаних **підсистем:**

- криптографічного захисту;
- забезпечення юридичного значення електронних документів;
- захисту від несанкціонованого доступу;
- організаційно-правового захисту;
- керування СЗІ.

Побудова системи захисту інформації у такому вигляді забезпечує комплексність процесу захисту інформації в ІС, керованість процесу і можливість адаптації при зміні умов функціонування ІС.

Підсистема криптографічного захисту об'єднує засоби такого захисту інформації і за рядом функцій кооперується з підсистемою захисту від несанкціонованого доступу.

Підсистема забезпечення юридичного значення електронних документів служить для надання юридичного статусу документам у електронному поданні і є визначальним моментом при переході до безпаперової технології документообігу. Цю підсистему зручно і доцільно розглядати як частину підсистеми криптографічного захисту.

Підсистема захисту від несанкціонованого доступу запобігає доступу несанкціонованих користувачів до ресурсів ІС.

Підсистема керування СЗІ призначена для керування ключовими

структурами підсистеми криптографічного захисту, а також контролю і діагностування програмно-апаратних засобів та забезпечення взаємодії всіх підсистем СЗІ.

Підсистема організаційно-правового захисту призначена для регламентації діяльності користувачів ІС і є упорядкованою сукупністю організаційних рішень, нормативів, законів і правил, які визначають загальну організацію робіт щодо захисту інформації в ІС

Система захисту інформації – це сукупність автоматизованих робочих місць (АРМ), що входять до складу ІС, і програмно-апаратних засобів, інтегрованих в АРМ користувачів ІС.

Важливо відрізняти поняття "захищена інформаційна система" і "система захисту інформації". Багато спеціалістів вважають, що точну відповідь на питання, що ж таке „захищена інформаційна система", поки що не знайдено.

Існують такі уявлення захищеності інформаційної системи (ІС):

- це сукупність засобів і технологічних прийомів для забезпечення захисту компонентів інформаційної системи;
- це мінімізація ризику, якому можуть бути піддані компоненти і ресурси інформаційної системи;
- це комплекс процедурних, логічних і фізичних заходів, спрямованих на запобігання загрозам інформації і компонентам операційної системи.

З урахуванням цього дається таке означення захищеної інформаційної системи.

Інформаційна система називається захищеною, якщо в ній реалізовано механізми виконання правил, які задовольняють встановленому на основі аналізу загроз переліку вимог до захисту інформації і компонентів цієї інформаційної системи.

При цьому механізми виконання зазначених правил найчастіше реалізуються у вигляді системи захисту інформації.

Отже, під **системою захисту інформації** розуміють сукупність механізмів захисту, що реалізують установлені правила, які задовольняють зазначені вимоги.

Таким чином, список загроз інформації визначає основу для формування вимог до захисту. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту. Ці правила, в свою чергу, визначають необхідні функції і засоби захисту, об'єднані в ***комплексну систему захисту інформації (КСЗІ).***

Чим повніший список вимог до захисту і відповідних правил захисту, тим ефективнішою буде СЗІ для даної ІС.

Для того, щоб побудувати захищену ІС, доцільно провести аналіз загроз інформації, скласти перелік вимог до захисту, сформулювати правила організації безпосереднього захисту і реалізувати їх виконання шляхом створення комплексної СЗІ, яка є сукупністю законодавчих,

організаційних, технічних та інших засобів для забезпечення захисту важливої інформації від усіх виявлених загроз і можливих каналів витоку.

До останнього часу, розглядаючи проблеми забезпечення інформаційної безпеки, говорили про створення систем захисту інформації, в той час як питання забезпечення інформаційної безпеки носили більш абстрактний характер. Сьогодні в інформаційному плані вже не ставлять істотної різниці між системами оброблення, передавання і зберігання інформації. У зв'язку з ідеологією єдиної інформаційної магістралі все більш практичне розповсюдження отримує поняття " інформаційна технологія" (ІТ) та його похідні: "системи інформаційних технологій" (ІТ – системи), "продукти інформаційних технологій" (ІТ – продукти), "безпека інформаційних технологій" (ІТ – безпека).

Тобто, одночасно з трансформуванням поглядів на процеси оброблення інформації відбувається і зміна поглядів на підходи до забезпечення інформаційної безпеки.

1.2. Вимоги до систем захисту інформації

Вимоги до захисту інформації визначаються власником інформаційної системи і погоджуються з виконавцем робіт щодо створення систем захисту інформації.

У процесі формування вимог до СЗІ доцільно знайти відповіді на такі питання:

1. Які заходи безпеки передбачається використати ?
2. Яка вартість доступних програмних і технічних засобів захисту ?
3. Наскільки ефективні доступні заходи захисту ?
4. Наскільки вразливі підсистеми СЗІ ?
5. Чи є можливість проведення аналізу ризику (прогнозування можливих наслідків, які можуть викликати виявлені загрози і канали витоку інформації) ?

У загальному випадку доцільно виділити такі групи вимог до систем захисту інформації:

- загальні вимоги;
- організаційні вимоги;
- конкретні вимоги до підсистем захисту, технічного і програмного забезпечення, документування, способів, методів і засобів захисту.

1.2.1. Загальні вимоги

Перш за все, необхідна повна ідентифікація користувачів, терміналів, програм, а також основних процесів і процедур, бажано до рівня запису чи елемента. Крім того, ***слід обмежити доступ до інформації, використовуючи сукупність таких способів:***

- ієрархічна класифікація доступу;
- класифікація інформації за важливістю і місцем її виникнення;
- зазначення обмежень до інформаційних об’єктів, наприклад, користувач може здійснювати тільки зчитування файлу без права запису в нього;
- визначення програм і процедур, наданих тільки конкретним користувачам.

Система захисту повинна гарантувати, що будь-яке переміщення даних ідентифікується, авторизується, виявляється і документується.

Загальні вимоги, зазвичай, висуваються до таких характеристик:

- способів побудови СЗІ чи її окремих компонентів (програмного, програмно-апаратного, апаратного забезпечення);
- структури систем обчислювальної техніки та інформаційних систем (до класу і мінімальної конфігурації ЕОМ, операційного середовища, орієнтації на ту чи іншу програмну і апаратну платформи, архітектури інтерфейсу);
- застосування стратегії захисту;
- витрат ресурсів на забезпечення СЗІ (до об’ємів дискової пам’яті для програмної версії та оперативної пам’яті для її резидентної частини, витратам продуктивності обчислювальної системи на вирішення питань систем захисту);
- надійності функціонування СЗІ (до кількісних значень показників надійності у всіх режимах функціонування ІС і при дії зовнішніх руйнівних факторів, до критеріїв відмов);
- кількості ступенів секретності інформації, що підтримуються СЗІ;
- забезпечення швидкості обміну інформацією в ІС, в тому числі з урахуванням використовуваних криптографічних перетворень;
- кількості підтримуваних СЗІ рівнів повноважень;
- можливості СЗІ обслуговувати певну кількість користувачів;
- тривалості процедури генерації програмної версії СЗІ;
- тривалості процедури підготовки СЗІ до роботи після подачі живлення на компоненти ІС;
- можливості СЗІ реагувати на спроби несанкціонованого доступу, або на „небезпечні ситуації”;
- наявності та забезпечення автоматизованого робочого місця адміністратора захисту інформації в ІС;
- складу використовуваного програмного і лінгвістичного забезпечення, до його сумісності з іншими програмними платформами, до можливості модифікації тощо;
- використовуваних закупних компонентів СЗІ (наявність ліцензії, сертифікату тощо).

1.2.2. Організаційні вимоги

Організаційні вимоги до системи захисту передбачають реалізацію сукупності адміністративних і процедурних заходів.

Вимоги щодо забезпечення цілісності повинні виконуватись перш за все на адміністративному рівні. ***Організаційні заходи, що проводять з метою підвищення ефективності захисту інформації, повинні передбачати такі процедури:***

- обмеження несупроводжуваного доступу до обчислювальної системи (реєстрація і супроводження відвідувачів) ***;***
- здійснення контролю за змінами у системі програмного забезпечення;
- виконання тестування і верифікації змін у системі програмного забезпечення і програмах захисту;
- організацію і підтримку взаємного контролю за виконанням правил захисту даних;
- обмеження привілеїв персоналу, що обслуговує ІС;
- здійснення запису протоколу про доступ до системи;
- гарантію компетентності обслуговуючого персоналу;
- розробку послідовного підходу до забезпечення цілісності інформації для всієї організації;
- організацію чіткої роботи служби дискової бібліотеки;
- комплектування основного складу персоналу на базі інтегральних оцінок здібностей, знань, рис характеру тощо;
- організацію системи навчання і підвищення кваліфікації обслуговуючого персоналу.

Для забезпечення доступу до ІС слід виконувати такі процедурні заходи:

- розроблення і затвердження письмових інструкцій на завантаження і зупинку роботи операційної системи;
- контроль використання носіїв інформації, лістингів, порядок зміни програмного забезпечення і доведення інформації щодо цих змін до користувача;
- розроблення процедури відновлення системи у разі відмов;
- встановлення політики обмежень при дозволених візитах в обчислювальний центр і визначення обсягу інформації, що видається;
- розроблення системи протоколювання використання ЕОМ, введення даних і виведення результатів;
- проведення періодичного чищення архівів і сховищ носіїв інформації для вилучення і ліквідації тих, що не використовуються;
- підтримування документації обчислювального центру згідно із стандартами інформаційної безпеки підприємства.

1.2.3. Вимоги до підсистем системи захисту інформації

В загальному випадку СЗІ поділяються на підсистеми (рис.2):

- управління доступом до ресурсів ІС (включає також функції управління системою захисту в цілому);
- реєстрації та обліку дій користувачів (процесів);
- криптографічну;
- забезпечення цілісності інформаційних ресурсів і конфігурацій ІС.

До кожної з підсистем висуваються такі вимоги:

- перелік забезпечуваних підсистемою функцій захисту;
- основні характеристики цих функцій;
- перелік засобів, що реалізують ці функції.

Підсистема управління доступом повинна забезпечувати:

- ідентифікацію, автентифікацію і контроль за доступом користувачів (процесів) до системи, терміналів, вузлів зв'язку, зовнішніх пристроїв, програм, каталогів, файлів, записів тощо;
- управління потоками інформації;
- очищення звільнюваних областей оперативної пам'яті та зовнішніх накопичувачів.

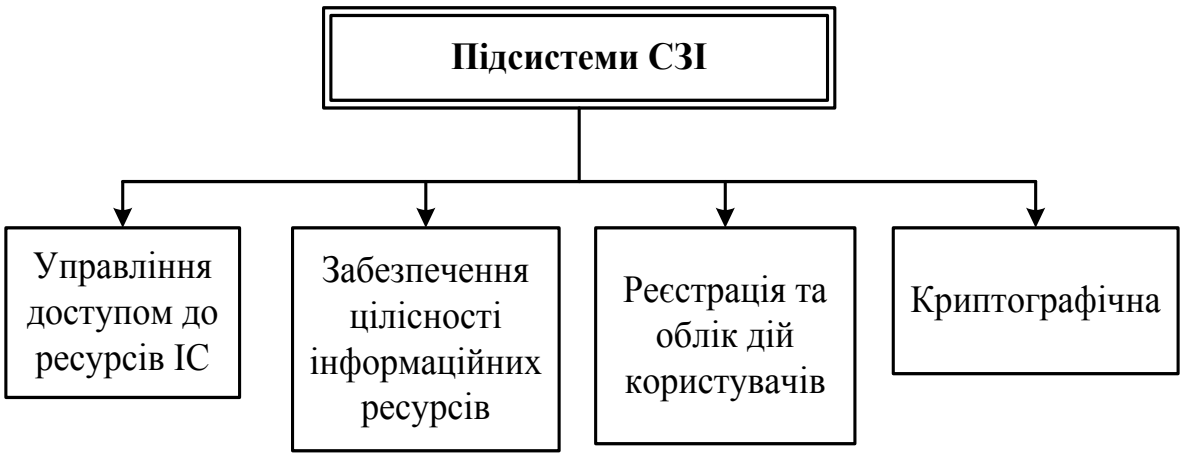

Рис. 2. Підсистеми системи захисту інформації

Підсистема реєстрації та обліку виконує:

- реєстрацію та облік: доступу в ІС, видачі вихідних документів, захисту програм і процесів, доступу до захищуваних файлів, передавання даних каналами зв'язку;
- реєстрацію змін повноважень доступу, створення об'єктів доступу, що підлягають захисту;
- облік носіїв інформації;

- сповіщення про спроби порушення захисту.

Криптографічна підсистема передбачає:
- шифрування конфіденційної інформації;
- шифрування інформації, що належить різним суб'єктам доступу (групі суб'єктів) з використанням різних ключів;
- використання атестованих (сертифікованих) криптографічних засобів.

Підсистема забезпечення цілісності здійснює:
- забезпечення цілісності програмних засобів і оброблюваної інформації;
- фізичну охорону засобів обчислювальної техніки і носіїв інформації;
- наявність адміністратора (служби) захисту інформації в ІС;
- періодичне тестування СЗІ;
- наявність засобів відновлення СЗІ;
- використання сертифікованих засобів захисту;
- контроль за цілісністю:
  - а) програмних засобів захисту інформації при завантаженні операційного середовища;
  - б) операційного середовища перед виконанням процесів;
  - в) функціонального програмного забезпечення і даних;
  - г) конфігурації ІС;
- оперативне відновлення функцій СЗІ після збоїв;
- тестування засобів захисту інформації;
- виявлення і блокування розповсюдження вірусів;
- резервне копіювання програмного забезпечення і даних;
- контроль доступу до засобів обчислювальної техніки, що дає впевненість у тому, що тільки авторизований користувач використовує наявні робочі програми та інформацію;
- контроль дій з персональною авторизацією, що забороняє операції, які можуть зробити операційне середовище вразливим;
- захист програмного забезпечення, що включає пошкодження інстальованих програм;
- використання тільки ліцензованого програмного продукту з метою забезпечення захисту від вбудованих модулів руйнування інформаційного середовища і дискредитації систем захисту;
- захист комунікацій для забезпечення недоступності інформації, що передається.

1.2.4. Вимоги до технічного забезпечення

У цій групі формуються ***вимоги до таких параметрів:***
- місця застосування засобів захисту;
- способів використання засобів захисту (наприклад, реалізація

вимог захищеності повинна досягатися без застосування екранування приміщень, активні засоби можуть застосовуватись тільки для захисту інформації головного сервера тощо);
- розмірів контрольованої зони безпеки інформації;
- необхідної величини показників захищеності, що враховує реальну обстановку на об'єктах ІС;
- способів, методів і засобів досягнення необхідних показників захищеності;
- рівнів електромагнітних випромінювань (ЕМВ);
- відсутності спеціальних електронних закладних пристроїв.

1.2.5. Вимоги до документування

Вимоги до документування системи захисту інформації поділяються на три групи: протоколювання, тестування програм і обробка загроз.

При розробці системи *протоколювання* враховуються такі специфічні вимоги:
- необхідність запису всіх переміщень захищуваних даних;
- можливість відтворення при необхідності ретроспективи використання захищуваного об'єкта, для реалізації якої забезпечується запам'ятовування станів програм і навколишнього середовища;
- накопичення статистики за протоколами використання інформації в системі.

У процесі *тестування програм* системи захисту інформації обов'язковим є використання спеціальної програми генерування неправильних адрес, несанкціонованих спроб доступу до даних, моделювання нештатних ситуацій та інших специфічних властивостей. Необхідно також звертати увагу на ретельну перевірку таблиць безпеки, системи паролів і програми доступу.

Система захисту інформації повинна мати спеціальне програмне забезпечення обробки загроз, яке включає:
- реєстрацію подій у системному журналі, захищеному від спроб зміни зі сторони програм користувачів;
- використання зібраних відомостей для аналізу якісного вирішення проблеми захисту інформації та розробки заходів для її удосконалення.

Перелічені вимоги і заходи щодо забезпечення збереження інформації показують, що воно пов'язане з вирішенням серйозних математичних і технічних проблем.

1.3. Етапи проектування сучасних систем захисту інформації

Згідно з міжнародним стандартом ISO/IEC15408 "Єдині критерії оцінювання безпеки інформаційних технологій" проектування СЗІ

здійснюється в п’ять етапів (рис.3).

На І етапі здійснюється:

- визначення сфери (меж) СЗІ і конкретизація мети її створення;
- визначення ступеня небезпеки середовища експлуатації для функціонування об’єкта оцінювання (ТОЕ – Target of Evaluation) шляхом виявлення загроз і виявлення ризиків;

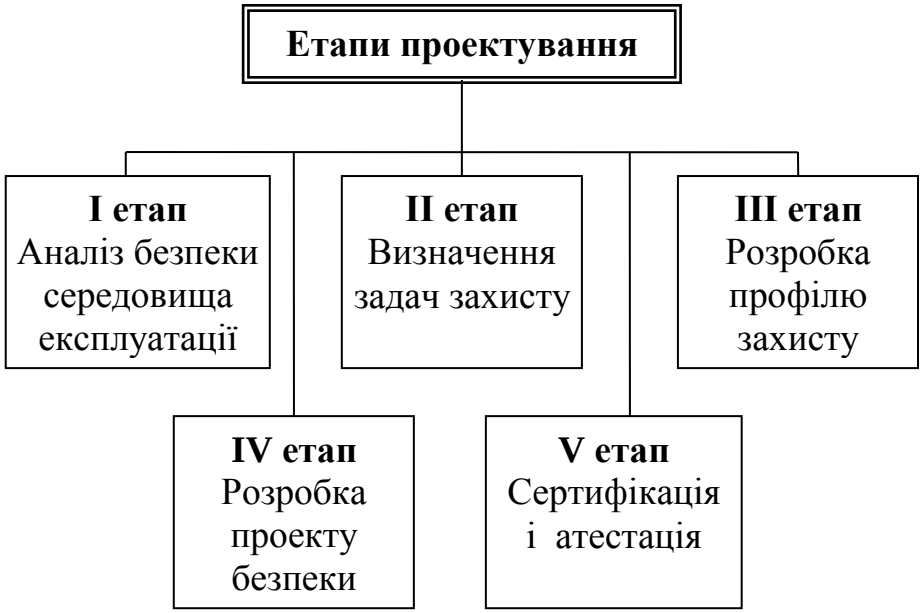

Рис. 3. Етапи проектування систем захисту інформації

- формування початкових передумов для визначення задач щодо забезпечення ІТ- безпеки.

Середовище експлуатації – це сукупність фізичних, інформаційних, технічних об’єктів і систем, зовнішніх відносно ТОЕ, а також організаційних заходів, правових норм, умов експлуатації і технологічних особливостей використання ТОЕ, які мають фізичний, інформаційний, енергетичний та інший вплив на функціонування ТОЕ .

На цьому етапі вирішуються такі задачі:

- аналіз середовища експлуатації з погляду забезпечення фізичної безпеки;
- оцінювання ресурсів, що підлягають захисту;
- створення моделі порушника, аналіз методів нападу і вразливостей системи;
- формування повного переліку загроз безпеці;
- оцінювання ризиків і вибір стратегії управління ризиками.

Таким чином, на першому етапі розробляється концепція забезпечення інформаційної безпеки і політика безпеки.

На ІІ етапі на основі результатів аналізу середовища експлуатації здійснюється формулювання множини задач захисту. Задачі захисту

повинні бути погоджені з множиною інших функціональних задач об'єкта оцінювання і не суперечити основному призначенню ТОЕ. Вони визначаються як для об'єкта оцінки, так і для середовища його експлуатації і спрямовані виключно на реалізацію вимог щодо забезпечення ІТ-безпеки.

ІІІ етап – вибір і розробка вимог ІТ-безпеки.

Сформульовані задачі захисту є базою для безпосередньої розробки профілю захисту, яка здійснюється шляхом:

- пошуку і вибору профілю прототипу;
- уточнення і синтезу ІТ-безпеки.

Профіль захисту(ПЗ) – це реалізаційно-незалежна сукупність функціональних вимог і вимог адекватності, направлених на задоволення потреб споживача (користувача і власника) захищуваних ресурсів у забезпеченні безпеки інформації. Профіль захисту є нормативним документом, який регламентує всі аспекти ІТ-безпеки у вигляді сукупності вимог ІТ-безпеки, що висуваються до функцій безпеки і, отже, до механізмів безпеки і засобів захисту.

Вимоги ІТ-безпеки є уточненням, конкретизацією і практичним відображенням задач захисту. Вони включають такі компоненти:

- функціональні вимоги безпеки;
- вимоги адекватності;
- вимоги безпеки до середовища експлуатації.

У ході розробки профілю захисту здійснюється вибір вимог безпеки, специфічних для конкретного середовища. Вибір здійснюється на основі оцінки ефективності реалізації даних вимог для розв'язання задачі протидії загрозам безпеки. Функціональні вимоги визначають властивості безпеки і характеризують функції безпеки ТОЕ, які є типовими для підтримання ІТ-безпеки.

На IV етапі здійснюється розробка специфікацій функцій безпеки і підсумкової специфікації забезпечення безпеки ТОЕ. Цей етап є, фактично, розробкою проекту безпеки.

Проект безпеки – це множина вимог ІТ-безпеки і специфікацій функцій безпеки.

Проект безпеки використовується як основа для розробки і оцінювання (атестації) ТОЕ на відповідність вимогам інформаційної безпеки. Підсумкова специфікація включає в себе опис заявлених функцій безпеки, які задовольняють функціональні вимоги, і визначення показників адекватності, що характеризують ступінь виконання вимог адекватності.

На V етапі здійснюється оцінювання повноти, коректності, погодженості та реалізованості профілю захисту і проекту безпеки.

1.4. Принципи побудови систем захисту інформації

Питання організації захисту інформації повинні вирішуватися уже на стадії передпроектної розробки.

Досвід проектування систем захисту ще недостатній. Проте вже можна зробити деякі узагальнення. Помилок захисту може бути значно менше, якщо при проектуванні враховувати такі основні принципи побудови систем захисту:

1. *Простота механізму захисту.* Цей принцип загальнодоступний, але не завжди глибоко усвідомлюється. Механізми захисту повинні бути інтуїтивно зрозумілі та прості в користуванні. Застосування засобів захисту не повинно бути пов'язане зі знанням спеціальних мов або з використанням трудомістких дій при звичайній роботі користувачів, що працюють на законних підставах.

2. *Постійність захисту.* Цей принцип полягає в тому, що захист, у свою чергу, повинен бути постійно захищеним від несанкціонованих змін. Жодна комп'ютерна система не може розглядатися як безпечна, якщо основні апаратні і програмні механізми, призначені забезпечити безпеку, самі є об'єктами несанкціонованої модифікації чи видозмінення.

3. *Наскрізний контроль.* Цей принцип передбачає необхідність перевірки повноважень будь-якого звернення до будь-якого об'єкта і лежить в основі системи захисту.

4. *Несекретність проектування.* Механізм захисту повинен функціонувати достатньо ефективно навіть у тому випадку, коли його структура і зміст відомі зловмиснику. Не має сенсу засекречувати деталі реалізації системи захисту, призначеної для широкого використання. Ефективність захисту не повинна залежати від того, наскільки досвідчені потенційні порушники. Захист не повинен забезпечуватись тільки секретністю структурної організації і алгоритмів функціонування її підсистем. Знання алгоритмів роботи системи захисту не повинно сприяти її подоланню (навіть автору).

5. *Ідентифікація.* Кожний об'єкт інформаційної системи повинен однозначно ідентифікуватися. При спробі отримання доступу до інформації рішення про його санкціонування слід приймати на основі даних претендента і визначення вищого ступеня секретності інформації, з якою тому дозволяється працювати. Такі дані про ідентифікацію і повноваження повинні надійно зберігатися і поновлюватися комп'ютерною системою для кожного активного учасника системи, щоб запобігти порушенню її цілісності. Користувачі повинні мати відповідні повноваження, об'єкти (файли) – відповідний гриф, а система повинна контролювати всі спроби отримання доступу.

6. *Розподіл повноважень.* Застосування декількох ключів захисту. Це зручно в тих випадках, коли право доступу визначається виконанням низки умов.

7. *Мінімальні повноваження.* Для будь-якої програми і будь-якого користувача повинно бути визначено коло повноважень, необхідних для

роботи.

8. *Надійність.* Система захисту інформації повинна мати механізм, який дозволяв би оцінити забезпечення достатньої надійності функціонування СЗІ (підтримання правил безпеки, секретності, ідентифікації і звітності). Для цього необхідні вивірені та уніфіковані апаратні та програмні засоби контролю. Метою застосування даних механізмів є виконання визначених задач методом, що забезпечує безпеку.

9. *Максимальна відособленість*. Цей принцип означає, що захист повинен бути відокремлений від функцій управління даними.

10. *Захист на місці.* Пакет програм, що реалізують захист, повинен розміщуватися в захищеному полі пам'яті, щоб забезпечити системну локалізацію спроб проникнення ззовні. Навіть спроба проникнення зі сторони програм операційної системи повинна автоматично фіксуватися, документуватися і відкидатися, якщо виклик виконаний некоректно.

11. *Зручність для користувачів*. Схема захисту повинна бути в реалізації простою, щоб механізм захисту не створював для користувачів додаткових труднощів.

12. *Контроль доступу*. Забезпечує захист від атак неавторизованих користувачів на доступ:

- до ресурсів персонального комп'ютера;
- до областей HD персонального комп'ютера;
- до ресурсів і серверів мережі;
- до модулів виконання авторизації користувачів.

13. *Авторизація користувача*. Використання фізичного ключа дозволяє виключити ненавмисні дискредитації прав доступу користувача.

14. *Звітність.* Слід захищати контрольні дані від модифікації і несанкціонованого знищення, щоб забезпечити викриття і розслідування виявлених фактів порушення безпеки. Надійна система повинна забезпечити відомості про всі події, що мають відношення до безпеки, в конкретних журналах. Окрім того, вона повинна гарантувати вибір подій, що складають інтерес при проведенні аудиту, щоб мінімізувати вартість витрат і підвищити ефективність аналізу. Наявність програмних засобів аудиту чи створення звітів ще не гарантує ні підсилення безпеки, ні можливості розкриття порушень.

15. *Доступність до виконання*. Тільки ті команди операційної системи, які не можуть зіпсувати операційне середовище і результат контролю попередньої автентифікації, допускаються до виконання.

16. *Наявність механізмів захисту* від:

- несанкціонованого зчитування інформації;
- модифікації інформації, що зберігається і циркулює в мережі;
- нав'язування інформації;
- несанкціонованої відмови від авторства переданої інформації.

17. *Системний підхід* до захисту інформації. Означає необхідність урахування всіх взаємопов'язаних, взаємодіючих і змінних у часі

елементів, умов і фактів, істотних для забезпечення безпеки інформаційних систем.

18. *Можливість нарощування захисту*. Система захисту повинна будуватися з урахуванням не тільки всіх відомих каналів проникнення і несанкціонованого доступу до інформації, але й з урахуванням появи принципово нових шляхів реалізації загроз безпеки.

19. *Комплексний підхід до захисту інформації*. Він полягає у тому, що передбачається погодження застосування різнорідних засобів захисту інформації.

20. *Адекватність*. Необхідний рівень захисту (визначення ступеня секретності інформації, що обробляється) повинен забезпечуватись мінімально можливими витратами на створення механізму захисту і забезпечення його функціонування.

21. *Мінімізація пільг доступу*. Кожному користувачеві повинні надаватись тільки дійсно необхідні йому права на звернення до ресурсів системи і даних.

22. *Повнота контролю.* Обов'язковим є контроль усіх звернень до захищених даних.

23. *Карність порушень.* Найпоширеніший спосіб покарання – відмова в доступі до системи.

24. *Спеціалізація.* Цей принцип організації захисту передбачає, що надійний механізм захисту може бути спроектований і організований тільки професійними спеціалістами із захисту інформації.

25. *Гнучкість системи захисту*. Прийняті заходи і встановлені засоби захисту, особливо на початку їх експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захисту. Для забезпечення можливості варіювання рівнем захищеності, засоби захисту повинні мати певну міру гнучкості. Ця властивість важлива особливо у тих випадках, коли встановлення засобів захисту треба здійснювати на працюючу систему, не порушуючи процесу її нормального функціонування.

26. *Безперервність забезпеченості захисту.* Цей принцип означає, що захист інформації – це не разовий захід і навіть не визначена сукупність проведених заходів і встановлених засобів захисту, а безперервний цілеспрямований процес, який передбачає прийняття відповідних заходів на всіх етапах життєвого циклу інформаційної системи. Розробка системи захисту повинна здійснюватись паралельно з розробкою захищуваної системи. Це дозволяє урахувати вимоги безпеки при проектуванні архітектури і, зрештою, створити більш ефективні захищені інформаційні системи.

Контрольні питання

1. Охарактеризуйте періоди розвитку систем захисту інформації.

2. Розшифруйте поняття термінів “інформаційна безпека“ та “захист інформації“.
3. Перелічіть фактори, які впливають на поняття захисту інформації.
4. Опишіть захисні пояси системи захисту інформації.
5. Наведіть класифікацію правил захисту інформації.
6. Розкрийте суть нормативно-методичної бази СЗІ.
7. Охарактеризуйте властивості системи захисту інформації.
8. Наведіть класифікацію підсистем СЗІ.
9. Розшифруйте поняття терміну “захищена інформаційна система.”
10. Наведіть класифікацію вимог до систем захисту інформації.
11. Охарактеризуйте загальні вимоги до СЗІ.
12. Поясніть суть характеристик, які слід враховувати при формулюванні загальних вимог до СЗІ.
13. Опишіть організаційні заходи, що підвищують ефективність захисту інформації.
14. Наведіть класифікацію підсистем СЗІ.
15. Опишіть функції підсистем управління доступом до інформаційних систем.
16. Охарактеризуйте функції підсистеми забезпечення цілісності інформації.
17. Поясніть особливості вимог до технічного забезпечення систем захисту інформації.
18. Опишіть особливості вимог до документування систем захисту інформації.
19. Наведіть класифікацію етапів проектування сучасних систем захисту інформації.
20. Розкажіть про особливості заходів, що здійснюються на 1 етапі проектування СЗІ.
21. Охарактеризуйте задачі 2 і 3 етапів проектування сучасних систем захисту інформації.
22. Розкрийте суть завдань 4 і 5 етапів проектування СЗІ.
23. Наведіть класифікацію основних принципів побудови систем захисту інформації.
24. Розкрийте суть принципів ідентифікації та простоти механізмів захисту.
25. Обґрунтуйте значення принципів контролю доступу та звітності в надійності захисту інформації
26. Поясніть суть гнучкості системи захисту інформації.
27. Опишіть особливості принципу безперервності захисту інформації.

Глава 2. ОРГАНІЗАЦІЙНІ ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1. Основні поняття

Організаційний захист інформації – це регламентація виробничої діяльності та взаємостосунків виконавців на нормативно-правовій основі, що виключає чи істотно утруднює неправомірне оволодіння конфіденціальною інформацією та проявлення внутрішніх і зовнішніх загроз.

Організаційний захист забезпечує:

- організацію охорони, режиму;
- роботу з кадрами, з документацією;
- використання технічних засобів безпеки;
- інформаційно-аналітичну діяльність щодо виявлення внутрішніх і зовнішніх загроз підприємницькій діяльності.

Значну роль у створенні надійного механізму захисту інформації відіграють ***організаційні заходи,*** так як можливості несанкціонованого використання конфіденційних відомостей у значній мірі обумовлюються не технічними аспектами, а зловмисними діями, неуважністю, недбайливістю і халатністю користувачів чи персоналу захисту. Вплив цих аспектів практично неможливо уникнути за допомогою технічних засобів. Для цього необхідна сукупність організаційно-правових і організаційно-технічних заходів, які б виключали чи зводили до мінімуму можливість виникнення небезпеки конфіденціальній інформації.

Організаційні заходи – це заходи обмежувального характеру, які зводяться, в основному, до регламентації доступу і використання технічних засобів обробки інформації.

Вони, як правило, проводяться силами самої організації застосуванням таких дій:

- визначення границь охоронюваної зони (території);
- визначення технічних засобів, використовуваних для обробки конфіденціальної інформації у межах контрольованої території;
- визначення “небезпечних”, з точки зору можливості утворення каналів витоку інформації, технічних засобів і конструктивних особливостей будівель і споруд;
- виявлення можливих шляхів доступу до джерел конфіденціальної інформації зі сторони зловмисників;
- реалізація заходів щодо виявлення і контролю за забезпеченням захисту всіма доступними засобами (рис. 4).

Організаційні заходи поділяються на територіальні, просторові та часові обмеження (рис. 5).

Територіальні обмеження зводяться до умілого розташування джерел інформації на місцевості чи в будівлях і приміщеннях з метою виключення

прослуховування переговорів чи перехоплення сигналів радіоелектронних засобів.

Рис.4. Основні заходи захисту інформації

Просторові обмеження виражаються у виборі напрямків випромінювання тих чи інших сигналів у сторону найменшої можливості їх перехоплення зловмисниками.

Часові обмеження проявляються у скороченні до мінімуму часу роботи технічних засобів, використанні прихованих методів зв'язку, шифруванні та інших заходах захисту.

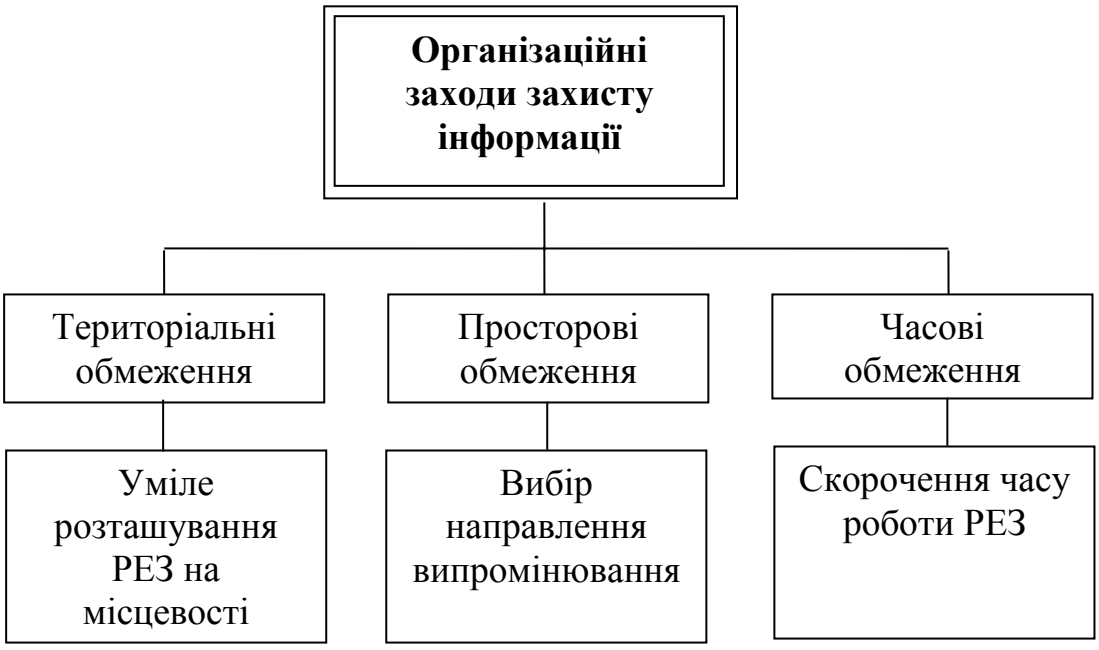

Рис.5. Основні організаційні заходи захисту інформації

Однією з найважливіших задач організаційної діяльності є визначення стану технічної безпеки об'єкта, його приміщень, підготовка і виконання організаційних заходів для виключення можливості неправомірного оволодіння конфіденційною інформацією, заборона її розголошення, витоку і несанкціонованого доступу до охоронюваних секретів.

У процесі розробки і реалізації організаційних заходів захисту інформації необхідно:

- визначити задачі захисту інформації;
- обґрунтувати структуру і технологію функціонування системи захисту інформації;
- розробити і впровадити правила реалізації заходів захисту інформації;
- визначити і встановити права і обов'язки підрозділів і осіб, які беруть участь у обробці інформації;
- придбати засоби забезпечення захисту інформації та нормативні документи, забезпечити ними організацію;
- встановити порядок впровадження захищених засобів обробки інформації, програмних, технічних і контролюючих засобів;
- встановити порядок контролю функціонування системи захисту інформації та її якісних характеристик;
- визначити зони безпеки інформації;
- встановити порядок проведення атестації системи технічного захисту інформації та її елементів, розробити програми атестаційних випробувань;
- забезпечити управління системою захисту інформації.

Оперативне розв'язання задач захисту інформації досягається організацією управління системою захисту інформації, для чого необхідно:

- вивчити і проаналізувати технологію проходження інформації в процесі інформаційної діяльності;
- оцінити уразливість інформації в конкретний момент;
- оцінити очікувану ефективність використання засобів забезпечення захисту інформації;
- визначити додаткову необхідність у засобах забезпечення захисту інформації;
- здійснити збирання, оброблення і реєстрацію даних, що відносяться до захисту інформації;
- розробити і реалізувати пропозиції щодо коректування плану захисту інформації у цілому чи окремих його елементів.

2.2. Організація режиму і охорони

Організація режиму і охорони проводиться з метою:

- виключення можливості таємного проникнення на територію і в приміщення сторонніх осіб;
- забезпечення зручності контролю проходу і переміщення співробі-

тників і відвідувачів;
- створення окремих виробничих зон типу конфіденційних зон з самостійними системами доступу;
- контролю і дотримання часового режиму роботи та перебування на території персоналу організації (фірми);
- організації і дотримання надійного пропускного режиму і контролю співробітників і відвідувачів тощо.

Сучасні способи контролю фізичного доступу поділяються на такі групи:

- система охорони периметра;
- система контролю і управління доступом;
- система відеоспостереження;
- система охоронної сигналізації (часто поєднується з системою охорони периметра, деколи включає систему пожежної сигналізації);
- система збереження (сейфи, шафи тощо).

2.2.1. Система охорони периметра

Слід визначити, яку територію необхідно охороняти і які типи суб'єктів повинні знаходитися на ній, режим знаходження суб'єктів.

Як приклад розглянемо будівлю, обнесену огорожею, усередині технічний поверх, на якому розміщена серверна кімната. Природно, що за огорожею може знаходитись будь-хто, але у безпосередній близькості до огорожі і біля воріт організації сторонні можуть знаходитися тільки обмежений час (мимохідь) – інші випадки повинні привертати увагу служби безпеки. За огорожу (охоронюваний периметр) можуть пройти тільки співробітники організації і особи, яких вони супроводжують, причому тільки у робочий час, скажімо з 8.00 до 18.00. У будівлю можуть пройти тільки ті, хто має пропуск, незалежно від організаційної та посадової належності, причому входити можна з 8.00 до 18.00, виходити – до 22.00, а сторонні ж можуть входити тільки до 16.00, а виходити – точно до 18.00. На технічний поверх можуть підійматися виключно працівники технічної служби і тільки у робочий час, у серверну кімнату може входити лише системний оператор (адміністратор) і тільки після інформування служби безпеки.

Тепер можна визначити, які механізми слід використати для розв'язання сформульованих задач. Бажано, щоб огорожа була повністю непрохідною (залежно від режимності організації, з виключенням можливості підкопу чи перелітання), а також була забезпечена камерами відеоспостереження для контролю наближення до огорожі. У внутрішній стороні огорожі можуть бути також встановлені датчики руху чи "наступу" для того, щоб, з однієї сторони, виявити суб'єктів, що проминули огорожу ззовні, а з іншої сторони – запобігти наближенню працівників організації до огорожі. На стіні огорожі (будівлі, підвалу) допускається встановлення датчиків вібрації на предмет спроби пролому стін. На воротах огорожі достатньо візуального контролю співробітника

служби безпеки для перевірки документів, а також наявність металошукача і\чи просвічувального пристрою для перевірки предметів, що вносяться.

2.2.2. Система управління доступом

Управління доступом можна умовно поділити на дві частини, а саме:

- *управління первинним проходом* на охоронювану територію;
- *управління переміщеннями* на охоронюваній території.

Якщо усередині однієї охоронюваної території знаходиться інша, ще більш суворо охоронювана, то кількість поділів, відповідно, подвоюється.

Задача первинного контролю – відсікти тих, до кого не можуть бути застосовані авторизаційні правила, тобто тих, у кого на території немає ніяких прав доступу; забезпечити, щоб на територію не були занесені заборонені предмети, а також ряд інших функцій, у тому числі, можливо, тих, які не можуть бути наперед регламентовані чи автоматизовані (наприклад, прийняття рішень при підозріванні, що пред'явлений пропуск належить іншій особі). Найбільш відомі механізми допуску у даному випадку такі:

- турнікети і металеві ворота, які забезпечують розподіл людського потоку на окремі персони;
- шлюзові кабіни, які забезпечують прохід тільки по 1 людині, без можливості супровідного заставити авторизованого співробітника до спільного проходу через контрольні ворота;
- металошукачі, бажано з можливістю налаштовування на габарити проносимих металевих предметів, щоб відрізнити , скажімо, зв'язку ключів від ножа;
- просвічувальні пристрої – необхідно тільки визначити, чи будуть ці пристрої безпечні для світло- та магніточутливих матеріалів, чи навпаки, жорстко будуть виводити такі матеріали з ладу (у даному разі необхідне попередження про показ таких матеріалів і здачу їх на збереження чи аналіз.);
- переговорні пристрої, якщо управління входом/виходом здійснюється на відстані (сюди входять домофони, відеодомофони, інтерфони тощо).

Окрім перерахованих, на вході можуть стояти пристрої зчитування параметрів доступу, такі ж, як на всіх контрольованих ділянках іншої території.

Задачі контролю переміщень – ідентифікувати /автентифікувати суб'єкта, який запитує дозвіл на прохід, і, застосувавши до нього авторизовані правила, пропустити його чи заборонити прохід.

Ідентифікація/автентифікація суб'єкта проводиться на основі стандартних принципів, а саме:

- щось, що суб'єкт знає. Звичайно це деякий ПІН (персональний ідентифікаційний номер) чи код, який необхідно набрати на панелі замка;
- щось, що суб'єкт має. Це може бути і звичайний дверний ключ чи токен-карточка з магнітною стрічкою, енергонезалежний

ідентифікатор Touch Memory, смарт-карта чи proximity-карта;

- щось, що фізично чи психологічно невіддільне від суб'єкта. Це звичайно біометричні параметри тіла суб'єкта. Деколи з даного розділу виділяють підрозділ "Щось, що суб'єкт робить" – швидкість і тип друку на клавіатурі, механіка особистого підпису, розпізнавання голосу. Інколи цей поділ важливий, так як при певних умовах, наприклад, під примусом, суб'єкт не може змінити, скажімо, відбитки пальців, але може змінити голос і, в останньому випадку, зловмисник не зможе пройти на територію, навіть примушуючи суб'єкт.

Враховуючи специфіку людської індивідуальності, можна сказати, що система контролю доступу, орієнтована тільки на набирання коду, недостатньо надійна, тому що навіть ПІН-коди мають тенденцію ставати широко відомими через деякий час, не кажучи уже про звичайний код доступу.

При виборі токена слід додатково враховувати такі параметри:

- знос (магнітна стрічка стирається з карточки при багаторазовому зчитуванні, енергозалежні елементи мають обмежений термін зберігання/використання);
- швидкість проходу (прикладання елемента до зчитування чи протягання/встановлення карточки у зчитувач вимагають певного часу);
- вартість;
- можливість нанесення фотографії власника на токен;
- міцність на можливий злам/ушкодження тощо.

Серед біометричних засобів автентифікації частіше зустрічаються: відбитки пальців, сітчатка ока, рисунок долоні, геометрія руки, форма обличчя, параметри голосу.

Проте перед прийняттям рішення про придбання того чи іншого засобу слід ознайомитися з останньою наявною статистикою щодо фальшивого спрацьовування і фальшивого відказування для даного виду біометрії. Окрім того, при використанні таких пристроїв слід урахувати культурні традиції та персональні звички – деякі люди, наприклад, не можуть доторкатися до поверхонь, яких торкалися декілька десятків чи сотень чоловік перед цим.

При проектуванні системи контролю переміщення слід врахувати необхідність застосування до суб'єкта єдиної політики доступу. Це значить, що політика доступу повинна бути:

- створена і зберігатися в одному місці для забезпечення однаковості застосування;
- розподілена на декількох пристроях для забезпечення продовження роботи при виході з ладу центрального сервера політики.

Додатково слід передбачити формат реєстрації переміщень суб'єктів у електронному журналі, можливості аналізу журналу, а також його інтеграцію з іншими журналами доступу у комп'ютерну мережу. Авторизаційна політика повинна не тільки визначити, дозволений чи заборонений прохід суб'єкта, але і дату, день тижня і час доби, а також

направлення проходу (наприклад, заборона виходу, якщо не фіксувався вхід). Окрім цього, у системі необхідно передбачити повідомлення на екран чергового співробітника (чи інші варіанти) у разі, якщо прохідні двері залишаються відкритими протягом проміжку часу більшого, ніж треба для проходу.

Можливо, ще слід урахувати змінення політики для масових явищ – ігнорування заборон і відкриття дверей у разі пожежі чи ігнорування дозволів і закривання дверей у разі виявлення зловмисника. Остання деталь – з одного боку, слід обов'язково мати майстер-ключі (ключі безумовного проходу) на випадок збоїв системи, але, з іншого боку, строго обліковувати їх зберігання і використання. Для приміщень, у які обмежений тільки вхід, а вихід дозволений всім, хто зайшов, слід мати на виході не зчитувач, а всього лише кнопку відкривання дверей.

2.2.3. Система відеоспостереження

Першим етапом установки подібної системи є визначення її мети: контроль проходів до периметру, проходів, поведінки працівника у приміщеннях тощо. Залежно від задач системи відеоспостереження потрібні будуть різні типи камер та іншого обладнання. Потім необхідно визначити:

- дію на камеру стеження зі сторони відкритого середовища (дощу, снігу, вітру, пилу);
- освітленість, площу і відкритість території (можливо прийдеться встановлювати джерела світла, демонтувати укриття тощо);
- використовувати камеру приховану чи відкриту;
- чи буде помітне її обертання (якщо камера обертається і не захована);
- чи можна бачити тільки загальні контури об'єктів, чи також і деталі (збільшення зображення);
- достатньо чорно-білого зображення чи треба кольорове;
- чи не стане сама камера об'єктом викрадення, якщо вона встановлена у доступному місці і за межами швидкої досяжності співробітників служби безпеки;
- як буде проглядатися зображення з камер – почергово, по декілька кадрів, всі кадри зразу;
- чи буде проводитися запис зображення і його зберігання.

До початку встановлення обладнання слід протестувати окремі екземпляри камер, моніторів, відеомагнітофонів. Можливо, потрібні будуть різні типи обладнання – скажімо, чорно-білі/статичні камери для спостереження за периметром і кольорові/обертові для спостереження за працівниками в офісі. У такому разі слід протестувати всі типи камер.

Якщо треба вести запис зображення, то бажано відповісти додатково на такі питання :

- чи буде записуватися зображення зі всіх камер, чи тільки з деяких;
- чи буде записування проводитися постійно, чи тільки у разі спрацювання сигналу тривоги в межах досяжності камери;

- записування буде вестися безперервно чи можливе дискретне записування (кадр за секунду/дві/три);
- необхідно на зображення накладати дату/час чи ні;
- записування буде цифровим чи аналоговим.

Є додаткові питання, на які представник служби безпеки не зможе відповісти самостійно, наприклад, який тип кронштейнів для кріплення камер використати тощо.

2.2.4. Система охоронної (пожежної) сигналізації

Для вибору типу/типів охоронної сигналізації необхідно визначити, які події потребують подачі сигналу тривоги. Можливо, це коливання чи проломлення – для огорожі та стін, торкання чи наближення – для огорожі, порушення цілісності – для вікон, наступання/поміщення і маси – для відкритого простору, зміна об'єму – для закритого простору, відкривання/закривання дверей, рух – для різних ділянок охоронюваної території. Для пожежних датчиків ознаками спрацювання є задимлення приміщення і/чи підвищення температури. Дорогим, проте достатньо надійним, рішенням є детектор полум'я, який визначає джерело вогню за інфрачервоною енергією полум'я чи його пульсацією.

Перед придбанням конкретного виду датчиків слід ознайомитися зі статистикою якості роботи пристрою – особливо з відсотками фальшивого спрацьовування від перешкод і неспрацьовування при реальному порушенні. Можливо, ці характеристики доведеться протестувати самим спеціалістам служби безпеки або запитати у незалежних експертів.

При проектуванні системи охоронної сигналізації необхідно зразу пов'язувати спрацьовування сигналів із певним сценарієм поведінки всієї системи безпеки. Наприклад, спрацювання датчика руху уночі одночасно викликає повертання камери у сторону датчика, перехід записування з дискретного на безперервний режим, блокування дверей проходу і подання сигналу на пульт охорони зміни. Пожежні датчики слід пов'язати з системою пожежогасіння і гучного зв'язку оповіщення персоналу.

2.2.5. Система зберігання

Система зберігання (сховище матеріальних цінностей) надто залежить від типу організації. Очевидно, що для банку, який проводить операції з готівкою, потрібні одні типи сейфів, а для компанії з розробки програмного забезпечення – зовсім інші. У будь-якому випадку необхідно визначитися з фізичним об'ємом об'єктів, що зберігаються, стійкістю сховища до фізичного чи електронного злому, пожежостійкістю, прихованістю монтажу тощо.

2.3. Організація роботи з персоналом

Методична робота з персоналом є дуже важливим профілактичним заходом у плані інформаційної безпеки.

Говорячи про безпеку персоналу, необхідно розділяти два поняття –

безпека самого персоналу як людського й інформаційного ресурсу і захист від персоналу як джерела чи основи зловмисних дій щодо інформаційних систем.

Напади, загрози, шантаж та інші дії зловмисників щодо персоналу – це об'єкт кримінального права й у загальному випадку знаходиться в компетенції уповноважених державних органів, з якими служба інформаційної безпеки організації може співробітничати, і у будь-якому випадку відіграють другорядну роль. Для конкретної організації ситуація може бути інша, і такі питання будуть вирішуватися власною службою безпеки.

Інший погляд автори мають на персонал як можливе джерело зловмисних впливів на інформаційну безпеку підприємства, коли некомпетентність, помилки, недбалість чи інші дії персоналу послужили основою загрози безпеці організації. Причому загрози безпеці через некомпетентність і низьку кваліфікацію персоналу залежно від регіону, соціального складу й інших причин, можуть мати значимість не меншу, а іноді й більшу, ніж загрози безпеці через злий намір.

2.3.1. Прийом на роботу

Початок аналізування складу персоналу починається, відповідно, з етапу прийому на роботу. Підрозділ для роботи з персоналом має власні критерії добору людей, але служба безпеки може і повинна брати у цьому активну участь. Таке оцінювання складається з двох частин – попереднього досвіду і поточної кваліфікації.

Що стосується попереднього досвіду, то тут повинні бути відпрацьовані системи збору інформації (професійний досвід, знання, персональні якості, характеристики з колишніх місць роботи як офіційні, так і неформальні), можливо, контакти зі службою безпеки з колишнього місця роботи кандидата; аналізу інформації – які якості є позитивними, а які негативними. Скажімо, готовність кандидата поділитися особливостями організації виробництва на колишньому місці роботи – це позитивна чи негативна характеристика? З одного боку, від нього очікується, що весь накопичений досвід він застосує на новому місці, з іншого боку – де гарантія, що при черговій зміні місця роботи він не буде розповідати про ту організацію, куди тепер приймається на роботу?

Поточний статус кандидата повинен перевірятися з погляду його технічної підготовки і здатності працювати з інформаційними системами, а також психологічного складу і рис характеру для виявлення тенденцій розвитку особистості (у тому числі як зловмисних, так і тих, що створюють незручності при спілкуванні в колективі). Можлива участь у цьому процесі штатного чи запрошеного психолога.

Одним із прикладів простого тесту для перевірки здібностей кандидата є тест на пароль. Для цього необхідне невелике програмне забезпечення, що імітує запрошення до введення пароля в інформаційну систему, зберігає пароль і може продемонструвати його представнику служби безпеки. Можливо, перед іспитом кандидату варто дати

ознайомитися з вимогами організації щодо паролів користувачів. Далі кандидату пропонується придумати і ввести власний пароль (наприклад, мотивуючи тим, що йому буде надана можливість тестової роботи в системі). Після введення пароля можна попросити кандидата ще раз ввійти в систему, але при цьому система видасть йому повідомлення про помилку з пропозицією звернутися в службу безпеки, або повідомить, наприклад, що час його останнього входу не відповідає тому, що реально було зроблено тільки що, чи що з часу останнього входу було дві-три спроби введення невірного паролю. Факторами, що насторожують, у даному випадку є такі:

- занадто довгі міркування при придумуванні пароля. Комбінацію з букв, цифр і спецсимволів нормальний користувач з досвідом роботи в інформаційних системах зможе придумати за 30-60 секунд або узагалі використати один зі своїх старих паролів. Довгі роздуми швидше за все означають, що кандидат уперше зіштовхується з такими вимогами до безпеки і, можливо, надалі він буде відчувати труднощі з їх дотриманням. Правда, довгі роздуми можуть означати, що він дійсно винаходить складний пароль, але це можливо буде перевірити після його введення;
- спроби запиту підказок пароля типу "Допоможіть мені підібрати пароль". Це означає, що користувач не усвідомлює важливість збереження паролю в секреті. Додатковою перевіркою може послужити провокація, наприклад: "Скажіть, який пароль ви зараз ввели?" - адже кандидат попереджений, що одержує вхід у систему, нехай і в тестовому режимі;
- помилки при підтвердженні паролю. Якщо користувач не може зосередитися настільки, щоб два рази ввести однакову комбінацію з 10-15 символів, то це може бути негативним знаком. При цьому варто робити поправку на можливе хвилювання кандидата при перевірці;
- занадто простий введений пароль. Якщо кандидат, ознайомившись з вимогами організації до паролів, все-таки ігнорує їх, сподіваючись, що пароль не буде нікому відомий, то це також негативна тенденція;
- відсутність реакції на тривожні повідомлення системи при подальшому вході в неї. Якщо система проінформувала користувача про помилку при введенні паролю, а потім пропустила його, і, також, дала невірну дату/годину останнього входу чи повідомила про невірні введення паролю, яких не було з боку користувача, – це всі сигнали, про які кандидат повинен проінформувати службу безпеки.

Якщо кандидат прийнятий на роботу і стає реальним користувачем – суб’єктом інформаційного простору, то служба інформаційної безпеки повинна забезпечити собі правовий простір для подальшої роботи з даним користувачем, у тому числі для випадків можливого переслідування даного користувача при виявленні з його боку порушень. Для цього необхідно вжити такі заходи:

- ознайомити з діючими нормативними документами (правилами,

інструкціями, методичними вказівками тощо) у сфері інформаційної безпеки і впевнитися, що надалі він не пошлеться на їхнє незнання, у тому числі взяти підписку;

- якщо кандидат укладає з організацією контракт, то в нього, без сумніву, повинен увійти ряд положень з інформаційної безпеки, особливо якщо вони не відображені адекватно в законодавстві держави. Наприклад, що суб'єкт зобов'язується визнавати цифровий підпис керівника нарівні зі звичайним підписом на папері;
- якщо організація висуває підвищені вимоги до збереження конфіденційності своєї інформації, можливо, це також необхідно включити в список положень, що підписується суб'єктом. При цьому слід дотримуватися діючого законодавства країни, для того щоб покладені на суб'єкта зобов'язання не порушували його конституційних прав;
- якщо організація збирається використовувати елементи втручання в приватні розділи робочої діяльності співробітника, наприклад, регулярно чи вибірково перлюструвати його електронну пошту чи відслідковувати відвідування інтернет-сайтів, то працівник повинен бути, як мінімум, про це попереджений;
- якщо співробітнику надається в його розпорядження персональний комп'ютер, то необхідно довести до співробітника, що дана одиниця техніки залишається власністю організації, а отже, організація буде визначати політику його використання. При цьому установка на комп'ютер ігор, навчальних програм, музики і відеофільмів найчастіше не входить у мету організації. А оскільки даний співробітник стає відповідальним за даний комп'ютер, він повинен забезпечувати у рамках своїх можливостей відповідність вимогам нормативів, у тому числі з інформаційної безпеки.
- якщо за даним персональним комп'ютером буде працювати два і більше чоловіки, то доцільно призначити одного, найбільш підготовленого, відповідальним за дотримання вимог інформаційної безпеки на даному комп'ютері.

2.3.2. Методична робота з персоналом

Незважаючи на будь-яку кваліфікацію користувача, оскільки розвиток інформаційного простору підприємства не стоїть на місці, необхідне регулярне навчання співробітників як роботі в нових інформаційних системах, так і заходам безпеки в цих системах. Крім того, розвиток злочинної частини світового інформаційного простору може потребувати від користувачів додаткових більш-менш кваліфікованих знань з низки атак (наприклад, як у випадку з відомим вірусом Kournikova – відрізняти розширення jpg від jpg.vbs). Це значить, що варто продумати систему оперативного оповіщення співробітників про необхідні заходи, а також можливе проведення регулярних семінарів для всіх чи найбільш підготовленої частини співробітників. Для великих розгалужених

корпорацій бажано застосовувати спосіб підготовки детальних методичних матеріалів, їхнього розсилання й обов'язкового ознайомлення співробітників з ними.

Як би старанно і якісно не працювали співробітники, періодично доводиться перевіряти їхню діяльність. Перевірки можуть бути вибірковими чи регулярними, їхній діапазон може сягати від аналізу реєстраційних журналів даної конкретної інформаційної системи до повного сканування вмісту твердого диска і зовнішніх носіїв користувача. При таких перевірках, як видно, будуть періодично виявлятися якісь порушення в роботі користувачів, у тому числі і з їхньої вини. Проведення розслідування інцидентів, визначення ступеню залежності провини користувача в тому чи іншому порушенні і розмір покарання повинні визначати уповноважені особи конкретної організації.

Хотілося б дати одну пораду: не завжди суворе покарання навіть за маленьку провину – це гарне рішення проблеми. З досвіду відомо, що навіть при інформованості користувачів про те, що їхня діяльність – це предмет спостереження відповідних служб, значна частина з них однаково буде намагатися шукати дрібні вигоди для себе в процесі своєї робочої діяльності. Можливо, це буде відвідування розважальних сайтів у Інтернеті чи установка комп'ютерних ігор. У таких випадках нагадування у вигляді електронного листа з таким, наприклад, змістом: "Учора ви відвідали сайт www.xxx.com і провели на ньому 42 хвилини робочого часу. Рекомендуємо вам для уникнення неприємностей не відвідувати сайти, не пов'язані з вашою робочою діяльністю. Служба безпеки" – буде гарною профілактикою розвитку зловживання корпоративними ресурсами.

Однак, навіть якщо даний незначний інцидент формально "вичерпаний", проте він повинен бути зафіксований у деякому "чорному списку", куди вносяться всі порушення інформаційної безпеки користувачем з першого дня роботи. Такий документ корисний. *По-перше*, користувачі схильні забувати про свої порушення (у цьому випадку даний документ буде корисний при деякому переповненні списку дрібних порушень, умовно прощених для цього користувача). *По-друге*, за допомогою даного документа можна відслідковувати тенденції розвитку роботи користувача з погляду інформаційної безпеки.

Дрібною, проте важливою деталлю є питання ідентифікації працівника при міжособистісному спілкуванні. В організації, що нараховує декілька десятків чоловік, фахівець з безпеки може знати кожного співробітника особисто, але у великій організації, де персонал складає 1000 і більше чоловік, питання розпізнавання особистості, особливо для нових працівників, стануть уразливістю, що може бути використана, наприклад, засобами соціальної інженерії.

Найпростішим прикладом є звертання користувача телефоном з проханням заміни пароля з тієї чи іншої причини. Яким чином перевірити відповідність реального користувача названому username? Якщо

користувач знаходиться неподалік, найбільш простий спосіб – запросити його прибути до адміністратора з документами, що підтверджують особистість. До речі, для цього гарним корпоративним стандартом вважається носіння на грудях пізнавального пропуску з необхідною інформацією (бажано продумати питання перешкодження їхньої підробки). Але що ж робити, якщо користувач географічно віддалений від адміністратора, а питання бізнесу вимагають забезпечення негайного початку роботи в інформаційній системі? У цьому випадку вступає в дію система тимчасових паролів для одноразового входу (з негайною заміною), для якої в Інтернеті напрацьовані два основних варіанти розв'язання проблеми.

1. *Контрольне питання*. При реєстрації в обліковий запис користувача, доступ до якого є тільки в адміністратора, заноситься питання і відповідна відповідь, які відомі тільки даному користувачу. Таким чином, перед зміною пароля адміністратор автентифікує користувача за відповіддю на контрольне питання. Якщо система дозволяє, варто зберігати кілька питань для одного користувача, також варто змінювати питання після їхнього використання.

2. *Альтернативний зворотний зв'язок*. Після звертання користувача адміністратор фіксує номер телефону і, перевіривши коректність номера, передзвонює користувачу сам. Крім того, тимчасовий пароль висилається користувачу електронною поштою, можливо, навіть не самому користувачу, а його безпосередньому керівнику.

Варто тільки врахувати важливість того, щоб тимчасовий пароль був досить унікальним, для того щоб у кожний конкретний момент не було відомо про те, який тимчасовий пароль використаний для даного працівника.

2.3.3. Організація роботи персоналу

Посадові інструкції персоналу. Для персоналу, допущеного до роботи в ІС, повинні бути посадові інструкції, в яких встановлюються обов'язки і відповідальність за забезпечення інформаційної безпеки згідно з прийнятою політикою.

В інструкціях необхідно відобразити як загальну відповідальність за втілення в життя чи підтримку політики безпеки, так і конкретні обов'язки щодо захисту конкретних ресурсів чи відповідальність за виконання певних процедур і дій для захисту. При розробці інструкцій рекомендується враховувати такі аспекти:

- робота з носіями інформації;
- знищення носіїв інформації.

Робота з носіями інформації. Повинні бути підготовлені інструкції для роботи зі всіма носіями конфіденційних даних: документів, магнітних стрічок, дисків, звітів тощо. В інструкції слід розглянути:

- правила роботи з носіями інформації та їх маркування;

- реєстрацію отримувачів даних, що мають відповідні повноваження;
- забезпечення повноти вхідних даних;
- підтвердження отримання переданих даних (при необхідності);
- надання доступу до даних мінімальній кількості осіб;
- маркування всіх копій даних для отримувача, що має відповідні повноваження;
- вчасне поновлення списків отримувачів з правом доступу до даних.

Знищення носіїв інформації. Повинні бути інструкції для знищення носіїв інформації. Пропонуються такі рекомендації.

Носії даних, що вміщують конфіденційну інформацію необхідно знищувати шляхом спалювання чи подрібнення (паперових носіїв) або стирати (для магнітних носіїв) при повторному використанні.

Для ідентифікації носіїв даних, які можуть потребувати знищення, пропонуються спеціальні ідентифікатори.

У деяких випадках буде простіше знищити всі непотрібні носії даних, ніж пробувати виділити з них носії, на яких записана конфіденційна інформація.

Кожний випадок видалення носіїв конфіденційної інформації необхідно (при можливості) реєструвати у контрольному журналі.

При накопичуванні інформації, яка підлягає видаленню, слід враховувати, що часто велика кількість несекретної інформації вміщує більш важливу інформацію, ніж мала кількість секретної інформації.

2.3.4. Адміністрування інформаційних систем

Адміністратор інформаційних систем повинен забезпечувати надійну роботу ІС і відповідність вимогам інформаційної безпеки.

Обов’язки адміністратора ІС і процедури щодо адміністрування повинні бути викладені у посадовій інтрукції.

Повинні бути описані інструкції щодо виконання кожного завдання, в тому числі:

- допустимі процедури оперування з файлами даних;
- вимоги до планування виконання завдань;
- інструкції з обробки помилок та інших виняткових ситуацій, які можуть виникнути при виконанні завдання, в тому числі обмеження на використання системних утиліт;
- звертання за допомогою у випадку виникнення технічних та інших проблем, пов’язаних з експлуатацією ІС;
- порядок отримання вихідних даних і забезпечення їх конфіденційності, включаючи процедури надійного видалення вихідної інформації у випадку збоїв завдань;
- процедури перезапуску і відновлення працездатності систем, використовувані у випадку їх відмови.

Повинні бути підготовлені інструкції для роботи щодо обслуговування систем, пов’язаних з адмініструванням ІС, в тому числі

процедури запуску і зупики ІС, резервне копіювання даних, технічне обслуговування обладнання.

2.3.5. Робота з представниками сторонніх організацій

Залучення представників стороніх організацій до роботи ІС може привести до додаткового ризику порушення режиму інформаційної безпеки.

Необхідно завчасно виявити такий ризик і вжити заходи для його зменшення. Слід розглянути такі питання:

- виявлення особливо вразливих чи надто важливих додатків, винесення яких за межі організації небажане;
- отримання санкції на використання додатків від їх власника;
- викладення в інструкціях правил роботи з представниками сторонніх організацій, перевірка дотримання вимог інформаційної безпеки.

2.3.6. Колишній кадровий склад підприємства

Інший важливий момент – взаємини зі співробітником, що збирається залишити організацію. Природно, повинні бути проведені деякі технічні заходи щодо блокування чи видалення облікових записів даного співробітника як користувача інформаційних систем. Але для цього служба безпеки, як мінімум, повинна бути оповіщена про майбутнє звільнення співробітника. Також у цій ситуації необхідний контакт із підрозділом роботи з персоналом.

Для ряду співробітників, що звільняються, а можливо і для всіх, доцільно проводити співбесіди, у ході яких нагадати про продовження дії зобов'язань, узятих на себе співробітником стосовно організації (якщо укладені контракти і домовленості не втрачають своєї сили при звільненні співробітника). Можливо залишаються ще які-небудь додаткові зацікавленості співробітника, що йде з організації. У будь-якому випадку краще зберегти гарні відносини між співробітником, що звільняється, і організацією.

Служба безпеки організації повинна розробити лінію поведінки відносно запитів щодо характеристик на колишніх співробітників організації, що влаштовуються на роботу на нове місце. Можливо, підприємство вважає, що воно не повинно надавати такі відомості, але тоді варто врахувати, що і на аналогічний запит самого підприємства на нового кандидата може надійти відмова. З загальних міркувань доцільніше організувати взаємодію між службами безпеки підприємств галузі, попередньо визначивши перелік даних, що можуть бути повідомлені колегам. Подібне співробітництво при правильній організації дозволить тільки поліпшити стан інформаційної безпеки окремого підприємства.

2.4. Організація роботи з документами

У комплексі організаційних заходів, що проводяться з метою підвищення ефективності захисту інформації, важливе значення належить розробці та затвердженню проектної і експлуатаційної документації.

До складу розроблюваної документації входять:

- проектна документація розробника системи (підсистеми, компоненти) захисту інформації;
- порадник (посібник) користувача;
- порадник адміністратора захисту інформації;
- порадник з тестування системи захисту інформації.

Проектна документація розробника системи (підсистеми, компоненти) захисту інформації складається з опису:

- системи захисту інформації;
- моделі захисту (формальної чи неформальної);
- концепції захисту;
- інтерфейсу системи захисту інформації і користувача, а також інтерфейсів між окремими модулями системи захисту інформації;
- застосовуваних засобів захисту;
- результатів аналізу та ідентифікації таємних каналів передавання інформації;
- таблиці відповідності формальних специфікацій і об'єктних кодів версій програмних компонентів системи захисту інформації.

Порадник користувача повинен містити короткий опис механізмів захисту та інструкцій для роботи з ними в процесі взаємодії користувача та інформаційної системи.

Порадник адміністратора захисту інформації використовується при виконанні функціональних обов'язків ним чи співробітниками служби захисту інформації в інформаційній системі і повинен складатися з таких документів:

- описів контрольованих функцій системи захисту інформації;
- інструкції з управління захистом, управління і контролю за привілейованими процесами при функціонуванні інформаційної системи;
- описів процедур роботи з засобами реєстрації;
- інструкції з супроводження копій програмного забезпечення системи захисту інформації, перевірки їх працездатності та тестування;
- інструкції з генерації нової версії після модифікації;
- опису процедури старту;
- опису процедур верифікації захищеності після старту (збоїв);
- опису процедур оперативного відновлення роботи системи захисту інформації.

Порадник з тестування системи захисту інформації повинен включати документацію розробника для оцінювання захищеності, яка містить повний опис порядку тестування і тестових процедур механізмів системи захисту, а також результатів функціонального тестування рівня захищеності інформації.

До документування систем захисту інформації висувають три групи вимог: протоколювання, тестування програм і обробка загроз.

При розробці системи *протоколювання* слід ураховувати такі специфічні вимоги:

- необхідність записів усіх переміщень захищуваних даних;
- можливість відтворення, при необхідності, ретроспективи використання захищуваного об'єкта, для реалізації якої забезпечується запам'ятовування станів програми і навколишнього середовища;
- накопичення статистики за протоколами використання інформації у системі.

Істотною особливістю тестування програм системи захисту інформації повинна бути наявність спеціальної програми генерації фальшивих адрес, несанкціонованих спроб доступу до даних, моделювання збійних ситуацій та інших специфічних властивостей. При тестуванні систем захисту інформації необхідно також звернути увагу на ретельну перевірку таблиць безпеки, системи паролів і програм доступу.

Система захисту інформації повинна мати спеціальне програмне забезпечення обробки загроз, яке включає в себе:

- реєстрацію подій у системному журналі, захищеному від спроб зміни зі сторони програм користувачів;
- використання зібраних відомостей для проведення аналізу відносно якісного розв'язання проблеми захисту інформації та розробки заходів щодо її удосконалення.

Одним іх основних засобів контролю, що сприяє запобіганню можливих порушень у інформаційній системі, є ***системний журнал***, у якому оперативно фіксуються події, що відбуваються у системі, наприклад:

- введені команди та імена виконуваних програм;
- доступ до визначених наборів даних чи пристроїв і його параметри;
- вхід/вихід користувачів із системи;
- ім'я терміналу чи іншого пристрою, з якого було здійснено введення команди чи запуск програми;
- чи виникали подібні події раніше і хто(що) був їх причиною;
- інші події.

Аналіз вмісту системного журналу може допомогти виявити засоби і апріорну інформацію, використані зловмисником для здійснення порушення. Адже очевидно, що без попередньої інформації будь-яка свідома спроба порушення обов'язково приречена на провал. До такої інформації можна віднести:

- дані про інформаційну систему;
- відомості про структуру організації;
- знання параметрів входу в систему (імена і паролі);
- інформація про використовуване обладнання і програмне забезпечення;

- характеристики сеансів роботи тощо.

Окрім того, аналіз вмісту системного журналу може допомогти визначити, як далеко зайшло порушення, підказати метод його розслідування і способи виправлення ситуації.

Природно, за допомогою одного системного журналу не завжди вдається визначити джерело порушення, проте він, без сумніву, дозволяє значно звузити коло підозрюваних.

На додаток до перелічених заходів ***рекомендується обов'язковий контроль таких подій за допомогою системного журналу:***

- події типу "помилка входу" чи "спроба проникнення" (якщо "помилка входу" фіксується надто часто – більше трьох разів підряд). Це кращий спосіб розпізнавання спроб проникнення у систему;
- події типу "вхід у систему". Допомагає контролювати роботу, особливо при доступі до вузла з мережі. Такий доступ є джерелом підвищеної небезпеки;
- події типу "помилка при доступі до набору даних". Дає можливість виявити спроби подолання захисту найбільш цінних об'єктів інформаційної системи;
- запис (доступ типу WRITE) у набори даних. Допомагає запобігти їх несанкціонованій модифікації. При цьому слід урахувати особливості модифікації деяких системних наборів;
- здійснення дій, на які потрібні різного роду привілеї. Дає можливість виявити зловживання ними.

2.5. Організація використання технічних засобів

Безпека устаткування також складається з варіантів, коли устаткування саме є загрозою і коли устаткування є об'єктом, на який спрямована загроза.

Коли організація купує устаткування інформаційних технологій, вона змушена йому довіряти, тому що в більшості випадків організація не має достатньої кількості ресурсів для аналізування складної техніки на відсутність недокументованих можливостей – апаратних закладок (англ. hardware backdoor). Причини виникнення таких закладок – це питання конкуренції між підприємствами чи політики окремих держав, але у будь-якому випадку воно поза розглядом даного посібника. Навіть якщо в організації є кваліфіковані фахівці з інформаційних технологій чи інформаційної безпеки, вони не візьмуть на себе сміливість підтверджувати чи спростовувати наявність апаратних закладок. На відміну від методик і засобів виявлення програмних закладок у більшості випадків для аналізу апаратного забезпечення необхідні спеціальні лабораторії і персонал високої кваліфікації.

З цієї причини устаткування необхідно купувати тільки після сертифікації уповноваженим органом держави або, якщо такий орган відсутній, у відомих виробників (брендів), що дорожать репутацією і не зацікавлені у скандалах з приводу апаратних закладок у їхній техніці. У

даному випадку збільшення ціни устаткування – це плата за гарантію відсутності “п’ятої колони” усередині підприємства.

Якщо припустити, що в устаткуванні немає вбудованих зі злим наміром недокументованих можливостей, воно, проте, може бути уразливим щодо інформаційної безпеки. Найчастіше в зв’язку з такою уразливістю вживають термін ПЕМВІН—побічне електромагнітне випромінювання і наведення (англ. side-channel). Дане явище ґрунтується на тому, що при своїй роботі устаткування неконтрольовано виділяє у навколишній простір деяку інформацію у тому чи іншому вигляді, причому, цю інформацію можна перехопити, обробити і використовувати несанкціоновано. Найбільшу увагу в інформаційних технологіях привертають ПЕМВІН, що виникають у середовищах передачі даних (проводах, кабелях тощо) і генеровані при роботі моніторів користувачів. Однак, перш ніж купувати складне і дороге устаткування для захисту від ПЕМВІН, варто зробити аналіз ризиків.

Можливо, досить забезпечити шифрування даних при передачі лініями зв’язку, у цьому випадку не тільки складна апаратура уловлювання електромагнітних наведень, але і пряме впровадження перехоплювача пакетів нічого не дасть зловмиснику.

Для віддаленого перехоплення інформації з екрана монітора потрібно дуже дороге і складне устаткування. А що отримає самий злісний конкурент, якщо він навіть зможе заглядати через плече найголовнішому системному адміністратору? Можливо, він зможе отримати цю інформацію більш легким і простим шляхом.

Варто врахувати, що, звичайно, аналізуються ризики для середнього підприємства. Якщо говорити, наприклад, про установи міністерства оборони, де в електронному вигляді зберігається інформація класу "державна таємниця", то міркування будуть, звичайно, зовсім іншими.

Припустимо, забезпечена ситуація коли все устаткування організації функціонує надійним і довіреним способом. Однак є можливість впровадження в інформаційний простір підприємства стороннього устаткування, принесеного співробітниками і відвідувачами.

У даному випадку оборону необхідно ешелонувати двома ступінями: контролювати внесення устаткування в будинок організації і перевіряти відсутність сторонніх включень в інформаційну мережу. І для першого, і для другого способів існують різні засоби і методи – від візуального огляду до автоматизованого виявлення.

На окрему увагу заслуговують, у даному випадку, зовнішні носії (які також можна віднести до устаткування), а, також, засоби для зчитування/записування на зовнішні носії і порти для зовнішнього підключення таких пристроїв. У даному випадку зовнішні носії можуть бути засобом доставки шкідливих інформаційних об’єктів/суб’єктів в інформаційний простір підприємства і засобом вилучення конфіденційної інформації з інформаційних об’єктів підприємства.

Найбільш надійним, хоча і непростим, рішенням буде фізичне відключення/видалення пристроїв зчитування/записування і

блокування/від-ключення вільних портів (COM, LPT, USB, інфрачервоний зв'язок тощо). При цьому є необхідним створення окремої служби, у розпорядженні якої залишиться один чи кілька пристроїв роботи з зовнішніми носіями. Фізично розміщувати цю службу доцільно недалеко від входу в будинок, для того щоб усі внесені і зовнішні носії, що виносяться, могли бути надані її співробітникам. У функції служби буде входити:

- перевірка відсутності на принесеному зовнішньому носії шкідливих елементів (вірусів, троянських програм, стороннього програмного забезпечення);
- копіювання чи електронна доставка інформації з принесеного зовнішнього носія на робочу станцію чи сервер, у розпорядження того користувача, для якого інформація призначена;
- отримання від користувача інформації, призначеної до виносу з організації на зовнішньому носії;
- перевірка відсутності в інформації для виносу конфіденційних даних і запису інформації на зовнішні носії.

Єдиним допустимим виключенням для цієї служби може бути тільки служба регулярного резервного копіювання критичної інформації з окремим регламентом роботи.

Закінчуючи розмову про зовнішні носії, необхідно згадати про проблему стирання інформації з зовнішніх носіїв після того, як інформація була доставлена за призначенням. Питання витрат на можливе відновлення нібито знищеної інформації з зовнішнього носія – це питання вартості самої інформації, яку необхідно відновити. У будь-якому випадку варто враховувати, що багаторазовий перезапис чи фізичне руйнування корпусу, чи навіть записуваної поверхні – це ще не гарантія неможливості відновлення. Якщо питання про гарантоване знищення інформації досить гостре, то варто проаналізувати можливість придбання спеціальної апаратури. При цьому необхідно розрізняти апаратуру з повним руйнуванням зовнішнього носія і з можливістю його подальшого використання.

Іншою важливою особливістю устаткування інформаційних технологій є наявність великої кількості дрібних деталей, що володіють рядом неприємних для інформаційної безпеки якостей:

- вони самооцінні, тобто мають окрему вартість стосовно іншого устаткування;
- співвідношення ціна/маса/розмір деяких деталей у певні періоди розвитку ринку перевищує аналогічне співвідношення, наприклад, навіть для золота;
- вони можуть бути замінені на схожі деталі гіршої якості і меншої вартості, при цьому заміна не буде очевидною для кінцевого користувача;
- вони користуються стійким попитом на ринках, де не вимагаються документи, що підтверджують легальне походження даних деталей.

Найбільш яскравим прикладом у даному випадку можуть бути плати оперативної пам'яті. Тільки кваліфікований користувач зможе помітити відмінність у роботі комп'ютера з 128 чи з 96 Мбайтами оперативної пам'яті. Таким чином, пропажа чи підміна може бути не виявлена досить довго, до чергової докладної інвентаризації (при відсутності автоматизованих засобів інвентаризації). Прийнятним засобом зниження даного ризику буде використання кожухів для приховання дрібних деталей (практично у всього устаткування такі кожухи наявні) і опечатування кожухів печаткою уповноваженого підрозділу – скажімо, інформаційної безпеки чи технічної підтримки. При цьому важливо, щоб цілісність печатки регулярно перевірялася самим користувачем устаткування, в іншому випадку ця міра буде носити лише фіктивний характер.

2.6. Організація фізичного захисту і контроль за дотриманням режиму захисту інформації

Контроль доступу в приміщення і загальні заходи для захисту обладнання є складовою частиною заходів щодо забезпечення захисту інформації. Обладнання і критично важливі чи уразливі елементи системи повинні бути розміщені в захищених місцях, обмежені периметром безпеки, з надійним контролем. Для зменшення ризику несанкціонованого доступу чи ушкодження документації і носіїв інформації рекомендується задати правила використання робочого столу.

Забезпечення конфіденційності. Користувачі інформаційних ресурсів організації повинні підписати зобов'язання про збереження кофіденційності. Особливу увагу слід приділити процедурі надання доступу до інформаційних ресурсів користувачам із сторонніх організацій. Для цього повинні бути розроблені спеціальні правила.

Журнали реєстрації подій. Необхідно підготувати журнал реєстрації виконуваних завдань, які будуть вести оператори ІС. У цьому журналі слід фіксувати:

- час запуску і зупинки систем;
- системні помилки, збої і вжиті заходи.

Забезпечення захисту документації ІС. Документація ІС може містити описання прикладних процесів, структур даних і процесів підтвердження повноважень. У цьому випадку система повинна бути захищена від несанкціонованого доступу. Рекомендуються такі засоби контролю:

- список осіб з правом доступу до документації повинен бути максимально обмежений, а дозвіл на її використання повинен видаватися власником додатків до документації;
- друковані матеріали, створювані у процесі роботи ІС, слід зберігати окремо від інших документів і розповсюджувати на них правила обмеження доступу.

Доступ до носіїв інформації та їх захист. Необхідно організувати контроль доступу до носіїв інформації і забезпечити їх фізичний захист. Для доступу до носіїв з конфіденційною інформацією необхідно мати

затверджені правила. При організації системи доступу слід враховувати таке:

система ідентифікації носіїв повинна бути такою, щоб за мітками, використовуваними для їх ідентифікації, не можна було визначити характер і зміст інформації, яка зберігається на носіях;

- необхідно вчасно видаляти непотрібний вміст повторно використо- вуваних носіїв інформації;
- винесення носіїв інформації зі сховища необхідно фіксувати в контрольному журналі;
- зберігати всі носії інформації в надійному захищеному місті згідно з інструкціями.

Всі процедури і рівні повноважень повинні бути задокументовані.

Контрольні питання

1. Дайте означення поняттям "організація захисту інформації" та "організаційні заходи".
2. Наведіть класифікацію організаційних заходів захисту інформації.
3. Опишіть задачі організації заходів захисту інформації.
4. Розкажіть про способи оперативного розв'язання задач захисту інформації.
5. Наведіть класифікацію задач організації режиму і охорони на підприємстві.
6. Поясніть суть системи охорони периметра.
7. Розкрийте особливості системи управління доступом.
8. Охарактеризуйте механізм допуску на територію організації.
9. Поясніть суть принципів ідентифікації/автентифікації суб'єкта.
10. Опишіть особливості системи контролю переміщення суб'єктів на території і у приміщеннях організації.
11. Розкрийте задачі та умови застосування системи відеоспостереження.
12. Поясніть суть системи охоронної (пожежної) сигналізації та системи зберігання.
13. Обґрунтуйте необхідність проведення аналізу персонала.
14. Опишіть особливості проведення аналізу персонала при прийомі на роботу.
15. Розкажіть про порядок перевірки тестуванням здібностей кандидата на посаду користувача.
16. Охарактеризуйте фактори тестування, які можуть вплинути на рішення про прийняття на роботу.
17. Обґрунтуйте необхідність проведення регулярної методичної роботи з користувачами інформаційних систем.
18. Розкрийте особливості проведення розслідування порушень зі сторони користувача.
19. Опишіть особливості організації роботи персоналу.
20. Розкажіть про порядок адміністрування інформаційних

систем.

21. Наведіть класифікацію проектної та експлуатаційної документації з питань захисту інформації.
22. Поясніть порядок контролю захисту інформації за допомогою системного журналу.
23. Обґрунтуйте необхідність проведення аналізу обладнання на наявність програмних закладок.
24. Опишіть порядок проведення контролю зовнішніх носіїв інформації.
25. Розкажіть про особливості контролю за дотриманням режиму захисту інформації.

Глава 3. ОРГАНІЗАЦІЙНО-ПРАВОВІ ФОРМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

3.1. Основні поняття

Право *– це система або сукупність норм – правил поведінки та діяльності особи та інших суб'єктів правовідносин, що відображають найбільш важливі економічні, політичні, моральні, громадянські та інші соціальні відносини у формі правових звичаїв, державних законів і інших нормативно-правових актів, правових прецедентів, правових договорів, які:*

- встановлені державною владою, всім населенням (референдумом, віче тощо) або загальновизнані суспільством;
- виражають суб'єктивні права і обов'язки громадян, юридичних осіб, держави та інших суб'єктів, а також форм та засобів їх захисту;
- виражають принципи рівності та рівноправ'я всіх суб'єктів, міру справедливості, принцип юридичної (правової) свободи і відповідальності за нанесення шкоди і суспільної небезпеки, принцип істини і правди;
- є загальнообов'язковими для всіх суб'єктів суспільних відносин, охороняються державною владою і суспільством від порушень і направлені на охорону соціальних (матеріальних і духовних) цінностей з позицій потреб і інтересів всього суспільства і народу;
- направлені на розвиток і зміцнення демократії, особистості, громадянського суспільства, загального блага, правопорядку і правової держави.

Право є засобом існування, функціонування і розвитку держави, народу, всієї цивілізації. Воно виникає на певному історичному і культурному етапі розвитку, діалектично розвивається від неправди, свавілля до досконалого демократичного, загальнонаціонального, міжнародного і космічного права.

Зі стрімким розвитком інформаційних технологій, розширенням виробництва засобів і сфери застосування комп'ютерної техніки, а разом з цим і виникненням злочинності у сфері використання комп'ютерних технологій ("кіберзлочинність"), нагальною стала проблема створення інформаційного законодавства – галузі інформаційного права.

Інформаційне право – це система охоронюваних державою соціальних норм і відносин, які виникають в інформаційній сфері – сфері виробництва, перетворення, використання і зберігання інформації.

Правовий захист інформації – це спеціальні закони, інші нормативні акти, правила, засоби і заходи, що забезпечують захист інформації на правовій основі.

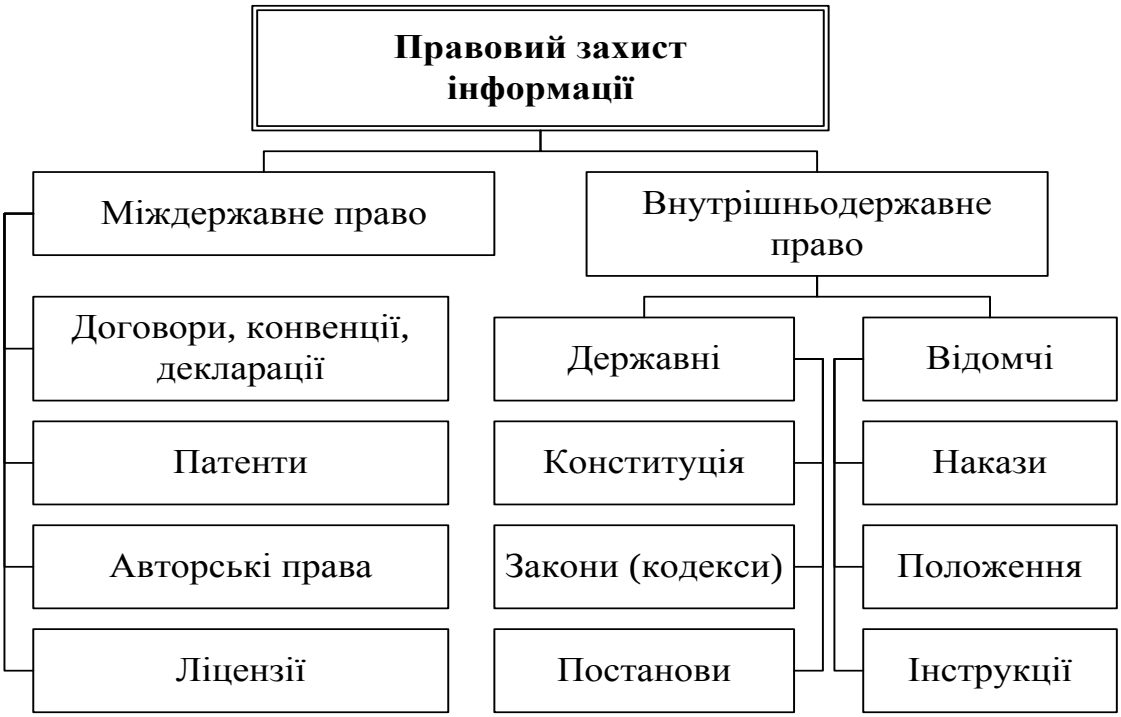

Рис. 6. Структура правового захисту інформації

Правовий захист інформації як ресурс визнаний на міжнародному, державному рівні і визначається міждержавними договорами, конвенціями, деклараціями та реалізується патентами, авторським правом і ліцензіями на їх захист. На державному рівні правовий захист регулюється державними і відомчими актами (рис.6).

У нашій країні такими правилами (актами, нормами) є Конституція України, закони України, цивільне, адміністративне, кримінальне право, викладені у відповідних кодексах. Щодо відомчих нормативних актів, то вони визначаються наказами, положеннями та інструкціями, що видаються відомствами, організаціями і підприємствами і діють у рамках певних структур.

Основу правового регулювання суспільних інформаційних відносин становить Конституція України, прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 року.

Розвиток положень Конституції України щодо регулювання суспільних інформаційних відносин відображений в конкретних нормах кодифікованих провідних галузей законодавства:

- Кримінальний Кодекс України від 5.04.2001 р. №2341-III;
- Кримінально-процесуальний кодекс України станом на 20.09.2001р.;
- Кримінально-виконавчий кодекс України від 11.07.2003 р. № 1129-IV;
- Цивільний кодекс України від 16.01.2003 р. №435-IV;
- Господарський процесуальний кодекс України від 6.11.1991р. №1798-XII;

- Кодекс України про адміністративні правопорушення станом на 20.06.2000 р.;
- Кодекс законів про працю України станом на 1.12.2000 р.;
- Господарський кодекс України від 16.01.2003 р. №436-IV;

Окремі норми суспільних інформаційних відносин містяться в:

- Митному кодексі України від 11.07.2002 р. №32-IV;
- Арбітражно-процесуальному кодексі України від 6.11.1991 р. №1798-XII;
- інших кодексах України;
- основах законодавства України щодо окремих галузей суспільних відносин.

Спеціальне законодавство щодо боротьби з комп'ютерною злочинністю базується на законодавстві провідних галузей права, у тому числі у сфері правоохоронної діяльності, і складається з законів, що визначають компетенції та функції окремих державних органів влади: прокуратури, міліції, служби безпеки, державної податкової служби. Також окремі положення боротьби з комп'ютерною злочинністю визначені у законодавстві України про оперативно-розшукову діяльність, про організаційні правові основи боротьби з організованою злочинністю, про боротьбу з корупцією, про оборону, про обмеження монополізму та недопущення недобросовісної конкуренції у підприємницькій діяльності, про захист від недобросовісної конкуренції, інших законодавчих актах, в яких визначаються компетенція та функції об'єктів інформаційних відносин.

3.2. Організація роботи з конфіденційною інформацією

3.2.1. Види конфіденційної інформації

За передбаченим правовими нормами порядком (режимом допуску) отримання, використання, поширення і зберігання інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Інформація з обмеженим доступом (ІзОД) за своїм правовим режимом поділяється на конфіденційну і таємну [1].

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно

визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту. Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої є загрозою життю і здоров'ю людей.

До ***таємної інформації*** належить інформація, що містить відомості, які становлять державну та іншу передбачену законом [3] таємницю, розголошення якої завдає шкоди особі, суспільству, державі у сферах:

- оборони;
- економіки, науки і культури;
- зовнішніх відносин;
- державної безпеки та охорони правопорядку тощо.

Конкретні відомості можуть бути віднесені до державної таємниці за ступенями секретності **"особливої важливості", "цілком таємно"** та **"таємно".**

Джерелами конфіденційної інформації є люди, документи, публікації, технічні носії інформації, технічні засоби забезпечення виробничої і трудової діяльності, продукція і відходи виробництва. Від того, як організована робота з людьми і документами, залежить і безпека підприємства.

3.2.2 Організація секретного діловодства

При роботі з важливими (таємними, конфіденційними тощо) *документами слід виконувати* такі вимоги:

- суворий контроль (особисто чи через службу безпеки) за допуском персоналу до секретних документів;
- призначення конкретних осіб з керівництва для організації і контролю секретного діловодства, наділення їх відповідними повноваженнями;
- розробка інструкції (пам'ятки) для роботи з секретними документами, ознайомлення з нею відповідних працівників;
- контроль за прийняттям співробітниками письмових зобов'язань про збереження таємниці;
- введення системи матеріального та іншого стимулювання службовців, що мають доступ до таємниці;
- впровадження в щоденну практику механізмів і технологій захисту важливих документів;
- особистий контроль зі сторони керівника організації служби внутрішньої безпеки і секретного діловодства.

Службовці, відповідальні за збереження, використання і вчасне знищення секретних документів, повинні бути захищені від спокуси

торгівлі секретами простим, проте радикальним способом – **гарною платою за роботу.**

У процесі зберігання і пересилання секретних документів можуть бути застосовані засоби захисту і сигналізації про несанкціонований доступ – невидиме світлочутливе покриття, що наноситься на документи, яке проявляється під дією світла, указуючи тим самим на факт несанкціонованого ознайомлення з документами чи їх фотографування.

Спеціалістам з питань захисту важливої інформації відомі й інші технології та системи охорони конфіденційних документів організації від несанкціонованого доступу чи можливого витоку охоронюваних відомостей.

Основні функції забезпечення безпеки інформації при роботі з секретними документами наведені у додатку 1.

До ведення секретного діловодства повинні притягатися особи, що пройшли спеціальну перевірку, і у чесності яких нема сумнівів. Окрім того, ці особи повинні бути відповідно підготовлені та навчені, так як професіональні недоліки і порушення робочих правил надто дорого обходяться організації

Приміщення, в яких проводиться робота з секретними документами, повинні добре охоронятися, а доступ туди повинен бути закритим для сторонніх осіб. Ці приміщення повинні мати міцні перекриття і стіни, підсилені металеві двері, міцні віконні рами з подвійним заскленням і ґратами, щільні штори. Сховище повинно бути обладнане охоронною і пожежною сигналізацією і пильно охоронятись. Не рекомендується розміщувати таке приміщення на першому і останньому поверхах будівлі. Секретні документи зберігаються у сейфах чи неспалимих металевих шафах з надійними замками.

Різні прийоми ведення секретного діловодства направлені на запобігання витоку секретів. Документи, що містять таємницю, розрізняються за ступенем секретності і постачаються відповідним грифом секретності.

3.2.3. Організація захисту комерційної таємниці

У статті 505 Цивільного кодексу України від 16.01.2003р. №435-IV наводиться поняття "***комерційна таємниця***". Згідно з цим документом до комерційної таємниці відноситься інформація, яка є секретною у тому розумінні, що вона в цілому чи у певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які, зазвичай, не мають справу з таким видом інформації, до якого вона належить. У зв'язку з цим така інформація має комерційну цінність та була предметом адекватних існуючих обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Майновими правами інтелектуальної власності на комерційну таємницю є:

- право на використання комерційної таємниці;
- виключне право дозволяти використання комерційної таємниці;
- виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці;
- інші майнові права інтелектуальної власності, встановлені законом.

Майнові права інтелектуальної власності на комерційну таємницю належить особі, яка правомірно призначила інформації гриф комерційної таємниці, якщо інше не встановлено договором.

Органи державної влади зобов'язані охороняти від добросовісного комерційного використання інформацію, яка є комерційною таємницею, створення якої потребує значних зусиль і яка надана їм з метою отримання встановленого законом дозволу на діяльність, пов'язану з фармацевтичними, сільськогосподарськими, хімічними продуктами, що містять нові хімічні сполуки. Ця інформація охороняється органами державної влади також від розголошення, крім випадків, коли розголошення необхідне для забезпечення захисту населення захисту населення або не вжито заходів щодо її охорони від недобросовісного комерційного використання.

Відповідальність за забезпечення режиму при роботі з матеріалами з грифом "Комерційна таємниця" ("КТ"), вчасне розроблення і здійснення необхідних заходів щодо збереження комерційної таємниці покладається на керівника організації, його заступників і керівників структурних підрозділів. Відповідальність за організацію і виконання роботи із захисту комерційної таємниці та проведення постійного контролю за її дотриманням покладається на службу безпеки.

Служба безпеки приймає заходи щодо збереження комерційної таємниці шляхом максимального обмеження кола осіб, фізичного зберігання документів, що містять такі відомості, оброблення інформації з грифом "КТ" на захищених ЕОМ, внесення вимог з конфіденційності конкретної інформації у договори з внутрішніми і зовнішньоторговими параметрами та інших заходів за рішенням керівництва.

Захист комерційної таємниці передбачає:

- порядок визначення інформації, що містить комерційну таємницю, і термінів її дії;
- систему допусків співробітників, приватних та осіб, що знаходяться у відрядженні, до відомостей, які містять комерційну таємницю;

- порядок роботи з документами з грифом “КТ”;
- забезпечення зберігання документів, справ і видань з грифом “КТ”;
- обов’язки осіб, допущенних до відомостей, що містять комерційну таємницю;
- принципи організації і проведення контролю за забезпеченням режиму при роботі з відомостями, що складають комерційну таємницю;
- відповідальність за розголошенням відомостей, втрату документів, що містять комерційну таємницю.

Контроль за здійсненням обміну, розмноження, зберігання і використання документів, справ і видань з грифом “КТ” покладається на уповноважених служби безпеки.

Контроль за нерозголошенням відомостей, що містяться у документах, справах і виданнях з грифом “КТ” здійснюється відділеннями служби безпеки.

3.3. Порядок визначення інформації, що містить комерційну таємницю, і терміни її дії

Визначення необхідності надання грифу “комерційна таємниця” проводиться на основі “Переліку конкретних відомостей, що складають комерційну таємницю”, затверджених і введених у дію наказом керівництва підприємства:

- на документі – виконавцем і особою, що підписує документ;
- на виданні – автором (укладачем) і керівником, що затверджує видання до друку.

Термін дії комерційної таємниці, що міститься у документі, визначається у кожному конкретному випадку виконавцем чи особою, що підписала документ, у вигляді конкретної дати чи “до укладення контракту”, чи “безстроково”.

На документах, справах і виданнях, що містить відомості, які складають комерційну таємницю проставляється гриф “комерційна таємниця”, а на документах і виданнях, окрім того, – номери примірників.

Гриф комерційна таємниця і номер примірника проставляється у правому верхньому кутку першої сторінки документу, на обкладинці, титульному листові видання і на першій сторінці супровідного листа до цих матеріалів.

На зворотній сторінці останнього листа кожного примірника документу, що містить комерційну таємницю, друкується помітка, в якій указується: кількість надрукованих примірників, номер, прізвище виконавця і його телефон, дата, термін дії комерційної таємниці, що міститься у документі (конкретна дата, до “укладення контракту” чи “безстроково”), прізвище оператора.

Вирішення питання про зняття грифу "комерційна таємниця" покладається на створену спеціальну комісію, до складу якої включаються представники служби безпеки і відповідних структурних підрозділів. Рішення комісії оформляється у довільній формі актом, який затверджується керівником організації чи його заступником. У акті перелічують справи, з яких гриф "комерційна таємниця" знімається. Один примірник акта разом зі справами передається в архів, а на справи постійного зберігання – у державний архів. На обкладинках справ гриф “комерційна таємниця” гаситься штампом чи записом від руки із зазначенням дати і номера акта на зняття грифу "комерційна таємниця".

Аналогічні відмітки вносяться у описи і номенклатури справ.

3.4. Допуск співробітників до відомостей, що складають комерційну таємницю

Допуск співробітників до відомостей, що складають комерційну таємницю, здійснюється керівником організації, його замісником і керівниками структурних підрозділів.

Керівники підрозділів і служби безпеки відповідальні за підбір осіб для роботи з відомостями з грифом “комерційна таємниця”, зобов’язані забезпечити систематичний контроль за тим, щоб до цих відомостей отримали доступ тільки ті особи, яким такі відомості потрібні для виконання службових обов’язків.

До відомостей, що містять комерційну таємницю, допускаються високоморальні ділові особи, здатні зберігати комерційну таємницю і тільки після оформлення у служби безпеки індивідуального письмового зобов'язання щодо зберігання комерційної таємниці.

Допуск співробітників до роботи зі справами з грифом “комерційна таємниця”, що мають до них безпосереднє відношення, проводиться згідно з оформленим на внутрішній стороні обкладинки списком за підписом керівника структурного підрозділу, а до документів – згідно вказівкам, що містяться у резолюціях керівників підрозділів.

Приватні особи та особи, що знаходяться у відрядженні, допускаються до ознайомлення і роботи з документами і виданнями з грифом “комерційна таємниця” за письмовим дозволом керівників організації і підрозділів, у віданні яких знаходяться ці матеріали, при наявності письмового запиту тих організацій, в яких вони працюють, з вказівкою теми і об’єму виконуваного завдання, а також розпорядження на виконання завдання.

Виписки з документів і видань, що містять відомості з грифом “комерційна таємниця” проводяться у зошитах, що мають такий же гриф, і після закінчення роботи представника надсилаються на адресу організації.

Справи і видання з грифом “комерційна таємниця” видаються виконавцям і приймаються від них під розписку в “Карточці обліку справ і видань, що видаються”.

3.5. Порядок роботи з документами з грифом “комерційна таємниця”

Документи з відомостями, що складають комерційну таємницю, підлягають обов’язковій реєстрації в канцелярії служби безпеки чи в загальному діловодстві підрозділу служби безпеки. Вони повинні мати реквізити, передбачені п.2.3, і гриф “КТ” (чи повністю “комерційна таємниця”). На документах, що передаються іноземцям, гриф “комерційна таємниця” не проставляється. Отримані від іноземців документи маркуються грифом “комерційна таємниця” графітовим олівцем.

У тексті документа і його реквізитах можуть бути додаткові застереження щодо права на інформацію, порядок користування нею, терміни обмеження на публікацію тощо.

Відсутність грифу “комерційна таємниця” і запобіжних застережень у тексті і реквізитах означає вільне розсилання і припускає, що автор інформації і посадова особа, що санкціонувала її розповсюдження, передбачили всі можливі наслідки від вільного розсилання і несуть за це всю повноту відповідальності.

Інформація з грифом “комерційна таємниця”, що надходить, приймається і розкривається працівниками канцелярії, яким доручена робота з цими матеріалами. При цьому перевіряється кількість списків і примірників документів і видань, а також наявність вказаних у супроводжувальному листі додатків.

У разі відсутності у конвертах (пакунках) документів з грифом “КТ” або додатків до них складається акт у двох примірниках, один з яких відправляється адресату.

Реєстрації підлягають вхідні та вихідні документи, а також видання з грифом “КТ”. Такі документи обліковуються за кількістю листків, а видання (книги, журнали, брошури) – за примірниками.

Облік документів і видань з грифом “КТ” ведеться у журналі (форма 1) чи на картках (форма 2) окремо від обліку іншої несекретної документації.

Листки журналів нумеруються, прошиваються і опечатуються. Видання, які не підшиваються у справи, обліковуються в журналі інвентарного обліку (форма 5).

Переміщення документів і видань з грифом “КТ” повинно вчасно реєструватися у журналах чи на картках.

На кожному зареєстрованому документі, а також на супровідному листі до видань з грифом “КТ” ставиться штамп, у якому указується найменування, реєстраційний номер документа і дата його надходження.

Тираж видання з грифом “КТ”, отриманий для розсилання, реєструється під одним вхідним номером у журналі обліку та розподілення видань (форма 3).

Додатково розмножені примірники документа (видання) обліковуються за номером цього документа (видання), про що робиться відмітка на розмноженому документі (виданні) і в облікових формах. Нумерація додатково розмножених примірників проводиться від останнього номера раніше облікованих примірників.

Друкування матеріалів з грифом “КТ” проводиться в бюро оформлення технічної документації чи у структурних підрозділах під відповідальність їх керівників.

Віддруковані та підписані документи з грифом “КТ” разом з їх чернетками і варіантами передаються для реєстрації працівнику канцелярії, який здійснює облік. Чернетки і варіанти знищуються цим працівником з підтвердженням факту знищення записом на копії вихідного документа: “Чернетка (і варіанти) знищені”. Дата. Підпис.

Розмноження документів і видань з грифом “КТ” у типографіях і на розмножувальних апаратах проводиться з дозволу служби безпеки і під контролем канцелярії за заявками, підписаними керівником підрозділу і затвердженими замісником керівника організації. Облік розмножених документів і видань здійснюється за примірниками у спеціальному журналі.

Розсилання документів і видань з грифом “КТ” здійснюється згідно з рознарядками, підписаними керівником підрозділу, з вказівкою облікових номерів примірників, що відправляються.

Документи з грифом “КТ” після їх виконання групуються в окремі справи. Порядок їх групування передбачається номенклатура ми справ несекретного діловодства. У номенклатуру справ обов’язково включаються всі довідкові картотеки, журнали і видання з грифом “КТ”.

При користуванні відкритим радіозв’язком забороняється передавати відомості, що мають гриф “КТ”. Такі відомості можуть передаватися тільки закритими технічними засобами зв’язку чи відкритим телетайпним звя’зком з поставленням на документах і телеграмах відповідного штампу.

При користуванні проводовим зв’язком забороняється вказувати посади адресантів, дозволяється вказувати тільки телеграфні адреси і прізвища відправників і отримувачів.

Зняття копій, а також проведення виписок з документів і видань з грифом “КТ” співробітниками робиться з дозволу керівників підрозділів.

Зняття копій для сторонніх організацій з документів і видань з грифом “КТ” робиться за письмовим запитом з дозволу керівників підрозділів, які підготували ці документи і видання.

Аналогічно вносяться відмітки в описи і номенклатури справ.

Порядок роботи на ЕОМ при обробці інформації з грифом “КТ” здійснюється відповідно до вимог “Інструкції про порядок роботи на ПЕОМ при обробці несекретної інформації”.

3.6. Забезпечення цілісності документів, справ і видань

Документи, справи і видання з грифом “КТ” повинні зберігатися в службових приміщеннях і бібліотеках у шафах, надійно закритих і опечатаних. При цьому повинні бути створені належні умови для забезпечення їх фізичної цілісності.

Видані для роботи справи з грифом “КТ” підлягають поверненню у канцелярію чи уповноваженому служби безпеки у той самий день.

Окремі справи з грифом “КТ” з дозволу начальника канцелярії чи уповноваженого служби безпеки можуть знаходитися у виконавця протягом строку, необхідного для виконання завдання, за умови забезпечення їх цілісності та дотримання правил зберігання.

Передача документів, справ і видань з грифом “КТ” іншим співробітникам, допущеним до цих документів, проводиться тільки через канцелярію чи уповноваженого служби безпеки.

Забороняється вилучення зі справ чи переміщення документів з грифом “КТ” з однієї справи в іншу без санкції канцелярії чи уповноваженого служби безпеки, який здійснює облік. Про всі проведені вилучення чи переміщення робляться відмітки в облікових документах, включаючи внутрішні описи.

Забороняється виносити документи, справи і видання з грифом “КТ” із службових приміщень для робот з ними вдома, у готелях тощо.

При необхідності керівник організації, його замісники чи керівники підрозділів можуть дозволити виконавцям чи співробітникам канцелярії винесення з будинку документів з грифом “КТ” для їх погодження, підпису тощо в організації, які знаходяться у межах даного міста.

Особам, відрядженим в інші міста, забороняється мати при собі на шляху переміщення документи, справи чи видання з грифом “КТ”. Ці матеріали повинні бути направлені завчасно на адресу організації за місцем відрядження співробітника, як правило, рекомендованими чи цінними відправленнями, а також з кур’єрами.

При заміні співробітників, відповідальних за облік і зберігання документів, справ і видань з грифом “КТ”, складається у довільній формі акт прийому – передачі цих матеріалів, затверджуваний замісниками керівника організації чи керівниками структурних підрозділів.

3.7. Обов'язки осіб, допущених до відомостей, що складають комерційну таємницю

Особи, допущені до робіт, документів і відомостей, що складають комерційну таємницю, несуть особисту відповідальність за дотримання ними установленого режиму. Перш ніж отримати дозвіл на доступ до комерційної таємниці, вони повинні вивчити вимоги інструкцій та інших нормативних документів щодо захисту комерційної таємниці у частині, що їх торкається, здати залік на знання вказаних вимог і дати індивідуальне письмове зобов'язання щодо зберігання комерційної таємниці.

Особи, допущені до робіт, документів і відомостей, що складають комерційну таємницю, зобов'язані:

- суворо зберігати комерційну таємницю, яка стала їм відомою, припиняти дії інших осіб, які можуть призвести до розголошення комерційної таємниці. Про такі факти а також про інші причини чи умови можливого витоку комерційної таємниці негайно інформувати безпосереднього керівника і службу безпеки;
- протягом договірного періоду не використовувати відому комерційну таємницю у своїх особистих інтересах, а також без відповідного дозволу керівництва не займатися будь-якою діяльністю, яка як конкурентна дія може нанести шкоду організації – власнику цієї комерційної таємниці;
- виконувати тільки ті роботи і знайомитися тільки з тими документами, до яких мають доступ за своїми службовими обов'язками;
- знати ступінь важливості виконуваних робіт, правильно визначати обмежувальний гриф документів, суворо дотримуватись правил користування ними, порядку їх обміну і зберігання;
- при складанні документів з відомостями, що складають комерційну таємницю, обмежуватися мінімальними, дійсно необхідними у документі відомостями;
- визначати кількість примірників документів у суворій відповідності з дійсною службовою потребою і не допускати розсилання їх адресатам, котрі не мають відношення до даних документів;
- на чернетках документів проставляти відповідний обмежувальний гриф та інші необхідні реквізити, передавати їх для друкування тільки з письмового дозволу керівника підрозділу;
- після отримання з машинописного бюро віддрукованих документів перевірити їх наявність, звірити ці дані з записами у журналі і розписатися (з зазначенням дати) за отримання віддрукованих документів і чернеток, після чого взяти на облік у канцелярії чи в уповноваженого служби безпеки;

- отримувати документи з грифом “КТ” особисто у канцелярії чи в уповноваженого служби безпеки. Вчасно знайомитися з отриманими документами і розбірливо розписатися на них з вказівкою дати ознайомлення;
- вхідні документи з грифом “КТ” вчасно направляти для прилучення до справи з відповідними відмітками про виконання (номер справи, що зроблено за вимогами документів, дата, підпис) і з резолюцією керівника підрозділу;
- здавати у канцелярію чи уповноваженому служби безпеки виконані вхідні документи, а також призначені для розсилання, підшивання у справу, знищення і взяття на інвентарний облік під розписку у журналах обліку;
- мати внутрішній опис документів з грифом “КТ”, у якому відводиться окремий розділ, і негайно вносити у нього всі отримані для виконання документи, зберігати їх тільки в окремій теці, а при виході з приміщення у робочий час теку з документами закривати у сейф;
- після закінчення роботи з документами з грифом “КТ” вчасно повертати їх у канцелярію чи уповноваженому служби безпеки;
- про втрату чи недостачу документів з грифом “КТ”, ключів від сейфів, особистої печаті негайно повідомляти у службу безпеки;
- при звільненні, перед виходом у відпустку, від’їздом у відрядження вчасно здати чи зробити звіт перед канцелярією чи уповноваженим за всі документи, що значаться за ним;
- знайомити представників інших закладів з документами з грифом “КТ” тільки з письмового дозволу керівника підрозділу;
- особисто знайомитися з дозволами керівників на приписах, у яких повинні бути визначені питання і об’єм відомостей, що підлягають розгляду;
- вимагати від осіб, що перебувають у відрядженні, розписки на документах, з якими вони ознайомились, чи у облікових картках цих документів;
- документи з грифом “КТ” під час роботи розміщувати так, щоб виключалась можливість ознайомлення з ними інших осіб, у тому числі допущених до подібних робіт і документів, але які не мають до них прямого відношення;
- за першою вимогою канцелярії та відділу служби безпеки надавати для перевірки всі наявні документи з грифом “КТ”;
- надавати за вимогою начальника відділу усні чи письмові пояснення про порушення встановлених правил виконання з грифом “КТ”, обліку і зберігання документів з грифом “КТ”, а також фактах розголошення відомостей з грифом “КТ”, втраті документів, що містять такі відомості.

3.8. Принципи організації і проведення контролю за забезпеченням режиму при роботі з відомостями, що містять комерційну таємницю

Контроль за забезпеченням режиму при роботі з відомостями, що складають комерційну таємницю, здійснюється з метою вивчення і оцінювання фактичного стану зберігання комерційної таємниці, виявлення недоліків і порушень при роботі з матеріалами з грифом “КТ”, установлення причин таких недоліків і порушень та розроблення пропозицій, направлених на їх ліквідацію і запобігання.

Контроль за забезпеченням режиму при роботі з матеріалами з грифом “КТ” здійснює служба безпеки і керівники структурних підрозділів.

Комісії з перевірки забезпечення режиму при роботі з матеріалами з грифом “КТ” комплектуються з досвідчених кваліфікованих співробітників у складі не менше 2-х чоловік, які мають допуск до цієї роботи. Участь у перевірці не повинна призводити до необґрунтованого збільшення поінформованості про ці відомості осіб, які перевіряють.

Перевірки забезпечення режиму при роботі з матеріалами з грифом “КТ” проводяться не рідше одного разу на рік комісіями на основі припису, підписаного керівником організації чи його замісником.

Перевірка проводиться у присутності керівника структурного підрозділу чи його замісника.

Члени комісії мають право знайомитися зі всіма документами, журналами (картками) обліку та іншими матеріалами, які мають відношення до питань, що перевіряються, а також проводити бесіди і консультації зі спеціалістами чи виконавцями, вимагати надання письмових пояснень, довідок, звітів зі всіх питань, що входять до компетенції комісії.

За результатами перевірки складається акт (довідка) з відображенням у ньому стану забезпечення дотримання режиму роботи з матеріалами з грифом “КТ”, виявлених недоліків і порушень та пропозицій щодо їх ліквідації.

З актом, після затвердження його керівником організації чи його замісником, під розпис знайомиться керівник структурного підрозділу.

Про ліквідацію виявлених при перевірці недоліків і порушень режиму при роботі з матеріалами з грифом “КТ” і реалізації пропозицій керівник підрозділу в установлені комісією строки повідомляє керівника служби безпеки.

При установленні факту втрати документів, справ і видань з грифом “КТ” чи розголошення вміщених у них відомостей негайно повідомляють керівника організації, його замісників і керівника служби безпеки.

Для розслідування факту втрати документів, справ і видань з грифом “КТ” при установленні факту розголошення відомостей, що містяться у цих матеріалах, наказом керівника організації (розпорядженням керівника структурного підрозділу) назначається комісія, висновок якої про результати розслідування затверджується керівником, що створив комісію.

На загублені документи, справи і видання з грифом “КТ” складається акт. Відповідні відмітки вносяться в облікові документи.

Акти на загублені справи постійного збереження після їх затвердження керівником організації чи його замісниками передаються в архів для внесення у справу фонду.

3.9. Відповідальність за розголошення комерційної таємниці, втрату документів, що містять комерційну таємницю

Розголошення відомостей, що складають комерційну таємницю – це оголошення відомостей особою, якій ці відомості були довірені за службовими обов’язками чи стали відомі іншим шляхом, через що вони стали надбанням сторонніх осіб.

Втрата документів, що містять відомості комерційної таємниці, – це вихід (у тому числі і тимчасовий) документів з-під контролю відповідальної за їх збереження особи, якій вони були довірені за службовими обов’язками, через порушення встановлених правил роботи з ними, через що ці документи стали чи могли стати надбанням сторонніх осіб.

Інші порушення при роботі з матеріалами комерційної таємниці – це порушення вимог, яке може призвести до розголошення цих відомостей, втраті документів, що містять такі відомості.

За втрату і незаконне знищення документів, справ і видань з грифом “КТ”, за розголошення відомостей, що містяться у цих матеріалах, а також за порушення вимог щодо їх зберігання та забезпечення цілісності винні особи притягаються до відповідальності за установленим порядком.

Контрольні питання

1. Наведіть структуру правового захисту інформації.
2. Наведіть класифікацію інформації з обмеженим доступом.
3. Поясніть суть поняття “комерційна таємниця”.
4. Опишіть задачі служби безпеки щодо захисту комерційної таємниці.
5. Розкажіть про порядок визначення інформації, що містить комерційну таємницю.

6. Опишіть порядок допуску співробітників до відомостей, що складають комерційну таємницю.
7. Розкажіть про порядок роботи з документами з грифом “КТ”.
8. Опишіть умови забезпечення цілісності документів, справ і видань з грифом “КТ”.
9. Поясніть суть обов’язків осіб, допущених до відомостей, що складають комерційну таємницю.
10. Охарактеризуйте принципи організації і проведення контролю за забезпеченням режиму при роботі з відомостями, що складають комерційну таємницю.

Глава 4. ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЇ

4.1. Основні поняття

Організаційно-технічні заходи забезпечують блокування розголошення і витоку конфіденційної інформації через технічні засоби забезпечення інформаційної діяльності, а також протидію технічним засобам промислового шпигунства спеціальними технічними засобами, які установлюються на елементи конструкцій будівель, приміщень і технічних засобів, які потенційно утворюють канали витоку інформації. Для цього можливе використання:

- технічних засобів пасивного захисту, наприклад фільтрів, обмежувачів та інших засобів розв’язки акустичних, електричних і електромагнітних систем захисту мереж телефонного зв’язку, енергопостачання, радіофікації тощо;
- технічних засобів активного захисту – датчиків акустичних шумів і електромагнітних перешкод.

Організаційно-технічні заходи захисту інформації поділяються на просторові, режимні, енергетичні та технічні (рис. 7).

Просторові заходи виражаються у зменшенні ширини діаграми направленості, послабленні бокових і заднього пелюстків діаграми направленості випромінювання радіоелектронних засобів.

Режимні заходи зводяться до використання секретних методів передавання інформації засобами зв’язку: шифрування, квазізмінні частоти передавання тощо.

Енергетичні заходи – це зниження інтенсивності випромінювання і робота радіоелектронних засобів на понижених потужностях.

Технічні заходи – це заходи, що забезпечують придбання, установлення і використання у процесі інформаційної діяльності спеціальних, за-

хищених від побічних випромінювань технічних засобів чи засобів, побічні електромагнітні випромінювання і наведення яких не перевищують границі території, що охороняється.

Технічні заходи захисту конфіденційної інформації поділяються на: приховування, заглушення і дезінформацію.

Приховування виражається у використанні радіомовчання і створенні пасивних перешкод приймальним засобам зловмисників.

Заглушення проводиться шляхом створення активних перешкод.

Дезінформація – це:

- організація фальшивої роботи технічних засобів зв'язку і обробки інформації;
- змінювання режимів використання частот і регламентів зв'язку;
- показ фальшивих демаскувальних ознак діяльності та розпізнавань.

Рис. 7. Організаційно-технічні заходи захисту інформації

Захисні заходи технічного характеру можуть бути направлені на конкретний технічний пристрій чи конкретну апаратуру і виражаються в таких заходах, як відключення апаратури на час ведення конфіденційних переговорів чи використання захисних пристроїв типу обмежувачів, буферних засобів, фільтрів і пристроїв зашумлення.

4.2. Задачі організаційно-технічного захисту інформації

Основними задачами організаційно-технічного захисту інформаційної діяльності є:

- розробка і затвердження функціональних обов'язків посадових осіб служби інформаційної безпеки;
- внесення необхідних змін і доповнень у всі організаційно-розпорядні документи (положення про підрозділи, обов'язки посадових осіб, інструкції користувачів системи тощо) з питань забезпечення безпеки програмно-інформаційних ресурсів ІС і дій у випадку виникнення кризових ситуацій;
- оформлення юридичних документів (угоди, накази і розпорядження керівництва організації) з питань регламентації відносин з користувачами (клієнтами), що працюють в автоматизованій системі, між учасниками інформаційного обміну і третьою стороною (арбітраж, третейський суд) про правила вирішення спорів, пов'язаних із застосуванням електронного підпису;
- створення науково-технічних і методологічних основ захисту ІС;
- виключення можливості таємного проникнення в приміщення, встановлення прослуховувальної апаратури тощо;
- перевірка і сертифікація використовуваних в ІС технічних і програмних засобів на предмет визначення заходів для їх захисту від витоку каналами побічних електромагнітних випромінювань і наведень;
- визначення порядку призначення, зміни, затвердження і надання конкретним посадовим особам необхідних повноважень з доступу до ресурсів системи;
- розробка правил керування доступом до ресурсів системи, визначення переліку задач, вирішуваних структурними підрозділами організації з використанням ІС, а також використовуваних при їх розв’язанні режимів оброблення і доступу до даних;
- визначення переліку файлів і баз даних, що містять відомості, які складають комерційну і службову таємницю, а також вимоги до рівнів їх захисту від несанкціонованого доступу при передаванні, зберіганні та обробленні в ІС;

- виявлення найбільш можливих загроз для даної ІС, виявлення вразливих місць процесу оброблення інформації і каналів доступу до неї;
- оцінка можливих втрат, викликаних порушенням безпеки інформації, розробка адекватних вимог з основних напрямів захисту;
- організація надійного пропускного режиму;
- визначення порядку обліку, видачі, використання і зберігання знімних магнітних носіїв інформації, що містять еталонні та резервні копії програм і масивів інформації, архівні дані тощо;
- організація обліку, зберігання, використання і знищення документів і носіїв з закритою інформацією;
- організація і контроль за підтриманням всіма посадовими особами вимог щодо забезпечення безпеки обробки інформації;
- визначення переліку необхідних заходів забезпечення безперервної роботи ІС в критичних ситуаціях, що виникають у результаті несанкціонованого доступу, перебоїв і відказів, помилок у програмах і діях персоналу, стихійного лиха тощо;
- контроль за реалізацією вибраних заходів захисту в процесі проектування, розроблення, введення в дію і функціонування ІС;
- періодичний аналіз стану і оцінювання ефективності заходів захисту інформації;
- розподілення реквізитів розмежування доступу (паролів, ключів шифрування тощо);
- аналіз системних журналів, вжиття заходів з виявлення порушень правил роботи;
- розробка правил розмежування доступу користувачів до інформації;
- періодичне (з залученням сторонніх спеціалістів) проведення аналізування стану і оцінки ефективності заходів і застосовуваних засобів захисту. На основі отриманої в результаті такого аналізу інформації оцінки приймати необхідні заходи для вдосконалення системи захисту;
- розгляд і затвердження всіх змін у обладнанні ІС, перевірка їх на задоволення вимог захисту, документальне відображення змін тощо;
- перевірка працівників, що приймаються на роботу, навчання їх правилам роботи з інформацією, ознайомлення з мірами відповідальності за порушення правил захисту, навчання, створення умов, при яких персоналу було б невигідно порушувати свої обов'язки.

4.3. Заходи запобігання розголошенню конфіденційної інформації

Розголошення – це зловмисні чи необережні дії посадових осіб і громадян, результатом яких стало розголошення конфіденційних відомостей, і, як наслідок, ознайомлення з ними осіб, недопущених до цих даних. Розголошення виражається у повідомленні, передаванні, пересиланні, опублікуванні, втраті та інших способах обміну діловою та науковою інформацією.

Розголошення охоронюваної інформації може статися при наявності певних умов і обставин службового та особистого характеру. Причини розголошення, як правило, пов'язані з недосконалістю розроблених норм щодо захисту інформації, а також порушенням цих норм (в тому числі і недосконалих), порушенням правил поводження з відповідними документами і відомостями, що вміщують конфіденційну інформацію.

До фактів і обставин, що призводять до розголошення інформації, відносяться:

- недостатнє знання співробітниками правил захисту конфіденційної інформації і нерозуміння необхідності чіткого їх виконання;
- слабий контроль за дотриманням правил роботи з відомостями конфіденційного характеру;
- плинність кадрів, у тому числі тих, що знають відомості конфіденційного характеру.

Розголошення конфіденційної інформації можливе при:

- *передаванні інформації каналами електрозв'язку;*
- *повідомленні, оголошенні:*

а) на ділових зустрічах і переговорах;
б) при діловій переписці;
в) на семінарах, симпозіумах, у пресі та ЗМІ;
г) на виставках;
д) у судових інстанціях і адміністративних органах;

- *пересиланні документів:*

а) каналами поштового зв'язку;
б) нарочними, кур'єрами, попутником;

- *опублікуванні:*

а) у пресі;
б) у наукових роботах і дисертаціях;

- *особистому спілкуванні*:

а) на зустрічах;
б) при телефонних переговорах;

- *втраті документів*:

а) на роботі;

б) за межами служби;

- *безконтрольному залишенні документів:*

а) на робочому місці;

б) на екрані ПЕОМ;

в) при ксерокопіюванні;

- *безконтрольному розробленні документів:*

а) необґрунтоване виготовлення документів;

б) внесення у звичайні документи відомостей конфіденційного характеру;

в) чернетки, намітки, зіпсовані варіанти;

- *безконтрольному документообігу*:

а) необґрунтоване розсилання документів;

б) необґрунтоване ознайомлення з документами співробітників та співвиконавців;

- *безконтрольному зберіганні та знищенні документів;*
- *безконтрольному прийомі документів, що надходять в організацію*.

Канали розповсюдження інформації – це засоби обміну діловою і науковою інформацією між суб'єктами ділових і особистих стосунків. Залежно від способу обміну канали розповсюдження інформації поділяються на формальні та неформальні (рис. 8).

До ***неформальних каналів*** розповсюдження інформації відносяться:

- особисте спілкування (зустрічі та переговори, ділова переписка тощо);
- виставки, семінари, симпозіуми, конференції, судові засідання та інші масові заходи;
- засоби масової інформації (преса, радіо, телебачення, інтерв'ю тощо).

Формальними каналами розповсюдження інформації є:

- ділові зустрічі, наради, переговори тощо;
- обмін офіційними діловими і науковими документами (доповідями, тезами тощо);
- засоби передавання офіційної інформації (пошта, телеграф, телефон тощо).

В основу захисту конфіденційної інформації від розповсюдження доцільно покласти такі принципи:

- максимальне обмеження числа осіб, допущених до роботи з конфіденційною інформацією, так як ступінь її збереження знаходиться у прямій залежності від числа допущених до неї осіб;
- персональна відповідальність за збереження інформації передбачає розробку заходів, які спонукають співробітників зберігати секрети не тільки із-за побоювання наслідків за вільне чи невільне

розкриття, але й забезпечують зацікавленість кожного конкретного працівника у збереженні таємниці.

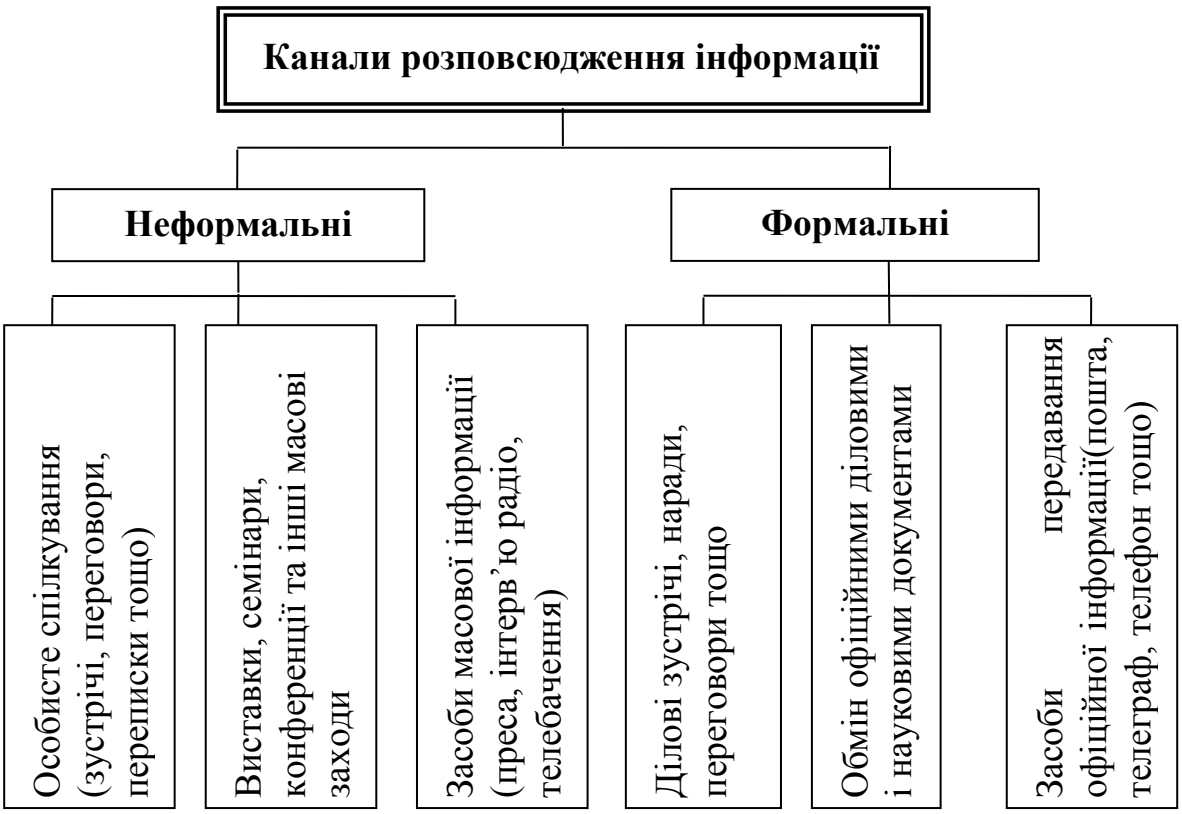

Рис. 8. Канали розповсюдження інформації

Звідси одним із направлень роботи є робота з кадрами, виховно–профілактична робота, яка включає в себе сукупність впливу на свідомість, почуття, волю і характер співробітників з метою формування в них вміння зберігати таємницю і суворо дотримуватися установлених правил роботи з закритою інформацією. Головними напрямками цієї діяльності є:

- підвищення відповідальності за збереження таємниць;
- створення обстановки нетерпимості до фактів порушення установленого порядку забезпечення інформаційної безпеки;
- суворий контроль за всіма видами переговорів зі сторонніми організаціями та їх представниками;
- контроль публікацій, виступів, інтерв'ю та інших форм спілкування з питань діяльності підприємства;
- контроль розмов у службових приміщеннях і телефонних переговорів співробітників на службові теми;
- вивчення дій і поведінки співробітників у позаслужбовий час, місць їхнього перебування, нахилів, захоплень, згубних звичок, задоволення від праці тощо.

Природно, що всі ці дії повинні проводитися згідно з чинними законодавчими актами, з точним дотриманням прав і обов'язків співробітників підприємства, без будь - якого втручання в особисте життя.

Систему заходів щодо запобігання розголошенню конфіденційної інформації рекомендується розробляти відповідно до рекомендацій, наведених у *додатку 5*.

4.4. Заходи забезпечення захисту інформації від витоку технічними каналами

Технічними засобами, які можуть бути джерелами витоку інформації каналами побічних електромагнітних випромінювань і наведень (ПЕМВІН), є:

- засоби і системи телефонного , телеграфного (телетайпного), директорського, гучномовного, диспетчерського, внутрішнього, службового і технологічного зв'язку;
- засоби і системи звукопідсилення, звукозапису і звуковідтворення;
- пристрої, що створюють дискретні канали зв'язку, абонентська апаратура з засобами відображення і передавання, каналоутворення тощо;
- апаратура перетворення, обробки, передавання і приймання відеоканалів, що містять факсимільну інформацію;
- засоби і системи спеціальної охоронної сигналізації (на розкривання дверей, вікон і проникнення у приміщення сторонніх осіб), пожежної сигналізації (з датчиками, що реагують на дим, світло, тепло, звук);
- система звукової сигналізації (виклик секретаря, вхідна сигналізація);
- контрольно-вимірювальна апаратура;
- засоби і системи кондиціонування (датчики температури, вологості, кондиціонери);
- засоби і системи проводової радіотрансляційної мережі і прийому програм радіомовлення та телебачення;
- засоби і системи часофіксації (електронні годинники, вторинні електрогодинники);
- засоби і системи електроосвітлення і побутового електрообладнання (світильники, електронагрівальні прилади, електровентилятори, проводова мережа електроосвітлення тощо);
- електронна і електрична оргтехніка.

Перелічені технічні засоби можуть бути випадковими антенами (апаратура та її блоки) і розподільними випадковими антенами (кабельні лінії і проводи).

Вказаними елементами можуть бути:

- технічні засоби і прилади;

- кабельні лінії та розводки, що з'єднують пристрої і обладнання;
- комутаційні пристрої (комутатори, кроси, бокси тощо);
- елементи заземлення і електроживлення.

У процесі функціонування засобів обчислювальної техніки у конструктивних елементах і кабельних з'єднаннях циркулюють електричні струми інформативних сигналів, внаслідок чого формуються електромагнітні поля, рівні яких можуть бути достатніми для прийому сигналів і витягнення інформації за допомогою спеціальної апаратури.

Канали витоку інформації можуть виникати внаслідок випромінювання інформаційних сигналів при роботі телефонних мереж і наведення цих сигналів у лініях зв'язку, колах електроживлення і заземлення, інших комунікаціях, що мають вихід за межі *контрольованої території*. Інформаційні сигнали можуть розповсюджуватись на великі відстані і реєструватися технічними засобами розвідок за межами контрольованої зони.

Частоти, на яких можуть випромінюватися (наводитися) інформативні сигнали, залежать від типів і видів апаратних засобів і можуть розповсюджуватись в діапазоні від сотень герц до декількох десятків гегагерц.

Відстань наведень визначається відстанню між джерелами випромінювання і апаратурою, що піддається впливу цих випромінювань, довжиною паралельного пробігу і величиною перехідного затухання ліній, напругою інформативного сигналу в лінії та рівнем шумів (перешкод).

Витоки інформації колами заземлення можуть виникнути при наявності рознесених точок заземлення і інформативних кіл при утворенні у різних точках системи заземлення різниці потенціалів і виникненні внаслідок цього струмів у колах заземлення, а також через недосконаліть екранів, що приводить до асиметрії лінії відносно екрана і до виникнення у колі між корпусом екрана і "землею" інформативних струмів.

Окрім того, *можливі канали витоку утворюються:*

- низькочастотними електромагнітними полями, що виникають при роботі телефонних ліній;
- при виникненні паразитної високочастотної (ВЧ) генерації;
- при проходженні інформативних (небезпечних) сигналів у колі електроживлення;
- при взаємному впливі кіл;
- при проходженні інформативних (небезпечних) сигналів у колі заземлення;
- при паразитній модуляції високочастотного сигналу;
- внаслідок фальшивих комутацій і несанкціонованих дій.

Організація захисту інформації в інформаційних системах від витоку каналами ПЕМВІН передбачає:

- категорування об'єктів електронно-обчислювальної техніки;
- включення у технічне завдання на монтаж інформаційних систем і систем обчислювальної техніки розділу із захисту інформації;

- монтаж інформаційних систем обчислювальної техніки згідно з нормативними документами;
- дослідження (в тому числі технічний контроль) об'єктів електронно-обчислювальної техніки;
- установку (за потребою) атестованих засобів захисту;
- технічний контроль за ефективністю прийнятих заходів.

За результатами дослідження складається акт, у якому відображається:

- категорія об'єктів електронно-обчислювальної техніки;
- перелік технічних засобів і комунікацій, що знаходяться на об'єкті електронно-обчислювальної техніки;
- оцінка відповідності монтажу нормативним документам;
- пропозиції щодо застосування додаткових заходів захисту (за потребою).

До акту додається:

- схема розміщення технічних засобів об'єкта – електронно-обчислювальної техніки і проходження комунікацій на ньому;
- протоколи вимірювань.

На етапі проведення організаційних заходів необхідно:

- визначати перелік відомостей, що підлягають технічному захисту (визначає власник інформації згідно з діючим законодавством України);
- обґрунтувати необхідність розробки і реалізації захисних заходів з урахуванням матеріальних чи інших втрат, які можуть бути нанесені внаслідок можливого порушення цілісності інформації чи її витоку технічними каналами;
- установити перелік виділених приміщень, у яких не допускається реалізація загроз і витік інформації з обмеженим доступом;
- визначити перелік технічних засобів, застосування яких не обґрунтовано службовою та виробничою необхідністю і підлягають демонтажу;
- визначити наявність використовуваних і не використовуваних повітряних, наземних, настінних і прихованих кабелів, кіл і проводів, що виходять за межі виділених приміщень;
- визначити системи, які підлягають демонтажу, кабельні мережі, кола живлення, заземлення, які слід переобладнати чи установити в них захисні пристрої.

Система організаційних, організаційно-технічних і технічних заходів щодо захисту джерел конфіденційної інформації від витоку технічними каналами наведена у *додатку 6.*

4.5. Заходи запобігання несанкціонованому доступу до джерел конфіденційної інформації

Несанкціонований доступ до джерел конфіденційної інформації – це протиправне навмисне оволодіння конфіденційною інформацією особою, яка не має доступу до неї.

Основними способами несанкціонованого доступу до джерел конфіденційної інформації є: *ініціативне співробітництво, схилення до співробітництва, вивідування, випитування, підслуховування, спостерігання, викрадення, копіювання, підробка (модифікація), знищення, незаконне підключення, перехоплення, таємне ознайомлення, фотографування, збирання та аналітичне оброблення інформації.*

Ініціативне співробітництво проявляється у певних діях осіб, які чимось незадоволені чи потребують матеріальних засобів для існування, з числа працюючих на підприємстві або ж просто жадібних, зажерливих, готових заради наживи на будь-які протиправні дії. Відомі приклади ініціативного співробітництва з політичних, моральних чи фінансових міркувань, та і просто з різних причин і мотивів.

Схиляння до співробітництва – це, як правило, насильна дія зі сторони зловмисників. Схиляння чи вербування може здійснюватися шляхом підкупу, залякування, шантажу. Схиляння до співробітництва реалізується у вигляді реальних загроз, переслідувань та інших дій, які проявляються у переслідуванні, скривдженні, нарузі тощо.

Вивідування, випитування – це намагання під виглядом наївних запитань отримати певні відомості. Випитувати інформацію можна і фальшивими працевлаштуваннями, і створенням фальшивих фірм та іншими діями.

Підслуховування – спосіб проведення розвідки і промислового шпіонажу, який застосовується агентами, спостерігачами, інформаторами, спеціальними постами підслуховування. З метою підслуховування зловмисники йдуть на самі різні хитрощі, використовують для цього спеціальних людей, співробітників, сучасну техніку, різні прийоми її застосування. Підслуховування може здійснюватися безпосереднім сприйняттям акустичних коливань особою при прямому сприйманні мовної інформації чи за допомогою технічних засобів.

Спостерігання – спосіб проведення розвідки про стан і діяльність противника. Проводиться візуально і за допомогою оптичних приладів. Процес спостерігання доволі складний, тому що вимагає значних затрат сил і засобів. Тому спостерігання, як правило, ведеться цілеспрямовано, у певний час і у необхідному місці спеціально підготовленими людьми. До технічних засобів відносяться оптичні прилади (біноклі, труби, перископи), телевізійні системи, прилади спостерігання вночі та при обмеженій видимості.

Викрадання – зловмисне протиправне оволодіння чужим майном, засобами, документами, матеріалами, інформацією. Крадуть все, що “погано лежить”, включаючи документи, продукцію, дискети, ключі, коди, паролі і шифри тощо.

Копіювання. У практиці кримінальних дій копіюють документи з відомостями, які цікавлять зловмисників, інформацію, яка обробляється в автоматизованих системах обробки даних (АСОД), продукцію.

Підробка (модифікація, фальсифікація) в умовах безсоромної конкуренції набула великих масштабів. Підробляють документи, які дозволяють отримати певну інформацію, листи, рахунки, бухгалтерську і фінансову документацію, ключі, пропуски, паролі тощо.

Знищення. Відносно інформації особливою небезпекою є її знищення в АСОД, у якій накопичуються на технічних носіях великі об'єми відомостей різного характеру, причому багато з них дуже важко виготовити у вигляді немашинних аналогів. Знищуються і люди, і документи, і засоби обробки інформації, і продукція.

Незаконне підключення – контактне чи безконтактне підключення до різних ліній і проводів з метою несанкціонованого доступу до інформації. Підключення можливе як до проводових ліній телефонного і телеграфного зв'язку, так і до ліній зв'язку іншого інформаційного призначення:

- ліній передачі даних;
- з'єднувальних ліній периферійних пристроїв великих і малих ЕОМ;
- ліній диспетчерського зв'язку, конференцзв'язку, живлення, заземлення тощо.

Перехоплення – отримання розвідувальної інформації шляхом прийому сигналів електромагнітної енергії пасивними засобами прийому, розміщеними, як правило, на достатній відстані від джерела конфіденційної інформації. Перехопленню доступні переговори будь-яких систем радіозв'язку, переговори, що ведуться з рухомих засобів телефонного зв'язку (радіотелефон), переговори всередині приміщення шляхом безпроводових систем зв'язку тощо.

Таємне ознайомлення – спосіб отримання інформації, до якої суб'єкт недопущений, але за певних умов він може отримати можливість дещо дізнатися (відкритий документ на столі під час бесіди з відвідувачем, спостереження екрана ПЕОМ зі значної відстані тощо). До таємного ознайомлення відноситься і перлюстрація поштових відправлень, підприємницької та особистої переписки.

Фотографування – спосіб отримання видимого зображення об'єктів кримінальних інтересів на фотоматеріалі. Особливість способу – документальність, яка дозволяє при дешифруванні фотознімків за окремими елементами і демаскувальними ознаками отримати надто цінні відомості про об'єкт спостереження.

Збирання і аналітичне оброблення є заключним етапом вивчення і узагальнення здобутої інформації з метою отримання достовірних і об'ємних відомостей про діяльність об'єкта, що цікавить зловмисника. Повний об'єм відомостей про діяльність конкурента не може бути

отриманий яким-небудь одним способом. Чим більшими інформаційними можливостями володіє зловмисник, тим більших успіхів він може досягти у конкурентній боротьбі. На успіх може розраховувати той, хто швидше і повніше збере необхідну інформацію, опрацює її і прийме правильне рішення.

Заходи щодо протидії несанкціонованому доступу до джерел конфіденційної інформації за допомогою технічних засобів проводяться за такими основними напрямами:

- захист від спостереження і фотографування;
- захист від підслуховування;
- захист від підключення;
- захист від перехоплення.

Захист від спостереження і фотографування передбачає:

- вибір оптимального розміщення засобів документування, розмноження і відображення (екрани ПЕОМ, екрани загального користування тощо) інформації з метою виключення прямого чи дистанційного спостереження (фотографування);
- використання світлонепроникного скла, завісок, драпувань, плівок та інших захисних матеріалів (решітки, віконниці тощо);
- вибір приміщень, звернених вікнами у безпечні зони (напрями);
- використання засобів гасіння екранів ЕОМ і табло колективного користування після визначеного часу роботи (робота у режимі реального часу).

Захист від спостереження і фотографування на місцевості передбачає застосування заходів маскування, захування об’єктів у рельєфі місцевості, лісових масивах і, природно, організацію режиму охорони на відстані, що забезпечує таємність діяльності.

У більш складних умовах можна застосовувати засоби активного маскування: маскувальні дими, аерозолі та інші засоби.

Захист від підслуховування. Істотною перешкодою на шляху зловмисника з підслуховувальною технікою є створення на комерційних об’єктах особливих, захищених від підслуховування приміщень для проведення засідань, переговорів і конфіденційних бесід. Таким приміщенням надається статус спеціальних, вони обладнуються з урахуванням таких вимог:

- будівлі, де розміщуються особливі приміщення, повинні мати цілодобову охорону і систему сигналізації;
- приміщення розміщується, за можливості, у центрі будівлі, поряд з кабінетами керівництва об’єкта;
- якщо у приміщенні повинні бути вікна, то бажано, щоб вони не мали балконів і не виходили на сусідні з об’єктом будівлі, а орієнтувалися на внутрішній двір чи закривалися глухими віконницями;

- усередині приміщення повинна бути мінімальна кількість меблів; конструкція меблів повинна бути пристосована для роботи спеціаліста з пошуку техніки підслуховування;
- у приміщенні не повинно бути радіоелектронних пристроїв, ком - п'ютерів, телевізорів, магнітофонів;
- телефонний зв'язок, як найбільш "зручний" для підслуховування засіб, повинен здійснюватися за рекомендацією спеціаліста із захисту.

Відомий і такий спосіб захисту, як проведення переговорів у прозорій, обладнаній із прозорого скла і пластиків кабіні. Це робиться для того, щоб зразу помітити будь-який сторонній (непрозорий) предмет, у тому числі і "залишену" кимось апаратуру підслуховування. У такій кабіні всі предмети, у тому числі і меблі роблять з прозорих пластиків. Спеціальна система вентиляції подає повітря всередину приміщення.

При виборі способу захисту приміщень слід пам'ятати про те, що його ефективність буде високою тільки за суворого дотримання режиму відвідувань і роботи у такому спеціальному приміщенні. Потрібна і періодична перевірка його спеціалістом з пошуку техніки прослуховування. Суворе дотримання всього комплексу заходів безпеки у сполученні з особистою зацікавленістю співробітників у процвітанні своєї фірми може створити нездоланний психологічний бар'єр для зловмисників і конкурентів, у яких страх швидкого розкриття їх злочинних дій на об'єкті буде сильнішим бажання отримати будь-які вигоди і винагородження за установлення техніки підслуховування.

Забезпечення безпеки телефонних переговорів. Проблема захисту телефонних переговорів в умовах широкої телефонізації суспільства стає надто актуальною, тому що зловмисники часто користуються підслуховуванням як службових, так і домашніх телефонів. При цьому широко застосовуються такі способи як підключення до телефонних ліній, установлення у телефонну лінію телефонних радіозакладок, високочастотне нав'язування та інші варіанти підслуховування.

До організаційних заходів захисту відноситься планування прокладення телефонних ліній у будівлях і приміщеннях так, щоб було зручно їх контролювати і важко застосовувати можливості підслуховування. Прокладку телефонних ліній слід проводити зі зменшенням можливого паралельного пробігу і перехрещування.

З метою вчасного визначення стороннього включення необхідно забезпечити постійне спостерігання співробітниками телефонної служби за станом телефонних ліній виділених приміщень. Про всякі зміни чутності розмови чи появу шумів, потріскування, що можуть засвідчувати про включення у лінію підслуховувальної апаратури, необхідно повідомляти у службу безпеки.

Організаційним заходом є відключення телефонного апарата від телефонної лінії за допомогою роз'ємної розетки на період проведення

конфіденційних переговорів. Це достатньо ефективний захід протидії від усіх варіантів підслуховування.

Дуже ефективним заходом протидії підслуховуванню є використання для ведення конфіденційного спілкування маскіраторів мови чи скремблерів. Сьогодні техніка шифрування мовних сигналів достатньо розвинута і з'явилася на ринку у вигляді зручних переносних чи стаціонарних апаратів, які надійно шифрують мовний сигнал до його подачі у телефонну лінію.

Захист від перехоплення. Перехоплення – це спосіб несанкціонованого отримання конфіденційної інформації за рахунок прийому електромагнітних сигналів радіодіапазону.

Методи захисту від перехоплення поділяються на:

- *організаційні*
  а) територіальні обмеження – уміле розміщення радіостанцій на місцевості, що виключає прийом радіосигналів;
  б) просторові обмеження – вибір направлення випромінювання у сторону найменшої можливості прийому сигналів;
  в) часові обмеження – скорочення до мінімуму часу випромінювання;
- *організаційно-технічні*
  а) просторові – використання направлених антен, зменшення ширини діаграми спрямованості антен, послаблення бокових і заднього пелюстків;
  б) режимні – використання секретних режимів передавання інформації;
  в) енергетичні – зниження інтенсивності випромінювання за рахунок зменшення потужності та зменшення довжини антени;
- *технічні*
  а) приховування – використання радіомовлення, створення пасивних перешкод, використання засобів маскування;
  б) подавлення – створення активних перешкод;
  в) технічна дезінформація – організація фальшивої роботи, зміна режимів роботи, показання фальшивих характеристик тощо.

Комплекс організаційних, організаційно-технічних і технічних заходів щодо запобігання несанкціонованого доступу до джерел конфіденційної інформації наведений у *додатку 7.*

4.6. Організаційно-технічні заходи щодо захисту локальної робочої станції

У деяких випадках заходи організаційно-технічного характеру можуть бути надійною заміною будь-яких інших засобів захисту інформації. Вони є додатковим рівнем забезпечення обраної політики безпеки і конкретний набір подібних заходів завжди залежить від ситуації.

Проте існує типовий перелік заходів, що застосовуються у будь-яких умовах. Цей перелік заснований на виконанні спеціальних вимог, які залежно від їхнього функціонального призначення поділяються на такі групи:

- вимоги щодо розміщення технічних засобів;
- рекомендації щодо встановлення системи захисту інформації (СЗІ);
- заходи щодо забезпечення надійності функціонування СЗІ, яка встановлена на локальній робочий станції (ЛРС).

Реалізація організаційно-технічних заходів щодо захисту інформації повинна починатися з розробки відповідних інструкцій і рекомендацій, а також створення структурних підрозділів, відповідальних за реалізацію політики безпеки і контроль за їхнім неухильним дотриманням.

4.6.1. Вимоги щодо розміщення технічних засобів

При розміщенні технічних засобів, що підтримують системи криптографічного захисту інформації (СКЗІ), слід керуватися такими рекомендаціями:

- розташування режимних приміщень і розміщеного у них устаткування повинно виключати можливість безконтрольного проникнення в ці зони сторонніх осіб і гарантувати збереження конфіденційних документів, що знаходяться в них;
- вхідні двері повинні бути обладнані замками, що гарантують санкціонований доступ у режимні приміщення в неробочий час. Для контролю над входом повинні встановлюватися замки з шифром;
- вікна і двері необхідно обладнати охоронною сигналізацією, зв'язаною з пультом централізованого спостереження;
- розміщення устаткування і технічних засобів, призначених для обробки конфіденційної інформації, повинно відповідати вимогам техніки безпеки, санітарним нормам та вимогам пожежної безпеки;
- у режимні приміщення допускаються тільки за затвердженим списком керівники установи, співробітники відділу безпеки і виконавці, що мають безпосереднє відношення до обробки, передачі і прийому конфіденційної інформації;
- допуск у приміщення допоміжного й обслуговуючого персоналу (прибиральниці, електромонтери, сантехніки тощо) здійснюється тільки у разі службової необхідності в супроводі відповідального за режим, причому потрібно подбати про заходи, що виключають можливість візуального перегляду конфіденційних документів;
- кожен виконавець робіт як користувач мережі конфіденційного зв'язку зобов'язаний зареєструватися в адміністратора служби безпеки;

- внутрішнє планування і розташування робочих місць у режимних приміщеннях повинні забезпечувати виконавцям збереження довірених їм конфіденційних документів і відомостей;
- після закінчення робочого дня режимні приміщення необхідно закривати й опечатувати. Потім їх (з опечатаними вхідними дверима) здають під охорону відділу безпеки або черговому по підприємству (за встановленим порядком) із зазначенням часу прийому-здачі й позначкою про ввімкнення і вимикання охоронної сигналізації в журналі обліку;
- здачу ключів і режимних приміщень під охорону, а також отримання ключів і відчинення режимних приміщень роблять співробітники, що працюють у цих приміщеннях і входять у затверджений керівництвом установи список зі зразками підписів цих співробітників. Список зберігається у начальника охорони чи в чергового по установі;
- перед відчиненням режимних приміщень повинна бути перевірена цілісність відбитків печаток і справність замків. При виявленні порушення цілісності відбитків печаток, пошкодження замків чи інших ознак, що вказують на можливе проникнення у ці приміщення сторонніх осіб, приміщення не відчиняються, а про те, що трапилося, негайно інформується керівництво і відділ безпеки установи;
- у випадку втрати ключа від вхідних дверей режимного приміщення про це негайно доводиться до відома відділу безпеки установи;
- на випадок пожежі, аварії чи стихійного лиха повинні бути розроблені спеціальні інструкції, затверджені керівництвом установи, у яких передбачається виклик адміністрації, посадових осіб, відкриття режимних приміщень, черговість і порядок рятування конфіденційних документів з подальшим їхнім збереженням;
- у приміщення, де знаходиться СЗІ, забороняється приносити і використовувати радіотелефони й іншу радіоапаратуру.

4.6.2. Рекомендації щодо установлення програмного забезпечення СЗІ

Установлюючи програмне забезпечення, що входить до складу СЗІ, потрібно керуватися такими рекомендаціями:

- установлення СЗІ здійснюється тільки особами, що мають відповідну ліцензію;
- апаратну частину ЛРС, на яку встановлюється СЗІ, необхідно перевірити на відсутність апаратних закладок;
- усе програмне забезпечення ЛРС, на якій буде встановлюватися СЗІ, повинно бути ліцензійно чистим, при цьому не допускається

наявність засобів розробки і налагодження програм;

- перед установкою СЗІ необхідно перевірити програмне забезпечення ЛРС на наявність вірусів і програмних закладок;
- мають бути вжиті заходи, що перешкоджають витяганню апаратної частини СЗІ з ЛРС; системні блоки ЛРС мають бути опечатані спеціально виділеною для цих цілей печаткою. Разом з цим допускається застосування інших засобів контролю за доступом до ЛРС;
- до експлуатації СЗІ допускаються особи, що пройшли відповідну підготовку і вивчили експлуатаційну документацію даної СЗІ;
- перед установленням програмного забезпечення СЗІ необхідно здійснити контроль цілісності дистрибутива;
- після завершення встановлення мають бути вжиті заходи, необхідні для здійснення щоденного контролю за встановленою СЗІ, а також її програмним і апаратним оточенням.

4.6.3.Заходи щодо забезпечення надійності функціонування СЗІ, яка встановлена на локальній робочій станції

Основними рекомендаціями щодо організаційно-технічних заходів захисту, які забезпечують безпеку функціонування робочих місць із вбудованими СЗІ, є такі:

- право доступу до робочих місць із вбудованими СЗІ можуть мати тільки особи, що пройшли відповідну підготовку. Адміністратор безпеки повинен ознайомити кожного абонента автоматизованої системи, що використовує СЗІ, із правилами користування чи з іншими нормативними документами, створеними на їхній основі;
- посадові інструкції адміністратора безпеки (його заступника) і відповідального виконавця не повинні суперечити правилам користування спеціальною апаратурою та іншим нормативним документам, створеним на їхній основі;
- адміністратор безпеки зобов'язаний періодично проводити контроль цілісності і легальності встановлених копій програмного забезпечення на всіх ЛРС із вбудованою СЗІ за допомогою програм контролю цілісності;
- при виявленні "сторонніх" (незареєстрованних) програм, порушення цілісності програмного забезпечення чи факту пошкодження печаток на системних блоках робота на ЛРС припиняється. За даним фактом має бути проведене службове розслідування комісією в складі представників служб інформаційної безпеки підприємства – власника мережі і підприємства – абонента мережі, де відбулося порушення, а також організовані роботи з аналізу і ліквідації негативних наслідків даного порушення;

- користувач повинен запускати тільки ті додатки, які дозволені адміністратором безпеки;
- установлене програмне забезпечення не повинно містити засобів розробки й налагодження додатків, а також засобів, що дозволяють здійснювати несанкціонований доступ до системних ресурсів;
- в інструкцію з використання робочої станції повинен бути внесений пункт, що забороняє залишати без контролю обчислювальні засоби, які входять до складу СЗІ, при ввімкненому живленні і завантаженому спеціальному програмному забезпеченні СЗІ;
- заборонити допуск користувачів у режим конфігурування BIOS (наприклад, з використанням парольного захисту);
- виключити можливість роботи на ЛРС, якщо вбудовані тести видають негативний результат під час її початкового завантаження;
- паролі, що призначаються користувачам, повинні відповідати вимогам відповідних інструкцій і нормативних документів;
- у випадку використання ЛРС декількома операторами з різними ключами не можна робити вивантаження ключової інформації (перезавантаження ЛРС).

При цьому забороняється:

- здійснювати несанкціоноване копіювання ключових носіїв;
- розголошувати вміст носіїв і ключової інформації чи передавати самі носії особам, що не мають до них допуску; виводити ключову інформацію на дисплей і принтер (за винятком випадків, передбачених даними правилами);
- вставляти ключовий гнучкий диск (чи інший ключовий носій) у дисковод ЛРС (чи в інший пристрій зчитування) у режимах, не передбачених штатним розкладом, а також у дисководи інших ЛРС;
- записувати на ключові носії сторонню інформацію;
- підключати до ЛРС додаткові пристрої і з'єднувачі, не передбачені в комплекті;
- працювати на комп'ютері, якщо під час його початкового завантаження не проходить вкладений тест ОЗП, передбачений у ЛРС;
- вносити будь-які зміни в програмне забезпечення СЗІ;
- несанкціоновано встановлювати, створювати і виконувати на ЛРС сторонні програми;
- використовувати в роботі колишні ключові носії для запису нової інформації без попереднього знищення на них ключової інформації;
- здійснювати несанкціоноване розкриття системних блоків ЛРС.

Контрольні питання

1. Наведіть класифікацію організаційно-технічних заходів захисту конфіденційної інформації.

2. Розкрийте суть технічних заходів захисту інформації.

3. Перелічіть основні задачі організаційно-технічного захисту інформації.

4. Опишіть причини можливого розголошення конфіденційної інформації.

5. Охарактеризуйте умови можливого розголошення конфіденційної інформації.

6. Наведіть класифікацію каналів розповсюдження інформації.

7. Поясніть особливості роботи щодо запобігання розголошенню закритої інформації.

8. Опишіть можливі джерела витоку інформації каналами ПЕМВІН.

9. Розкрийте причини виникнення каналів витоку інформації.

10. Опишіть суть заходів організаційного захисту інформації в інформаційних системах від витоку каналами ПЕМВІН.

11. Наведіть класифікацію способів несанкціонованого доступу до джерел конфіденційної інформації.

12. Розкрийте суть заходів захисту джерел конфіденційної інформації від спостереження і фотографування.

13. Поясніть особливості захисту джерел конфіденційної інформації від підслуховування.

14. Розкажіть про порядок забезпечення безпеки телефонних переговорів.

15. Охарактеризуйте методи захисту джерел конфіденційної інформації від перехоплення каналами побічних електромагнітних випромінювань і наведень.

16. Опишіть особливості організаційних заходів захисту джерел інформації від розголошення.

17. Розкрийте суть організаційних заходів захисту джерел конфіденційної інформації від несанкціонованого доступу.

18. Поясніть особливості організаційно-технічних заходів захисту джерел конфіденційної інформації від витоку технічними каналами.

Глава 5. СЛУЖБА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1. Загальні положення

У державних установах та організаціях можуть створюватись підрозділи, служби, які організують роботу, пов'язану із захистом інформації, підтримки рівня захисту інформації в автоматизованих системах (АС) і несуть відповідальність за ефективність захисту інформації відповідно до вимог чинного законодавства.

Склад, призначення і функції служби інформаційної безпеки визначаються індивідуально для кожної конкретної автоматизованої системи і залежать від вимог, що висуваються безпосередньо до інформаційних систем.

Служба інформаційної безпеки повинна:

- керуватися нормативно-методичною базою, де описані її склад, призначення і функції;
- діяти згідно зі встановленими заходами, тобто дотримуватись прийнятої в організації політики інформаційної безпеки;
- мати у своєму розпорядженні відповідні засоби, тобто технічне оснащення.

При цьому служба інформаційної безпеки повинна вирішувати такі задачі забезпечення безпеки інформації:

- визначення інформаційних і технічних ресурсів, що підлягають захисту;
- виявлення кількості потенційно можливих загроз і каналів витоку інформації;
- проведення оцінювання вразливості та ризиків інформації для наявних загроз і каналів витоку;
- визначення вимог до системи захисту;
- здійснення вибору засобів захисту інформації та їх характеристик;
- впровадження і організацію використання вибраних заходів, способів і засобів захисту;
- здійснення контролю цілісності та управління системою захисту.

Забезпечення безпеки інформації повинно здійснюватися за такими *напрямками:*

- захист об'єктів корпоративних систем;
- захист процесів, процедур і програм оброблення інформації;
- захист каналів зв'язку;
- послаблення побічних електромагнітних випромінювань;
- управління системою захисту.

Основу політики безпеки складає перелік обов'язкових заходів, спрямованих на розробку плану дій щодо інформаційного захисту об'єктів: визначення складу служби інформаційної безпеки, її місця в організаційній структурі підприємства, сфери її компетенції, прав і повноважень,

варіантів дій у різних ситуаціях для уникнення конфліктів між підрозділами.

Захисні заходи, як правило, направлені на забезпечення конфіденційності, цілісності та доступності інформації. Для режимних державних організацій на першому місці завжди стоїть конфіденційність відомостей, а цілісність розуміється виключно як їх незмінність. Комерційним структурам важливішим за все є цілісність і доступність даних та послуг для їх обробки. Порівняно з державними, комерційні організації більш відкриті і динамічні, тому можливі загрози для них відрізняються не тільки кількістю, але й якістю.

Використання якісних засобів захисту дозволить закрити більшість вразливих місць, якщо інформація про "діри" у системах безпеки оновлюється достатньо оперативно – в міру їх знаходження спеціальними групами експертів в області інформаційної безпеки.

Правильно відпрацьована методика проведення робіт із захисту інформації гарантує, що ні один аспект інформаційної безпеки не залишається без уваги.

5.2. Задачі служби інформаційної безпеки

Служба інформаційної безпеки повинна брати участь у роботах зі створення корпоративної системи з початку її проектування до моменту введення в експлуатацію. Разом з тим систему, що працює, необхідно періодично обстежувати з метою виявлення нових "слабких місць".

Розглянемо зміст деяких задач (рис. 9) служби інформаційної безпеки.

Рис. 9. Основні задачі служби інформаційної безпеки

1. Визначення інформаційних і технічних ресурсів, що підлягають захисту. Для розв'язання цієї задачі слід розглянути функції органів (осіб), відповідальних за визначення інформації (відомостей) і засобів, що підлягають захисту:

- на об'єктах інформаційної системи;
- при використанні їх у процесах і програмах;
- під час передавання каналами зв'язку;
- схильних до витоків за рахунок побічних електромагнітних випромінювань;
- у процесі управління системою захисту.

Сучасна система безпеки інформації була розроблена для документів у вигляді "твердих копій". Вся облікова інформація – вхідний номер, дата документа, кількість сторінок – відноситься до "твердих копій".

В останні роки інформаційні технології розвиваються з надзвичайною швидкістю. Оптимісти – користувачі цих нових технологій вважають, що папір буде замінений електронним розподіленням і збереженням інформації. Проте безпека інформації, незалежно від того, який носій (паперовий чи електронний) використовується, тісно пов'язана з загальним управлінням потоками інформації. Якщо в організації є чітке розподілення обов'язків, потоки інформації добре організовані, заходи безпеки інформації застосувати легко.

На жаль, часто буває так, що заходи безпеки інформації стають і заходами розподілення потоків інформації. Це може призвести до доволі громіздких процедур і викликати враження у співробітників, що заходи безпеки ускладнюють їх роботу.

Якщо доведеться створювати систему безпеки інформації, рекомендується спочатку придивитися до процедур розподілення інформації в цій організації.

В ідеальному варіанті організація повинна мати відділ (режимний) для приймання і відправлення всіх документів, повинні бути виразні інструкції про розподілення вхідних документів між співробітниками і про підготовку та затвердження вихідних документів.

Системне зберігання повинно забезпечувати доступність і постійне оновлення інформації з визначених питань. Всі передачі документів повинні реєструватися у відповідних журналах, щоб прийом (передача) документа були підтверджені і було ясно, звідки він прийшов чи куди направляється. На кожному документі повинен бути зафіксований вхідний та обліковий номер і дата. Із записів повинно бути видно, кому документ розписаний, де він знаходиться в даний момент і коли його підшито на зберігання. Якщо такі правила діють незалежно від ступеня секретності інформації, то заходи з безпеки інформації будуть введені легко.

2. Виявлення потенційно можливих загроз і каналів витоку інформації

Одним із найбільш вразливих місць будь-якої організації з точки зору безпеки інформації є її персонал і, відповідно, великого значення набувають грамотна реалізація внутрішньої політики і робота з персоналом.

Робота з персоналом передбачає:

- підбір і розстановку кадрів;
- адаптування працівника до нового колективу;
- розподілення задач і відповідальності;
- навчання і підвищення кваліфікації;
- мотивацію поведінки працівників;
- контроль за виконанням працівником покладених на нього функцій;
- моніторинг психологічного клімату в колективі;
- виявлення незадоволених своїм положенням і нелояльних працівників;
- звільнення працівників.

Серед перелічених задач до компетенції служби безпеки організації входить виявлення нелояльних співробітників (співробітників, які працюють на конкурента) і співробітників, незадоволених своїм положенням у колективі і тому потенційно готових працювати на конкурента.

3. Проведення оцінювання вразливості та ризиків для інформації і ресурсів ІС.

Для побудови надійного захисту необхідно виявити можливі загрози безпеці інформації, оцінити їх наслідки, визначити необхідні заходи і засоби захисту та оцінити їх ефективність.

Оскільки аналіз всієї інформаційної інфраструктури (особливо для великих об’єктів) не завжди виправданий з економічної точки зору, деколи буває доцільно зосередитися на найбільш важливих об’єктах, усвідомлюючи приблизність підсумкового оцінювання. З цих самих позицій слід оцінювати можливі загрози та їх наслідки.

Різноманітність потенційних загроз така велика, що не дозволяє передбачити кожну з них, тому види загроз, які будемо аналізувати, слід вибирати з позицій здорового глузду, одночасно виявляючи не тільки загрози, вірогідність їх здійснення, розмір потенційних втрат, але і їх джерела.

Оцінювання ризиків проводиться за допомогою різних інструментальних засобів, а також методів моделювання процесів захисту інформації. На основі результатів аналізу виявляються найбільш високі ризики, що вимагають прийняття додаткових захисних заходів. Як правило, для кожної подібної загрози існує декілька варіантів рішення для її нейтралізації.

При оцінюванні їх вартості та ефективності слід враховувати не тільки витрати на закупівлю обладнання і програмних засобів, але й такі обставини, як можливість екранування одним сервісом безпеки декількох прикладних, його сумісності з апаратно-програмною структурою організації, вартість навчання персоналу для роботи з ними.

4.Визначення вимог до систем захисту інформації.

На основі аналізу ризиків складається функціональна схема системи захисту інформації, заснована на задачах останньої, а також висунутих до неї вимог з урахуванням специфіки конкретного об'єкта. Дана схема разом з політикою безпеки, відповідальністю персоналу, порядком введення в дію засобів захисту, планом їх розміщення і модернізації складають план захисту.

Елементи системи захисту вибираються шляхом порівнювального аналізу технічних і економічних показників пропонованих на ринку засобів захисту, які розміщуються на об'єкті в суворій відповідності з розробленою схемою.

Загальні витрати на забезпечення інформаційної безпеки об'єкта відповідно до вимог захищеності визначаються у специфікаціях засобів реалізації плану захисту інформації. Слід враховувати, що пряме скорочення рекомендованих засобів захисту неминуче призведе до появи слабких місць у системі безпеки. У випадку відсутності засобів для повноцінної реалізації плану захисту необхідно або знижувати вимоги до захищеності об'єкта, або обновляти допустимі затрати на його захист перед початком робіт з обстеження.

5. Здійснення вибору засобів захисту інформації та їх характеристик.

Вирішенню організаційних питань передує етап робіт, який повинен відповісти на питання: що необхідно зробити для реалізації вибраної політики безпеки? Ринок засобів захисту інформації такий різноманітний за вартістю, призначенням і якістю продуктів, що вибір найбільш оптимальних з них для конкретного об'єкта є дуже непростою задачею.

6. Впровадження і організація використання вибраних заходів, способів і засобів захисту.

Впровадження і експлуатація системи захисту вимагають організаційно-технічної і організаційно-правової підтримки. Така підтримка передбачає розробку відповідних нормативних документів, керування засобами захисту, їх адміністрування і контроль за правильною експлуатацією, виявлення спроб і фактів несанкціонованого доступу до інформаційних ресурсів, підтримання безперервності процесу оброблення інформації.

В зв'язку з тим, що оброблення інформації на об'єкті здійснюється за децентралізованим принципом, управління системою захисту також не

може бути покладено виключно на службу інформаційної безпеки. Певну частину подібних функцій (експлуатацію засобів захисту, присвоєння ідентифікаторів користувачам, моніторинг функціонування комп'ютерних систем, аналіз реєстраційних журналів тощо) доцільно покласти на спеціально призначених співробітників тих підрозділів, в яких проводиться оброблення важливої інформації.

Умови для успішної реалізації задачі з впровадження і експлуатації системи захисту інформації полягають у забезпеченні належної організаційної підтримки та створенні підрозділу, виконуючого функції управління засобами захисту, контролю за правильною їх експлуатацією, дотримання плану захисту і плану забезпечення безперервної роботи та відновлення інформації, виявлення спроб і фактів несанкціонованого доступу до неї та прийняття заходів для їх нейтралізації.

7. Здійснення контролю цілісності та управління системою захисту.

План захисту необхідно щорічно переглядати, враховуючи зміну зовнішньої обстановки. Такий строк достатній для вчасного внесення необхідних змін, але тільки у тому випадку, якщо не виникають причини для позачергового перегляду, а саме:

- реорганізація організаційно-штатної структури підприємства;
- зміна територіального розміщення компонентів чи архітектури автоматизованої системи;
- модифікація використовуваного програмного забезпечення чи обчислювальної техніки.

Коли намічені заходи прийняті, необхідно перевірити їх дієвість, наприклад, провести автономне і комплексне тестування програмно-технічного механізму захисту. Якщо перевірка показує, що в результаті проведеної роботи залишкові ризики знизились до прийнятного рівня, то можна намічати дату найближчого переоцінювання, якщо ж ні, слід проаналізувати допущені помилки і провести повторне оцінювання ризиків.

5.3. Створення служби інформаційної безпеки

5.3.1. Критерії необхідності створення служби

Потрібна чи не потрібна служба інформаційної безпеки? Як визначити час, коли необхідно відповісти на це питання позитивно (якщо така служба ще не створена)? Це залежить від безлічі причин і умов, але перша стадія може визначатися, виходячи з комбінації таких пунктів:

- у вашій організації вже більше 10 комп'ютерів, розміщених у різних приміщеннях;
- у вашій організації створена локальна мережа;
- один з комп'ютерів вашої організації з'єднаний з модемом;

- ви зберігаєте/обробляєте на комп'ютері інформацію, втрата чи розголошення якої може принести вашій організації істотний збиток.

Чому кожний з перелічених пунктів вимагає уваги?

1. Якщо у вас досить багато комп'ютерів і до них має доступ значна кількість обслуговуючого персоналу, то необхідно задуматися про збереження вашого устаткування. Нехай у вас ще немає навіть локальної комп'ютерної мережі й у комп'ютерах немає ніякої істотної інформації – самі по собі вони є значною цінністю. Часом, міркуючи про питання інформаційної безпеки, фахівці випускають з уваги такий її аспект, як контроль фізичного доступу до інформаційних ресурсів. Тим часом, за існуючими оцінками, співвідношення маса/ціна в ряду комп'ютерних складових (наприклад, у плат оперативної пам'яті) порівняні зі співвідношенням маса/ціна золота. А це означає, що вони самі по собі є мішенню для зловмисників.

Продовжуючи приклад із платами оперативної пам'яті, можна привести типовий сценарій злочину – з 128 чи 256 Мбайт оперативної пам'яті викрадається половина (чи чверть). А тепер задумайтеся, чи усі ваші співробітники уважно стежать за процесом завантаження при вмиканні комп'ютера і здатні визначити, що оперативна пам'ять зменшилась? Чи кожний з них негайно повідомить, якщо комп'ютер став повільніше працювати? А може у вас є комп'ютери, які ніхто не вмикає по кілька днів? Через який термін тоді виявиться пропажа?

2. Якщо у вас з'явилася локальна мережа, це означає, що ви почали використовувати комп'ютери у виробничому процесі, навіть якщо ваші співробітники всього лише обмінюються файлами через спільно використовувані каталоги. Припустимо, що навіть при цьому ніякої істотної інформації у вашій мережі не має. Однак, як ви будете себе почувати, якщо виявиться, що ранком чергового дня жоден з ваших комп'ютерів не зможе завантажитися через помилку збою в операційній системі, тому що напередодні ввечері один з ваших співробітників запустив на своєму комп'ютері гру з піратського диска? Де в такому випадку взяти нехай не дуже важливий, але дуже великий звіт, який ви протягом останнього тижня готували в Microsoft Word?

3. У вас з'явився модем – його відразу ж спробують підключити до одного з комп'ютерів. Ну і що, скажете ви, телефонна мережа – це ще не Інтернет з його злісними хакерами. Але, може бути, нещодавно один з ваших співробітників купив своєму сину (який знає телефони батькових співробітників) домашній комп'ютер з модемом, а в того є диск із програмами, що скачав із сервера http://hackzone.ru/, і багато вільного часу. Чи не виявите ви одного дня ситуацію, аналогічну описаній у попередньому пункті?

4. Ви зберігаєте у своєму комп'ютері (навіть не підключеному до загальної локальної мережі) конфіденційну інформацію і вважаєте, що

вона захищена, тому що у вас стоїть пароль на включення комп'ютера, а сам комп'ютер знаходиться у вашому персональному кабінеті. А пароль – це, випадково, не номер вашого домашнього телефону? І чи завжди ви присутні в кабінеті, коли проводиться прибирання приміщень?

Якщо ви задумалися над цими питаннями, виходить, ви готові до створення відповідної служби чи наймання співробітника, якому треба їх переадресувати.

У розвинутих країнах на утримання служби безпеки виділяється до 20% чистого прибутку на рік. Таким чином, якщо фірма "заробляє" п'ять мільйонів на рік, то один мільйон може бути витрачений на службу безпеки.

Як же раціонально розподілити затрати? Практика діяльності деяких фірм у цій області показує, що на утримання фізичної охорони витрачається до 50%, на технічне оснащення – до 30%, на інші потреби служби безпеки – до 20% коштів.

Керівники великих виробничих підприємств і комерційних організацій утримують охорону чисельністю в декілька сотень чоловік. Оцінивши витрати на послуги охоронців, оплату керівників служби безпеки, придбання технічних засобів і оснащення захисту (охоронна і пожежна сигналізація, блокувальні замки, генератори шуму, криптографічна апаратура тощо) економісти можуть легко підрахувати, у скільки обійдеться утримання служби безпеки і зробити відповідні висновки про доцільність її створення.

Не завадить навести довідки про особу найманого до служби безпеки, зробити запит характеристик з попередніх місць роботи, отримати рекомендації від довірених осіб. Ефективний спосіб перевірки – випробувальний строк з відповідними дорученнями для кандидатів, коли доречно підготувати і провести декілька безневинних експериментів, під час яких можна пересвідчитися у наявності необхідних для цієї роботи якостей випробуваного, наприклад: знання законодавства, гарної професійної і фізичної підготовки, критичного творчого мислення, здатності швидко і глибоко аналізувати події тощо.

Бажаний ефект приносить і вчасне отримання достовірної інформації про клієнтів, передбачуваних партнерів і конкурентів, а також забезпечення угод кваліфікованими спеціалістами.

В зв'язку з тим, що до 80% випадків витоку інформації і втрати документів відбуваються з вини персоналу, служба безпеки ретельно проводить підбір і перевірку співробітників, навчає їх роботі з секретною інформацією

Служба інформаційної безпеки може мати відкриту і закриту області діяльності. Робота відкритого характеру пов'язана з підтриманням офіційних контактів з представниками інших підприємств, пресою, персоналом фірми. Закрита діяльність зазвичай не афішується. Це, як правило, прихована перевірка персоналу, виконання різних конфіденційних дору-

чень керівництва фірми.

Економічно виправданим для невеликих фірм, з метою забезпечення безпеки, є залучення спеціалізованих організацій, за допомогою яких професійно визначається об'єм послуг для захисту інформації і приймаються необхідні заходи.

З метою забезпечення прийнятого порядку захисту інформації всіма співробітниками необхідно розробити і довести до них чіткі, продумані правила, що визначають заходи забезпечення безпеки інформаційних технологій.

5.3.2. Формування складу служби інформаційної безпеки

Як створити таку службу "з нуля" і хто повинен входити до її складу?

Звичайно, відповіді на ці питання також залежать від самої організації, її цілей, від умов, у яких вона існує, і багатьох інших факторів. Як модель розглянемо досить велике підприємство, у якому описувані задачі і функції можуть бути розподілені між різними співробітниками служби інформаційної безпеки. Для більш скромних компаній різні ролі можуть поєднуватись меншою кількістю співробітників чи навіть одним.

Отже, склад служби. Потрібний, власне, керівник служби – той, хто буде визначати її загальну стратегію і тактику, звітувати керівництву, приймати оперативні рішення і нести за них відповідальність. Це повинен бути досить підготовлений фахівець, тому що йому необхідно:

1. Розбиратися загалом у технічних особливостях використовуваного інформаційного забезпечення (включаючи апаратне і програмне забезпечення, прийняті де-юре і де-факто методи роботи в інформаційному просторі організації тощо). Інакше він просто не буде розуміти, чим займаються його підлеглі, а ті, у свою чергу, зможуть маніпулювати своїм керівником.

2. Здійснювати наглядові функції як формалізовані, так і ні, у тому числі керування проектами, тому що впровадження багатьох механізмів безпеки (наприклад, таких як придбання і впровадження технічних рішень) потребує проектної роботи.

3. Розбиратися у психології працівників, уміти розв'язувати конфлікти (тому що служба безпеки часто сама є основою для репресивного чи обмежувального впливу). Можливо, доведеться використовувати слабкі чи сильні сторони окремих співробітників організації.

4. Знати основи діючого законодавства, тому що, можливо, доведеться проводити розслідування, у яких будуть фігурувати такі поняття, як "право приватної власності на інформацію", "докази і санкції", "свідчення" тощо.

5. Налагоджувати зв'язки як з колегами в інших організаціях, так і з вищими організаціями для захисту інтересів своєї компанії у відповідній

сфері.

6. Користуватися довірою керівництва, тому що за певного бажання можна створити таку ситуацію, коли на службу безпеки буде замкнуто багато того, що дасть можливість її керівнику використовувати свою посаду в особистих інтересах.

Підлеглі описаного вище "ідеального" керівника будуть фахівцями, підбір яких також необхідно здійснювати за різними критеріями. У першу чергу, варто враховувати характер функцій, які вони мають виконувати.

Операційний. Сюди входить виконання щоденних процедур із моніторинга мережі й окремих сервісів (додатків), інструктаж і реєстрація користувачів,

контроль виконання процедур (наприклад, резервного копіювання) тощо. Можна додати до переліченого також проведення розслідувань.

Дослідницький. Сюди входить вивчення поточної обстановки в інформаційному просторі, як найближчому, так і всесвітньому, аналіз нових можливостей і вразливостей. Можливо, тут буде проводитись вибір, розробка і впровадження нових технологій.

Методичний. Даний набір функцій є об'єднувальним між першими двома. Завершений проект з впровадження технології необхідно поставити на рейки щоденного рутинного функціонування, тобто забезпечити відповідними процедурами і порядками, нормативною і технічною документацією тощо. Ця ж група може проводити аналіз ризиків.

Тепер, коли керівник і фахівці підібрані, чи можна починати працювати? Не можна, а потрібно, тільки це ще буде не робота, а підготовка до неї.

Адже вам треба визначити:

- стратегію і тактику вашого захисту;
- що, від чого і як ви будете захищати;
- необхідні засоби для цього (у тому числі і фінансові);
- забезпечити необхідний нормативно-правовий простір.

5.4. Структура і обов'язки служби інформаційної безпеки

5.4.1. Структура служби інформаційної безпеки

До структури служби безпеки можуть входити (рис.10):

- директор (заступник директора) чи керівник, безпосередньо підпорядкований голові фірми;
- заступник начальника служби безпеки – на деяких підприємствах він керує фізичною, а деколи і технічною службою охорони;
- аналітик;
- юрист;
- спеціалісти в області забезпечення безпеки, економічної розвідки, промислової контррозвідки;
- технічні спеціалісти, що вміють застосовувати спеціальну техніку для захисту приміщень;
- співробітники фізичної охорони і пропускного режиму (за наймом), підпорядковані керівнику служби безпеки.

Умовно співробітників служби інформаційної безпеки можна поділити за функціональними обов'язками:

Співробітник групи безпеки. До його обов'язків входить забезпечення контролю за захистом набору даних і програм, допомога користувачам і організація загальної підтримки груп управління захистом і менеджменту у своїй зоні відповідальності. При децентралізованому

управлінні кожна підсистема ІС має свого співробітника групи безпеки.

Адміністратор безпеки системи. До його обов'язків входить щомісячне опублікування нововведень в області захисту, нових стандартів а також контроль за виконанням планів безперервної роботи і відновленням (за необхідності) роботи та за зберіганням резервних копій.

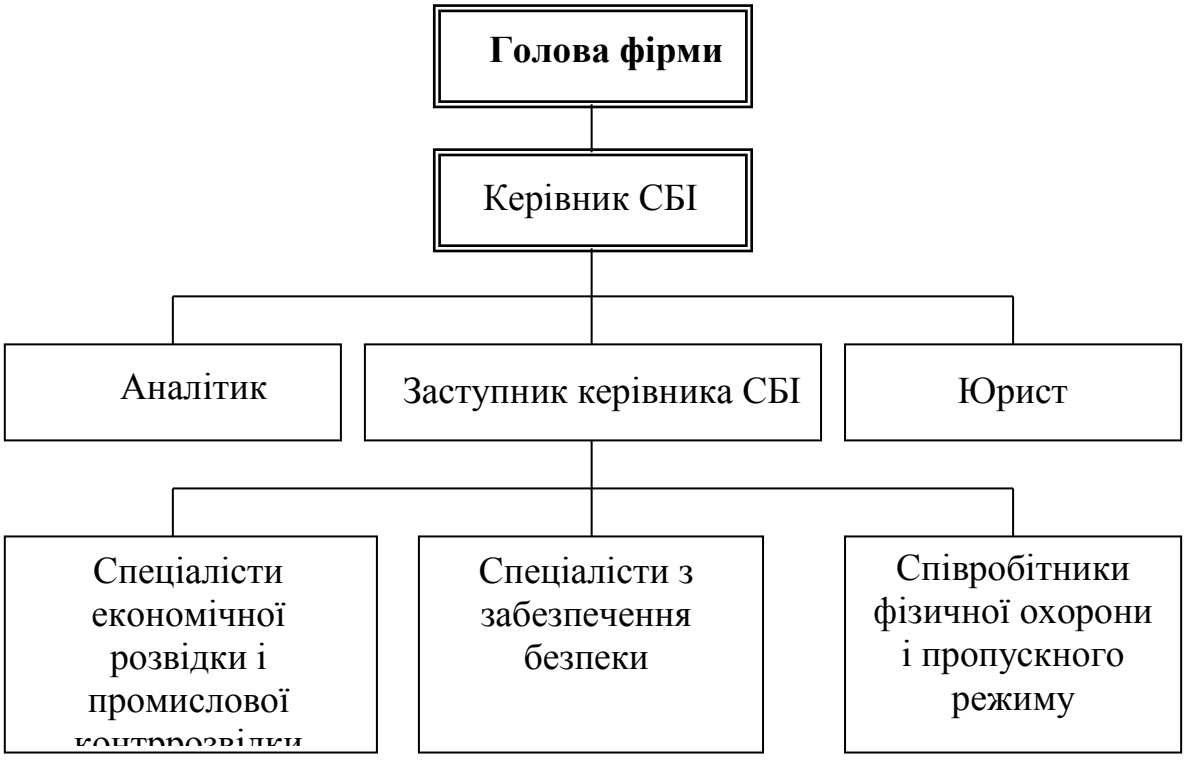

Рис. 10. Структура служби захисту інформації

Адміністратор безпеки даних. До його обов'язків входить реалізація і зміна засобів захисту даних, контроль за станом захисту набирання даних, посилення захисту за необхідності, а також координування роботи з іншими адміністраторами.

Керівник групи. До його обов'язків входить розробка і підтримка ефективних заходів захисту при обробці інформації, обладнання і програмного забезпечення; контроль за виконанням плану відновлення і загальне керівництво адміністративними групами у підсистемах ІС (при децентралізованому управлінні).

У невеликих організаціях функції керівника служби, зазвичай, виконує або голова фірми, або його замісник.

Кількісний склад служби безпеки різний і залежить, перш за все, від можливостей самої фірми. Можливі різні варіанти складу такої групи. Окрім того, перелік необхідних знань і навиків, а також функціональних

обов’язків осіб, що входять до групи захисту інформації, також може істотно відрізнятися залежно від призначення, структури і задач, вирішуваних у конкретній інформаційній системі.

5.4.2. Організаційно-правовий статус служби інформаційної безпеки

- Чисельність служби захисту повинна бути достатньою для виконання всіх перелічених функцій;
- служба захисту повинна підпорядковуватися тій особі, яка у даному закладі несе персональну відповідальність за дотримання правил поводження з інформацією, що захищається;
- штатний склад служби захисту не повинен мати інших обов’язків, пов’язаних з функціонуванням ІС;
- співробітники служби захисту повинні мати право доступу у всі приміщення, де встановлена апаратура ІС і право припиняти автоматизоване оброблення інформації за наявності безпосередньої загрози для інформації, що захищається;
- керівнику служби захисту повинно бути надано право забороняти включення до числа діючих нових елементів ІС, якщо вони не відповідають вимогам захисту інформації;
- служба захисту інформації повинна мати всі умови, необхідні для виконання своїх функцій.

5.4.3. Обов’язки служби інформаційної безпеки

Основною задачею служби інформаційної безпеки є визначення напрямку розвитку і підтримки зусиль організації, спрямованих на захист інформації від несанкціонованого ознайомлення, змінення чи руйнування. Це досягається шляхом впровадження відповідних правил, інструкцій і вказівок.

Служба інформаційної безпеки відповідає за:

- розробку і видання правил (інструкцій і вказівок) забезпечення безпеки, відповідних загальним правилам роботи організації і вимогам до обробки інформації;
- впровадження програми забезпечення безпеки, включаючи класифікацію ступеня секретності інформації (якщо така є) і оцінювання діяльності;
- розробку і забезпечення виконання програми навчання і ознайомлення з основами інформаційної безпеки в масштабах організації;
- відбір, впровадження, перевірку і експлуатацію відповідних методик планування відновлення роботи для всіх підрозділів організації, що беруть участь в автоматизованій обробці

найважливішої інформації;
- розробку переліку мінімальних вимог до процедур контролю за доступом до всіх комп'ютерних систем, незалежно від їх розмірів;
- розробку і впровадження процедур перегляду правил забезпечення інформаційної безпеки, а також робочих програм, призначених для дотримання правил, інструкцій, стандартів і вказівок організації;
- участь в описуванні, конструюванні, створенні та придбанні систем з метою дотримання правил безпеки при автоматизації виробничих процесів;
- вивчення, оцінювання, вибір і впровадження апаратних і програмних засобів, функцій і методик забезпечення інформаційної безпеки, застосовуваних для комп'ютерних систем організації.

За необхідності на службу інформаційної безпеки покладається виконання інших обов'язків, а саме:

- формування вимог до системи захисту в процесі створення інформаційної системи;
- участь у проектуванні системи захисту, її випробовуваннях і прийомі в експлуатацію;
- планування, організація і забезпечення функціонування системи захисту інформації в процесі функціонування ІС;
- розподілення між користувачами необхідних реквізитів захисту;
- спостереження за функціонуванням системи захисту та її елементів;
- організація перевірок необхідності функціонування системи захисту;
- навчання користувачів і персоналу ІС правилам безпечного оброблення інформації;
- контроль за дотриманням користувачами і персоналом ІС встановлених правил поводження з інформацією, що захищається в процесі її автоматизованого оброблення;
- прийняття заходів при спробах несанкціонованого доступу до інформації і при порушенні правил функціонування системи захисту.

5.4.4. Контроль функціонування служби інформаційної безпеки

Тим, хто збирається контролювати роботу служби інформаційної безпеки, слід, у першу чергу, ознайомитися з організаційною структурою підприємства і місцем у ній служби безпеки. Далі потрібно спиратися на наявний досвід перевірки роботи інших підприємств і підрозділів або на логічне мислення. Зрештою, всі організаційні схеми, у тому числі й оптимальні, придумують люди і людина з аналітичним складом розуму

може розібратися в їхніх принципах.

Якщо при проведенні перевірки виникають питання доцільності організації роботи сформованим способом, необхідно отримати роз'яснення, на підставі чого було прийняте саме таке рішення. Цілком можливо, що це обумовлено специфікою роботи підприємства.

Для проведення перевірки доцільно розглянути таке коло питань:

- у рамках якої структури функціонує служба інформаційної безпеки;
- кому підпорядковується служба і як відбувається прийняття рішень;
- як співвідносяться один з одним служба інформаційної безпеки і підрозділ інформаційних технологій;
- до яких інформаційних систем має доступ служба безпеки і з якими правами, як ці права співвідносяться з правами адміністратора системи;
- які правила інформаційної безпеки для різних категорій користувачів;
- чи бере участь служба безпеки в розробці проектів нових інформаційних систем;
- як контролюється статус працівника (прийнятий на роботу, звільнений, хворий, у відпустці, у відрядженні тощо).

При відповідях на ці питання необхідно з'ясувати, чому було зроблено саме так, а не інакше і як можна оптимізувати функціонування служби.

5.5. Взаємодія служби інформаційної безпеки зі службою інформаційних технологій

5.5.1. Питання підпорядкування і взаємодії служб

Інтеграція служби безпеки з іншими суб'єктами спрямована на здійснення контролю з боку служби безпеки, причому адміністратори і розробники повинні самі брати участь у винаході механізмів їхнього контролю. Цей процес повинен бути двостороннім. Відомо, що безконтрольність навіть стосовно самих довірених осіб, провокує нестійкі особистості до можливих зловживань. Крім того, створювати драбинку "перевіряючих над перевіряючими" також не завжди доцільно, оскільки у цьому випадку "верхня" служба все-таки знаходиться поза контролем. Найкращим способом контролю є створення можливості перехресної перевірки, скажімо, контролерів (фахівців з безпеки) і адміністраторів, причому перевірка контролерами адміністраторів носить характер обов'язку, а перевірка адміністраторами контролерів носить характер можливості. Тобто вона не входить до обов'язків адміністратора, але, проте, може проводитися за його розсудом регулярно чи вибірково. У

даному випадку важливу роль відіграє не сама перевірка, а саме її можливість, що дисциплінує контролюючого.

Прикладом може бути контроль корпоративного використання Інтернету. Співробітник, що перевіряє, щоб працівники організації не використовували корпоративний канал для відвідування розважальних та інших, не пов'язаних з роботою, Веб-сайтів, може також мати доступ до Інтернету. Таким чином, необхідно фіксувати його інтернет-активність у реєстраційному журналі, який повинен бути доступний для читання, наприклад, адміністратору домена-доступу до Інтернету чи іншому адміністратору. Відповідно, адміністратор із правами контролера в будь-який момент зможе проконтролювати те, як сам контролер Інтернету використовує довірений йому ресурс. Якщо для аналізу реєстраційних журналів сервісу використовується яке-небудь додаткове програмне забезпечення, воно також повинно бути у розпорядженні адміністратора. Очевидно, що і для перевірок адміністратором контролера також необхідно установити певний регламент.

Ще одним важливим моментом є розміщення служби інформаційної безпеки в структурі організації. Конкретне місце розташування служби в ієрархії комерційної структури може бути різним і залежати від безлічі факторів – особливостей самого бізнесу і способів його ведення, традицій організації, місцевості і країни, персональних переваг і якостей керівника організації, керівника служби і багатьох інших факторів. Однак є питання, на які варто звернути увагу при плануванні структурного розміщення.

Служби інформаційних технологій і інформаційної безпеки не повинні мати принципово різних цілей, у положенні про підрозділи необхідно вказати взаємопідтримувальні, що погоджують і доповнюють, риси.

Підпорядкованість служб керівникам, що знаходяться в персональному конфлікті, є негативним фактором.

Доцільно (за наявних можливостей) розміщати ключових фахівців безпеки й адміністраторів в одному будинку, на одному поверсі, у сусідніх приміщеннях, забезпечувати спільну їхню участь у семінарах, навчанні тощо.

Уповноважені фахівці служби інформаційної безпеки повинні мати можливість прямого звертання до керівника організації чи його найближчого заступника.

Для забезпечення ефективної роботи можливі більш вигадливі комбінації, коли фахівець з інформаційної безпеки знаходиться у штаті підрозділу інформаційних технологій і за звичайною діяльністю (трудовий розпорядок, відрядження тощо) підлеглий начальнику ІС, але з інцидентів безпеки прямо підзвітний тільки керівнику організації.

У будь-якому випадку той чи інший формат роботи служби інформаційної безпеки повинен бути строго регламентований і націлений на загальну зі всією організацією мету в бізнесі.

Усі працівники організації повинні бути впевнені, що служба безпеки проводить ті чи інші заходи (особливо, пов'язані з вторгненням у персональний робочий простір і, тим більше, репресивні) не через свої примхи, а відповідно до правил та інструкцій, що схвалені керівництвом і доступні для ознайомлення всім працівникам.

Залежно від того, як служба інформаційної безпеки поставить себе відносно інших суб'єктів інформаційного простору, її робота може бути більш-менш ефективною. Вона може стати каральним органом для інших співробітників підприємства або захисником їхніх інтересів.

Питання це прямо не пов'язане з технічними особливостями функціонування інформаційних систем, однак може істотно впливати на забезпечення інформаційної безпеки. Воно також пов'язане з побудовою моделі зловмисника. Статистика показує, що значна частина порушень інформаційної безпеки робиться або самими співробітниками організації, або за їх участі. З цієї причини очевидно, що "внутрішній ворог" повинен ввійти у модель зловмисника.

Загалом специфіка проблеми зводиться до того, що розглядається кожен працівник як зловмисник чи ні. Тут дуже важливо "не перегнути ціпок" і не перетворити всіх користувачів, адміністраторів тощо у потенційних зловмисників, дуже багато залежить від персоналу служби безпеки і її керівника. Завжди варто пам'ятати, що бізнес первинний, а безпека відносно нього вторинна (мова йде про комерційні установи, а не про армійські і спеціальні установи). У першу чергу організація повинна працювати, а потім уже піклуватися про безпеку. Тобто необхідно побудувати роботу з безпеки таким чином, щоб вона не заважала веденню бізнесу.

Як правило, фахівці інформаційної безпеки:

- мають повний контроль над інформаційною системою, рівний правам адміністратора системи;
- мають доступ в інформаційній системі до всіх об'єктів, але мають право тільки читати зведення про них;
- не мають доступу в систему, використовують для контролю роботи адміністраторів реєстраційні журнали, конфігураційні звіти тощо.

Усі ці варіанти зазначені навмисно, тому що питання взаємин служби безпеки і, скажімо, адміністратора локальної мережі може бути дуже напруженим, особливо якщо служба тільки створюється, а адміністратор уже кілька років виконував свої функції. Як бути, якщо адміністратор дійсно чесно працює тривалий час, а фахівці з безпеки тільки прийшли в організацію, вимагають значних прав у системі для себе й обмеження прав адміністратора? Що робити, якщо адміністратор у цьому випадку вирішив залишити організацію? А коли кваліфікація фахівців з безпеки у конкретній інформаційній системі значно нижча, ніж в адміністратора і вони можуть, за наявності визначених прав, внести

перешкоди в роботу системи? А коли система влаштована таким чином, що для того, щоб контролювати адміністратора, необхідний повний контроль над усією системою? Питань більше, ніж відповідей, рішення необхідно приймати з урахуванням усіх цих проблем.

Можливо, хворобливий процес передачі чи поділу прав доведеться розтягти на тривалий період, доки фахівці служби безпеки не набудуть відповідного досвіду, а адміністратори поступово не звикнуть до часткового, а потім і повного контролю.

5.5.2. Робота з користувачами

Відомо, що самий безпечний корабель – той, котрий стоїть на березі, а, з іншого боку, найпростіше працювати, коли у співробітників немає ніяких обмежень і сторонніх зобов'язань, не пов'язаних безпосередньо з бізнес-діяльністю (необхідність запам'ятовувати паролі, виконувати складні процедури входу в інформаційну систему, проводити періодичні заходи щодо підвищення рівня безпеки тощо). Ідеальна ситуація для служби безпеки – коли всі комп'ютери виключені, мережа відрізана від зовнішнього світу, приміщення порожні, замкнені й опечатані. Для інших працівників ідеальною є ситуація прямо протилежна – у вигляді повної відсутності вимог безпеки. З такими суперечливими цілями побудова безпеки –складний процес, майже мистецтво. Таким чином, служба безпеки повинна виступати не як цербер, що примушує працівників виконувати складні, незрозумілі заходи, а як помічник, який бере на себе значний вантаж щодо забезпечення безпеки, у тому числі даного конкретного працівника, і який очікує, що працівник буде співробітничати з нею, а не протидіяти її вимогам.

Дуже важливо налагодити прямий і зворотний зв'язок з користувачем, привчити його у випадку будь-яких підозрілих чи просто незрозумілих подій консультуватися з представниками служби безпеки. Служба безпеки у відповідь повинна демонструвати, що звертання користувача не пропадають у "чорній дірі", а приносять свої, нехай невеликі, результати. Очевидно, що при такому підході з'являється велика ймовірність помилкових спрацьовувань. Приклад тому – звертання користувача в антивірусну службу у випадку появи повідомлення Doctor Watson при збоях додатків у середовищі Windows. Однак не можна, ґрунтуючись на низькій кваліфікації користувача в області інформаційних технологій, ігнорувати чи принижувати значимість подібних повідомлень. Краще мати повну картину інформаційного простору, із зайвими чи навіть другорядними деталями, аніж не мати її взагалі.

Гарний контакт із користувачами можна налагодити під час семінарів чи занять з основ інформаційної безпеки, які варто проводити регулярно, а також у бесідах чи інтерв'ю при прийомі на роботу.

5.5.3. Робота з адміністраторами

Адміністратори інформаційних систем, як правило фахівці високої кваліфікації, з невдоволенням відносяться до вторгнення в сферу їхньої роботи, особливо коли метою вторгнення є контроль роботи адміністраторів з імовірністю подальшого покарання за які-небудь порушення. Грубе втручання в їхню роботу, особливо з боку фахівця з безпеки з більш низькою кваліфікацією в якій-небудь конкретній області, ніж у адміністратора (а таке зустрічається досить часто, тому що адміністратор, звичайно, проводить набагато більше часу за вивченням можливостей конкретної інформаційної системи), може призвести до опору з боку даної категорії працівників керування. Півбіди, якщо опір буде пасивним, у вигляді небажання поділитися знаннями і навичками роботи у системі. Набагато гірше, коли скривджений адміністратор, для того щоб виставити фахівця з безпеки в безглуздому вигляді, спеціально починає створювати вразливості і знижувати безпеку даної системи.

Розумним засобом у такому випадку буде залучення адміністратора до розробки моделі безпеки даної інформаційної системи як експерта і консультанта. Необхідно запропонувати йому самому визначити найбільш тонкі й уразливі місця системи і вислухати його пропозиції щодо посиленню їхньої безпеки. Дії фахівця з безпеки (звичайна назва контролера системи безпеки інформаційної системи) даної системи необхідно побудувати за можливістю так, щоб не тільки він сам контролював дії адміністратора, але й адміністратор міг, за бажання, перевірити дії фахівця з безпеки, наприклад, за реєстраційним журналом системи. Можливо, найкращим рішенням буде зворотний спосіб, коли адміністратор має можливість будь-яких дій (відповідно до його функціональних обов’язків) у системі, однак усі його дії є предметом аналізування фахівцями служби безпеки (за допомогою, скажімо, реєстраційних журналів). У загальному випадку це може бути виражено формулою: "Адміністратор – повний доступ, фахівець з безпеки – доступ на читання".

У випадках, коли адміністратор був залучений до процесу розроблення моделі безпеки, він сам стає учасником процесу контролю роботи системи і, звичайно, варто розраховувати на його співробітництво. Якщо ж у процесі подальшого вивчення системи буде виявлено, що адміністратор цілеспрямовано приховав чи навіть створив уразливість, то цього буде достатньо, щоб підняти питання про доцільність його роботи на посаді адміністратора.

Всі заходи щодо контролю адміністратора (чи взаємного контролю адміністратора і фахівця з безпеки) повинні супроводжуватися відповідними нормативними документами. Усе це знизить ризик можливого конфлікту і забезпечить якісну обстановку для функціонування інформаційної безпеки.

5.5.4. Робота з розробниками

Розробники відрізняються від адміністраторів тим, що другі працюють у системах, розроблених третьою стороною; про механізми і схеми функціонування таких систем можна довідатися з документації, курсів, у виробника тощо , а перші самі є творцями механізмів функціонування систем і в плані інформаційної безпеки мають більше можливостей для маніпулювання ресурсами системи.

Для забезпечення високої ефективності роботи служби інформаційної безпеки фахівець з інформаційної безпеки повинен стати складовою частиною робочої групи розробки проекту нового програмного забезпечення. При цьому він повинен мати достатню кваліфікацію для читання коду, навички роботи з налагоджувальником (дизассемблером), оскільки, можливо, функціональність деяких найбільш важливих частин коду, таких як стадії автентифікації, авторизації, аудиту, доведеться перевіряти від рядка. Також необхідно разом з розробниками розробити процедури тестування механізмів безпеки, причому врахувати можливість перспективного проведення незалежної сертифікації продукту на безпеку третьою стороною.

Контрольні питання

1. Поясніть суть етапів розв’язання задач, що стоять перед службою захисту інформації.
2. Охарактеризуйте напрямки забезпечення безпеки інформації.
3. Розкажіть про особливості заходів захисту інформації в державних і комерційних організаціях.
4. Наведіть класифікацію основних задач служби інформаційної безпеки.
5. Опишіть особливості виявлення потенційно можливих загроз і каналів витоку інформації.
6. Охарактеризуйте порядок проведення оцінки вразливості та ризиків для інформації і ресурсів ІС.
7. Розкажіть про особливості визначення вимог до систем захисту інформації.
8. Розкрийте суть вибору та впровадження і експлуатації засобів захисту інформації.
9. Опишіть особливості створення служби інформаційної безпеки для великих і малих підприємств.
10. Охарактеризуйте вимоги до особи найманого в службу безпеки працівника.
11. Розкажіть про основні обов’язки служби інформаційної безпеки.

12. Дайте характеристику організаційно-правового статусу служби захисту інформації.

13. Наведіть класифікацію структури служби інформаційної безпеки.

14. Розкажіть про функціональні обов'язки співробітників служби безпеки.

Глава 6. ОРГАНІЗАЦІЙНИЙ ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ

6.1. Політика інформаційної безпеки

Політика інформаційної безпеки – *набір законів, правил, практичних рекомендацій і практичного розвитку, що визначають управлінські та проектні рішення в галузі захисту інформації.* На основі політики інформаційної безпеки будується управління, захист і розподілення критичної інформації в системі. Вона повинна охоплювати всі особливості процесу оброблення інформації, визначаючи поведінку ІС у різних ситуаціях.

6.1.1. Принципи політики безпеки

Розробляючи політику безпеки та втілюючи її в життя доцільно керуватися такими принципами.

1. *Принцип неможливості минути захисні засоби* означає, що всі інформаційні *потоки* в мережу, що захищається, і з неї *повинні проходити* через СЗІ, не повинно бути "таємних" модемних входів чи тестових ліній, що йдуть обминаючи екран.

2.*Надійність будь-якої СЗІ визначається найслабкішою ланкою.* Часто такою ланкою є не комп'ютер, а людина і тоді проблема забезпечення інформаційної безпеки набуває нетехнічного характеру.

3. *Принцип недопустимості переходу у відкритий стан* означає, що за будь-яких обставин (навіть нештатних), СЗІ або повністю виконує свої функції, або повинна повністю блокувати доступ.

4. *Принцип мінімізації привілеїв* пропонує виділяти користувачам і адміністраторам тільки ті права доступу, які необхідні їм для виконання службових обов'язків.

5. Принцип розподілу обов'язків передбачає таке розподілення ролей і відповідальності, при якому одна людина не може порушити критично важливий для організації процес. Це особливо важливо для запобігання зловмисним чи некваліфікованим діям системного адміністратора.

6. *Принцип багаторівневого захисту* пропонує не покладатися на один захисний рубіж, яким би надійним він не здавався. За засобами фізичного захисту повинні бути програмно-технічні засоби, за ідентифікацією і автентифікацією – керування доступом і, як останній

рубіж, – протоколювання і аудит. Ешелонована оборона захисту здатна, у крайньому випадку, затримати зловмисника, а наявність такого рубежу, як протоколювання і аудит істотно утруднює непомітне виконання зловмисних дій.

7. *Принцип різноманітності захисних засобів* рекомендує організовувати різні за своїм характером оборонні рубежі, щоб від потенційного зловмисника вимагалося володіння різноманітними і, за можливістю, несумісними між собою навичками подолання СЗІ.

8. *Принцип простоти і керованості інформаційної системи у цілому і СЗІ, зокрема*, визначає можливість формального чи неформального доведення коректності реалізації механізмів захисту. Тільки у простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.

9. *Принцип загальної підтримки законів безпеки* носить нетехнічний характер. Рекомендується з самого початку передбачити комплекс заходів, спрямованих на забезпечення лояльності персоналу, на постійне теоретичне і, головне, практичне навчання.

6.1.2. Види політики безпеки

Основу політики безпеки складає спосіб керування доступом, який визначає порядок доступу суб'єктів системи до об'єктів системи. Назва цього способу, як правило, визначає назву політики безпеки.

Нині найкраще вивчені два види політики безпеки, засновані відповідно на вибірковому і повноважному способах керування доступом.

Основою вибіркової політики безпеки є вибіркове керування доступом, яке припускає, що:

- всі суб'єкти і об'єкти системи повинні бути ідентифіковані;
- права доступу суб'єктів до об'єктів системи визначаються на основі деякого правила (властивість вибірковості).

Для опису властивостей вибіркового керування доступом застосовується модель системи на основі **матриці доступу,** інколи її називають матрицею контролю доступу. Така модель отримала назву матричної.

Матриця доступу – це прямокутна матриця, в якій об'єкту системи відповідає рядок, а суб'єкту – стовпець. На перетині стовпця і рядка матриці указується тип дозволеного доступу суб'єкта до об'єкта, як "доступ на читання", "доступ на записування", "доступ на виконання" тощо.

Вибіркова політика безпеки найширше застосовується у комерційному секторі, оскільки її реалізація на практиці відповідає вимогам комерційних організацій з розмежуванням доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати.

Основу повноважної політики безпеки складає повноважне керування доступом, яке припускає, що:

- всі суб'єкти і об'єкти системи повинні бути однозначно ідентифіковані;
- кожному об'єкту системи присвоєна мітка критичності, що означає цінність інформації, яка міститься у ньому;
- кожному об'єкту системи присвоєний рівень прозорості, що означає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

Коли сукупність міток має однакове значення, кажуть що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру і, таким чином, у системі можна реалізовувати ієрархічно висхідний потік інформації (наприклад, від рядових виконавців до керівництва). Чим важливіший об'єкт чи суб'єкт, тим вище його мітка критичності. Тому найбільш захищеними виявляються об'єкти з найбільш високим значенням мітки критичності.

Основне призначення повноважної політики безпеки – регулювання доступу суб'єктів системи до об'єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії в нижні, а також блокування можливого проникнення з нижніх рівнів у верхні. При цьому вона функціонує на фоні вибірної політики, надаючи її вимогам ієрархічно упорядкованого характеру (згідно з рівнем безпеки).

6.1.3. Політика безпеки для Internet

Щоб правильно врахувати можливі наслідки підключення до Internet потрібно відповісти на такі питання:

- чи можуть хакери зруйнувати внутрішні системи?
- чи може бути скомпрометована (замінена чи прочитана) важлива інформація організації при її передачі по Internet?
- чи можливо перешкодити роботі організації?

Мета політики безпеки для Internet – прийняти рішення про те, як організація передбачає захищатися. Політика інформаційної безпеки, зазвичай, складається з двох частин – загальних принципів і конкретних правил роботи. Загальні принципи визначають підхід до безпеки в Internet. Правила ж визначають що дозволено, а що заборонено. Правила можуть бути доповнені конкретними процедурами та різними рекомендаціями.

Система Internet при проектуванні не планувалася як захищена мережа, тому її ***проблемами є:***

- *легкість перехоплення даних* і фальсифікації адрес та шин у мережі – основна частина трафіка Internet – це нешифровані дані. E-mail, паролі і файли можуть бути перехоплені шляхом використання доступних програм;

- *вразливість засобів TCP/IP* – ряд засобів TCP/IP спроектовано незахищеними і це може бути скомпрометовано кваліфікованими зловмисниками; засоби, використовувані для тестування, особливо вразливі;
- *відсутність політики* – багато сайтів сконструйовані так, що надають широкий доступ до себе з боку Internet, не враховуючи можливості зловживання цим доступом; багато сайтів дозволяють роботу більшій кількості сервісів TCP/IP, ніж їм необхідно для роботи, і не намагаються обмежити доступ до інформації про свої комп'ютери, якою можуть скористатися зловмисники;
- *складність конфігурації* – засоби управління доступом до ***хосту*** складні; часто важко правильно сконфігурувати і перевірити складність установок. Засоби, що неправильно сконфігуровані, можуть призвести до неавторизованого доступу.

6.2. Основні напрямки захисту інформаційних систем

Для конкретної ІС політика безпеки повинна бути індивідуальною. Вона залежить від технології оброблення інформації, використовуваних програмних і технічних засобів, структури організації тощо.

Слід розглядати такі *напрями захисту* ІС (рис.11):

- захист об'єктів інформаційної системи;
- захист процесів, процедур і програм оброблення інформації;
- захист каналів зв'язку;
- подавлення побічних електромагнітних випромінювань;
- контролю та управління системою захисту.

Рис.11. Основні напрямки захисту інформаційних систем

Забезпечення захисту ІС за вказаними напрямками досягається організаційно-режимними, організаційно-технічними та організаційно-правовими заходами, здійснюваними в процесі створення і експлуатації системи.

Наскільки важливі *організаційно-режимні* заходи у загальному арсеналі засобів захисту, говорить уже хоча б той факт, що ні одна ІС не може функціонувати без участі обслуговувального персоналу. Окрім того, організаційно-режимні заходи охоплюють всі структурні елементи системи захисту на всіх етапах їх життєвого циклу: будівництво приміщень, проектування системи, монтаж і налагодження обладнання, випробовування і перевірка в експлуатації апаратури, оргтехніки, засобів оброблення і передавання даних.

Організаційно-режимні заходи захисту базуються на законодавчих і нормативних документах з безпеки інформації і повинні охоплювати *основні шляхи збереження інформаційних ресурсів* (рис.12):

- обмеження фізичного доступу до об’єктів оброблення і зберігання інформації та реалізація режимних заходів;
- обмеження можливості перехоплення інформації внаслідок створення фізичних полів;
- обмеження доступу до інформаційних ресурсів та інших елементів системи оброблення даних шляхом встановлення правил розмежування доступу, криптографічного закриття каналів передавання даних, вживляння і знищення “закладок”;
- створення твердих копій на випадок втрати масивів даних;
- проведення профілактичних та інших заходів від проникнення “вірусів”.

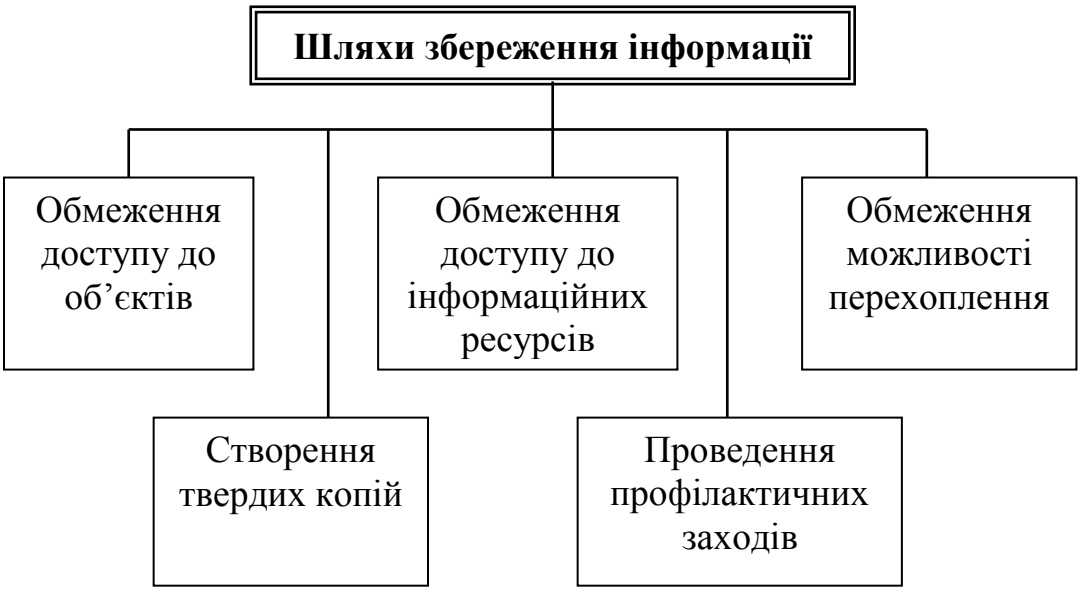

Рис.12. Основні шляхи збереження інформаційних ресурсів в ІС

За змістом усі організаційні заходи поділяють на три групи.

1. Заходи, здійснювані при створенні ІС. Вони спрямовані на реалізацію вимог захисту під час:

- розробки загального проекту системи та її структурних елементів;
- будівництва чи переобладнання приміщень;
- розробки математичного, програмного, інформаційного чи лінгвістичного забезпечення;
- монтування та налагодження обладнання;
- випробовування та прийманні системи.

2. *Заходи, здійснювані в процесі експлуатації ІС:*

- організація пропускного режиму;
- організація автоматизованого оброблення інформації;
- організація ведення протоколів;
- розподілення реквізитів розмежування доступу (паролів, повноважень тощо);
- контроль виконання вимог службових інструкцій тощо.

3. *Заходи загального характеру:*

- урахування вимог захисту при підборі та підготовці кадрів;
- організація перевірок механізму захисту;
- планування заходів із захисту інформації;
- навчання персоналу;
- проведення занять із залученням спеціалістів провідних організацій;
- участь у семінарах і конференціях з проблем безпеки інформації тощо.

Крім цього політика інформаційної безпеки повинна передбачати такі *етапи створення систем захисту інформації:*

- визначення інформаційних і технічних ресурсів, які необхідно захищати (інвентаризація інформаційної системи);
- виявлення потенційно можливих загроз і каналів витоку інформації;
- проведення оцінювання вразливості та ризиків за наявності загроз та каналів витоку;
- визначення вимог до системи захисту;
- здійснення вибору засобів захисту інформації та їх характеристик;
- впровадження і організація використання вибраних заходів, способів і засобів захисту;
- здійснення контролю цілісності та управління системою захисту.

6.3. Інвентаризація інформаційних систем

6.3.1. Загальний підхід до інвентаризації інформаційних систем

Інвентаризація – це складання переліку об'єктів, що підлягатимуть захисту і суб'єктів, які задіяні у даному інформаційному просторі і будуть впливати на інформаційний захист системи. При цьому необхідно не просто скласти перелік, а вказати ряд особливостей об'єктів і суб'єктів, тобто коротко описати їх з погляду інформаційної безпеки. Чим ретельніше зробити це на початковому етапі, тим легше буде далі робити уточнення і будувати остаточну модель захисту.

Дана робота, зазвичай, ініціюється службою інформаційної безпеки, але виконується з залученням фахівців інших служб.

Це відбувається тому, що фахівці з безпеки, швидше за все, не мають повного бачення моделі і способів функціонування конкретного об'єкта чи інформаційної системи такими, як адміністратор системи чи її активні користувачі.

Проведення інвентаризації рекомендується у такий спосіб. На першому етапі уповноважений фахівець служби інформаційної безпеки складає, за необхідності консультуючись з підрозділом інформаційних технологій, загальний перелік об'єктів/систем і пов'язаних з ними суб'єктів. Потім у цей перелік вносяться первинні характеристики об'єктів з метою їх описання саме з погляду інформаційної безпеки. На наступному етапі починається робота з адміністраторами (якщо такі є), користувачами і/чи бізнес-менеджерами об'єктів і систем. У рамках заданих фахівцем з безпеки характеристик вони роблять уточнення і доповнення описів об'єктів для того, щоб описати де-факто сформовані процедури і способи роботи із системою для виявлення надалі можливих уразливостей і загроз.

Проведення такого роду обстеження звичайно здійснюється за такою схемою:

1. Загальне знайомство із системою, візуальний огляд фізичного розміщення окремих компонентів чи складових.
2. Попередня бесіда з адміністратором/менеджером про загальний напрямок функціонування системи.
3. Ознайомлення з документацією про інформаційну систему.
4. Складання опису системи з погляду інформаційної безпеки.
5. Уточнення опису на основі роботи з документацією та із запрошеними фахівцями.

Для якісної подальшої роботи дані характеристики слід добре структурувати, наприклад, за такими параметрами:

- апаратне забезпечення інформаційної системи (комп'ютери, модеми, маршрутизатори, мости, повторювачі, принтери та інші периферійні пристрої);
- мережне забезпечення (мережні кабелі, розетки, конектори тощо);
- системне програмне забезпечення (операційна система, інші засоби створення середовища роботи, наприклад, програми резервного копіювання чи СКБД);

- прикладне програмне забезпечення, тобто програми, що виконують, власне, функції виробничі, допоміжні і супутні виробництву;
- організаційне забезпечення, тобто користувачі чи суб'єкти системи і їхні функціональні обов'язки у системі;
- нормативне забезпечення – правила й інструкції роботи із системою, можливо, окремі витяги з них;
- дані – інформація, що використовується у роботі системи в її виробничому значенні.

Залежно від конкретної організації, опис може бути доповнено іншими розділами. Наприклад, можна включати функціональне призначення окремих об'єктів системи.

Крім того, необхідно визначитися з тим, що вважати окремим об'єктом системи, який підлягає захисту? Можна, наприклад, вважати всю систему єдиним об'єктом, а можна кожну ланку розглядати окремо.

6.3.2. Принципи і напрямки проведення інвентаризації

Перед початком інвентаризації необхідно розробити, погодити і затвердити порядок і методику проведення обстеження. Цей документ (чи документи) повинен містити цілі та принципи проведення даного заходу для того, щоб вони були прозорі для тих, хто буде цим займатися. Можливо, необхідно затвердити в керівника підприємства повноваження служби чи фахівця, що будуть проводити інвентаризацію, а також перелік учасників –запрошених фахівців для надання процесу необхідного статусу значимості.

У методичній частині документа повинно бути описано що потрібно зробити запрошеним фахівцям, щоб виконати свою роботу. Доцільно укомплектувати документ додатком у вигляді анкети, структурованої таким чином, щоб максимально полегшити її заповнення – вибір із уже наявних варіантів, числові оцінки тощо.

Проводячи інвентаризацію, доцільно дотримуватися таких принципів:

Принцип однакового підходу має на меті розгляд будь-якого об'єкта/системи з погляду технології створення, оброблення, зберігання, відправлення чи приймання інформації.

Принцип об'єктивності означає підхід з позицій оцінки інформаційної безпеки при критичному аналізі системи/об'єкта.

Принцип багаторівневого підходу означає розгляд об'єкта/системи шляхом поділу його на складові частини (апаратне забезпечення, програмне забезпечення тощо).

Принцип сполучення означає, що необхідно вказати, із яких систем інформація надходить у дану систему і в які системи інформація передається із неї.

Напрямки проведення інвентаризації такі:

Фізичний – описує географічне розташування і розміщення системи чи окремих компонентів з урахуванням опису підсистем розмежування доступу.

Технологічний – описує використовувані технічні засоби (апаратне і програмне забезпечення, алгоритми, схеми тощо).

Функціональний – описує місце системи у виробничому процесі і виконувані задачі.

Організаційний – описує персонал, задіяний у роботі системи, і його обов'язки.

Нормативний – описує наявні документи, що регламентують роботу системи.

Інформаційний – описує виробничий чи бізнес-характер інформації (даних), з якою працює система.

6.3.3. Інформація, що збирається

Поряд із проведенням загальної інвентаризації, що має на меті визначення об'єктів захисту, з подібного обстеження можна отримати й інші дані, які є для самої інвентаризації допоміжними, але можуть мати самостійну цінність. Це, наприклад, перелік програмного забезпечення (системного і прикладного), використовуваного на підприємстві. Маючи подібний перелік, за умови підтримки його актуальним, можна відслідковувати автоматизованими чи іншими способами появу в інформаційному просторі підприємства стороннього програмного забезпечення, установленого без санкції уповноважених служб (наприклад, комп'ютерні ігри).

Можна просто скласти перелік програмного забезпечення з переліком ключових характеристик (виробник, номер версії, дата установки, призначення, якщо є можливість – контрольна сума файлів), але краще відразу зробити його класифікацію, наприклад, за такими параметрами:

- категорія застосування (загальне, спеціалізоване, індивідуальне);
- функціональне призначення (виробнича чи іншого роду задача, для якої використовується дане програмне забезпечення);
- належність користувачу (хто керує використанням даного програмного забезпечення, тобто його адміністратор);
- розміщення компонентів програмного забезпечення (робочі станції, сервери);
- способи доступу (локальний, віддалений).

Додатково в порядку інвентаризації варто передбачити форми документів, що будуть використані, а саме:

- опитувальні аркуші чи анкети – джерело одержання даних для аналізу;
- проміжні документи – засоби оброблення даних;
- звіти – результат проведеного обстеження.

Працюючи за напрямками інвентаризації інформаційної систем необхідно зафіксувати ряд деталей, що можуть показатися і зайвими на даному етапі, але надалі будуть дуже корисними.

Фізичне розташування:

- будинок, приміщення;
- номера телефонів приміщень;
- механізми контролю доступу в приміщення й інші захисні механізми;
- номери чи адреси мережних вузлів;
- відповідальний за приміщення, якщо такий існує.

Апаратне забезпечення:

- фізичне розташування в приміщенні;
- найменування фірми-виробника;
- серійний номер;
- функціональне призначення в системі;
- вмонтовані механізми захисту;
- адреси портів та інші мережні адреси (MAC, IP тощо);
- відповідальний за дану одиницю устаткування, якщо є.

Програмне забезпечення (крім уже зазначених параметрів):

- виробник;
- номер версії;
- вмонтовані механізми захисту;
- статистика збоїв, якщо є.

Функціональне призначення (даний розділ дуже залежить від особливостей виробництва, але такі пункти повинні бути наявними):

- які підрозділи є споживачами даної системи;
- хто займається технічною підтримкою системи;
- роль системи в загальному виробничому циклі.

Організаційне забезпечення:

- функціональні і/чи посадові обов’язки персоналу;
- професійний рівень підготовки персоналу (освіта, додаткове навчання);
- існуючі процедури щодо забезпечення безпеки;
- часовий графік виконання робіт у системі;
- логічні схеми руху інформації між користувачами.

Нормативне забезпечення:

- перелік наявних документів – правил, інструкцій тощо;
- окремо – документи з безпеки;
- дати останнього внесення змін у документи;

- сертифікати на апаратне і/чи програмне забезпечення.

Дані (цей розділ також дуже залежить від особливостей виробництва, але такі пункти обов'язкові незалежно від його специфіки):

- звідки надходять дані у систему;
- куди надходять дані із системи;
- яка робота з даними відбувається в системі;
- формат зберігання даних у системі;
- вид даних – первинні таблиці даних, трансакції, звіти тощо;
- логічні схеми руху інформації між об'єктами.

Усі зібрані дані, крім того що служать основою для моделі керування ризиками, ще і допоможуть у подальшій роботі, наприклад, при попередній підготовці відомостей розслідування у випадках порушення інформаційної безпеки.

6.4. Принципи організації управління і контролю систем захисту

Налагодження засобів захисту, управління системою захисту і здійснення контролю функціонування інформаційних систем – все це складові однієї задачі – реалізації політики безпеки організації.

Налагодження засобів захисту інформації необхідне для приведення їх у відповідність з розробленим планом. При налагодженні доданих засобів захисту необхідно особливу увагу приділити питанням перевірки їх сумісності з застосовуваними прикладними програмами.

Управління системою захисту полягає у періодичному внесенні змін у базу даних захисту, яка містить відомості про користувачів, допущених до роботи у системі, їх правах доступу до різних об'єктів системи тощо.

Основну увагу при управлінні системою слід звернути на:

- документованість всіх змін у базі даних захисту. Найкраще було б організувати систему заявок від посадових осіб організації на дозвіл доступу тому чи іншому співробітнику організації до якого-небудь ресурсу системи. При цьому відповідальність за допуск співробітника покладається на відповідну особу, яка підписала заявку;
- періодичне резервне копіювання бази даних, щоб уникнути втрати їх актуальної копії при збої (відмові) обладнання.

Контроль за функціонуванням інформаційної системи полягає у стеженні за небезпечними подіями, аналізі причин, які призвели до їх виникнення, і ліквідації наслідків.

Як правило, задачі управління і контролю вирішуються адміністративною групою, особовий і кількісний склад якої залежить від конкретних умов. Звичайно до складу цієї групи входять: адміністратор безпеки, менеджер безпеки і оператор.

Забезпечення і контроль безпеки – це комбінація технічних і адміністративних засобів. За даними зарубіжних джерел у працівників

адміністративної групи звичайно третину часу займає технічна робота (управління програмами та іншими засобами контролю доступу, захист портів, криптозахист тощо) і біля двох третин – адміністративна (розроблення документів пов'язаних із захистом інформаційної системи, процедурами перевірки системи захисту тощо). Раціональне сполучення цих заходів допомагає підтримувати адекватний захист ІС і сприяє зменшенню можливості порушень політики безпеки.

6.5. Управління доступом до робочих місць в інформаційній системі

Користувачі повинні знати свої обов'язки щодо забезпечення контролю доступу; особливо – використання паролів. Доступ користувачу до ресурсів ІС повинен надаватися згідно з політикою управління доступом. Зокрема, рекомендується надавати користувачам тільки прямий доступ до серверів, використання яких їм дозволено. Особливу увагу адміністратора безпеки слід приділяти контролю мережевих підключень до конфіденційних чи критично важливих доповнень, а також контролю за роботою користувачів у зонах підвищеного ризику, наприклад, в загальнодоступних місцях чи місцях, що знаходяться за межами організації.

Доступ до робочих місць в ІС слід надавати тільки зареєстрованим користувачам.

Системи управління доступом повинні забезпечувати:

- ідентифікацію і автентифікацію користувачів, а також, за необхідності, термінала і місцезнаходження кожного зареєстрованого користувача;
- ведення журналу обліку спроб доступу (успішних і невдалих) до ІС;
- за необхідності обмежувати підключення користувачів у неурочний час.

Для організації доступу до ІС на етапі підготовчих робіт рекомендується розглянути такі питання:

- реєстрація користувачів;
- управління привілеями;
- управління паролями користувачів;
- перегляд прав доступу користувачів;
- використання паролів;
- обладнання користувачів, залишене без нагляду;
- відстежування часу простою терміналів;
- обмеження періоду підключення.

Для управління доступом до багатокористувацького сервісу повинна бути розроблена процедура реєстрації користувачів. Ця

процедура повинна:

- перевіряти, чи наданий користувачеві дозвіл на використання сервісу відповідальним за його використання;
- вести облік усіх зареєстрованих осіб, що використовують інформаційну систему;
- перевіряти чи достатній рівень доступу користувача до системи і чи не суперечить він політиці безпеки, прийнятої в організації, наприклад, чи не компрометує він принцип розподілення обов'язків;
- своєчасно анулювати права доступу у користувачів, які залишили організацію;
- періодично перевіряти і видаляти застарілі ідентифікатори та облікові записи.

У багатокористувацьких ІС повинна існувати система контролю надання привілеїв. При організації такої системи рекомендується:

- ідентифікувати привілеї, пов'язані з кожним програмним продуктом чи сервісом, підтримуваним системою, а також категорії працівників, яким їх необхідно надавати;
- надавати привілеї окремим особам тільки у випадку крайньої потреби і залежно від ситуації, тобто тільки коли привілеї потрібні для виконання працівниками своїх функцій;
- реалізувати автоматичний процес визначення повноважень і вести облік всіх наданих привілеїв;
- за можливістю використовувати системні програми, для яких немає необхідності надавати спеціальні привілеї користувачам;
- надавати інший ідентифікатор для звичайної роботи користувачам, які мають великі привілеї для спеціальних цілей.

Вимоги до системи контролю (управління) паролями користувачів такі:

- зобов'язати користувачів зберігати в секреті персональні паролі та паролі робочих груп;
- коли користувачі повинні самі вибирати свої паролі, видати їм надійні тимчасові паролі. Тимчасові паролі видаються також у випадку, коли користувачі забувають свої паролі;
- передавати тимчасові паролі користувачам надійним способом. Уникати передавання паролів через посередників чи за допомогою незахищених (незашифрованих) повідомлень електронної пошти. Користувач повинен підтвердити отримання паролю.

Перегляд прав доступу користувачів через регулярні проміжки часу проводиться з метою забезпечення ефективного контролю за дотриманням режиму захисту інформації. Процес перегляду повинен забезпечувати:

- перегляд повноважень доступу користувачів через регулярні проміжки часу (6 місяців);
- перегляд дозволу на надання спеціальних привілеїв через більш короткі проміжки часу (3 місяці).

Для підтримання режиму ЗІ при ***виборі та використанні паролів*** пропонуються такі рекомендації:

- вибирати паролі, що містять не менше шести символів;
- при цьому не слід використовувати:
  а) назви місяців року, днів тижня;
  б) прізвища, ініціали, реєстраційні номери автомобілів;
  в) назви та ідентифікатори організацій;
  г) номери телефонів чи групи символів, що ідуть один за одним;
  д) групи символів, що складаються тільки з цифр;
- змінювати паролі через регулярні проміжки часу (місяць) і уникати повторного чи „циклічного” використання старих паролів;
- частіше змінювати паролі для привілейованих системних ресурсів (до системних утилітів);
- змінювати тимчасові паролі при першому вході в систему;
- не включати паролі в процедуру автоматичного входу в систему (макроси, функціональні клавіші);
- не допускати використання одного паролю декількома користувачами;
- забезпечувати зберігання паролів у секреті;
- змінювати паролі, коли є вказівки на можливу компроментацію їх;
- використовувати один надійний пароль, якщо потрібен доступ до декількох серверів, захищених паролями.

Користувачі повинні знати процедури захисту обладнання, залишеного без нагляду, а також свої обов’язки щодо забезпечення такого захисту.

Рекомендується:

- завершувати сеанси зв’язку з закінченням роботи, якщо їх не можна захистити шляхом відповідного блокування;
- використовувати логічне відключення від серверів із закінченням сеансу зв’язку. Не обмежуватись виключенням ПК чи термінала;
- захищати невикористовувані ПК чи термінали шляхом блокування ключем чи іншими засобами контролю доступу.

Для недіючих терміналів у зонах з підвищеним ризиком порушення ЗІ (у загальнодоступних місцях чи за межами досяжності) необхідно встановити допустимий час простою для запобігання доступу незареєстрованих користувачів. З закінченням цього часу екран термінала повинен очищатись, а сеанси зв’язку з додатками і мережевими сервісами завершатися. Допустимий час простою повинен задаватись, виходячи з

аналізу ризику несанкціонованого доступу до термінала користувача.

Додатковий захист сервісів від НСД можна забезпечити шляхом ***обмеження допустимого періоду підключення***. Обмеження дозволеного періоду підключення термінала до ІС дозволяє зменшити ймовірність НСД до ресурсів ІС. Можливість застосування такого захисту контролю слід розглядати для ІС з терміналами, встановленими в зонах підвищеного ризику порушення ЗІ.

6.6. Управління доступом до сервісів

Користувачам і обслуговувальному персоналу ІС слід надавати доступ до сервісів згідно з прийнятою політикою управління доступом до інформації. ***Рекомендується розглянути можливість таких засобів контролю:***

- доступ до додатків (сервісів) через систему меню, що забезпечує контроль повноважень доступів користувачів;
- обмеження доступу користувачів до інформації про структурні дані та функції ІС, доступ до яких їм не дозволений, шляхом відповідного редагування документації користувачів;
- контроль за вихідною інформацією додатків на предмет вмісту в ній конфіденційної інформації. Така інформація повинна посилатись тільки на певні термінали і комп'ютери. Потрібен періодичний аналіз вихідної інформації та видалення, за необхідності, зайвої інформації.

В організації повинні бути визначені чіткі правила відносно статусу і використання електронної пошти. ***Для зменшення ризику порушень ЗІ, пов'язаного з застосуванням електронної пошти, рекомендується:***

- враховувати вразливість повідомлень у відношенні до несанкціонованого перехоплення і модифікації;
- враховувати ймовірність неправильної адресації чи направлення повідомлень не за призначенням, а також надійність і доступність сервісу в цілому.

При використанні систем електронного документообігу слід враховувати виконання вимог ЗІ:

- необхідність виключення деяких категорій конфіденційної інформації у випадку, якщо у даній системі не забезпечується належний рівень захисту;
- необхідність визначення правил і засобів контролю для адміністрування колективно використовуваної інформації (електронні дошки оголошень);
- використання засобів обмеження доступу до інформації, яка відноситься до різних робочих груп;
- визначення категорії персоналу і працівників сторонніх організацій, яким дозволено використовувати систему і ділянки, з

яких можна отримати доступ до систем електронного документообігу.

Для запобігання несанкціонованого доступу до інформації в ІС необхідно використовувати логічні засоби контролю доступу. Логічний доступ до додатків слід надавати тільки зареєстрованим користувачам.

Додатки повинні виконувати такі функції:

- контролювати доступ користувачів до даних і додатків згідно з політикою управління доступом, прийнятою в організації;
- забезпечувати захист від НСД до системних програм, здатних обійти засоби контролю і створити можливість НСД;
- не порушувати захист інших систем, з якими вони розділяють інформаційні ресурси.

В ІС можуть використовуватись системні програми, здатних обійти засоби контролю операційних систем і додатків. Необхідно обмежити і старанно контролювати використання таких системних утиліт.

Рекомендується використовувати такі заходи контролю (за можливості):

- захист системних утиліт за допомогою паролів;
- ізоляцію системних утиліт від прикладного програмного забезпечення;
- надання доступу до системних утиліт мінімальному числу користувачів;
- надання спеціального дозволу на використання системних утиліт;
- обмеження доступу системних утиліт, наприклад, часом внесення санкціонованої зміни;
- реєстрацію всіх випадків використання системних утиліт;
- визначення і документування рівнів повноважень доступу до системних утиліт;
- видалення всіх необхідних утиліт і системних програм.

Для зведення ризику пошкодження програмного забезпечення до мінімуму необхідно здійснювати жорсткий контроль за доступом до *бібліотек початкових текстів програм.*

Рекомендується дотримуватись таких правил:

- не зберігати бібліотеки початкових текстів програм у ІС;
- призначити відповідального за зберігання бібліотеки початкових текстів програм;
- зберігати роздруківки програм у бібліотеці початкових текстів;
- обмежити доступ до бібліотек початкових текстів програм;
- не зберігати розроблювані програми у бібліотеці початкових текстів робочих програм;
- оновлення бібліотеки початкових текстів програм і видача текстів програм програмістам повинні проводитись тільки призначеним відповідальним працівником після отримання дозволу на доступ до додатків у встановленій формі;

- фіксувати всі випадки доступу до бібліотек початкових текстів програм у контрольному журналі;
- застарілі версії початкових текстів програм слід архівувати з вказанням дати закінчення їх використання разом зі всім допоміжним програмним забезпеченням та інформацією про організацію виконання завдань для цієї версії програмного забезпечення;
- супроводження і копіювання бібліотек початкових текстів програм здійснювати згідно з процедурами управління процесом внесення змін.

За наявності *вразливих місць у захисті* ІС може бути потреба в організації виділеного (ізольованого) обчислювального середовища. Можливе застосування інших спеціальних заходів: запуск додатку на виділеному комп'ютері чи розподілення ресурсів тільки з надійними прикладними системами.

У загальному випадку ***рекомендується дотримуватися таких правил:***

- вразливі місця в ІС повинні бути явно визначені і задокументовані;
- при запуску вразливого додатку в колективно використовуваному середовищі необхідно вказати прикладні процеси, з якими він може працювати одночасно.

Всі надзвичайні ситуації і події, пов'язані з порушенням режиму ЗІ, необхідно реєструвати у журналі. Останній слід зберігати протягом заданого періоду часу. Крім невдалих спроб входу в систему доцільно також реєструвати випадки успішного доступу.

Контрольний журнал повинен включати:

- ідентифікатори користувачів;
- дату і час входу і виходу з системи;
- ідентифікатор чи місцезнаходження термінала (за можливості).

Необхідно встановити процедури ***відстежування за використанням сервісів*** ІС. Користувачам повинні бути доступні тільки явно дозволені сервіси. Рівень контролю слід визначити за допомогою оцінки ризиків.

Рекомендується слідкувати за такими подіями:

- невдалими спробами доступу до ІС;
- спробами несанкціонованого використання відновлених ідентифікаторів користувачів;
- використанням ресурсів з привілейованим доступом;
- окремими діями, потенційно небезпечними з точки зору порушення захисту інформації;
- використанням конфіденційних ресурсів.

Всі дії, пов'язані з відстежуванням і реєстрацією, повинні бути формально дозволені керівництвом.

6.7. Захист цілісності даних і програм від шкідливого програмного забезпечення

Існує, як відомо, ряд шкідливих методів, які дозволяють порушувати цілісність даних і програм: “комп’ютерні віруси”, “мережеві хробаки”, “троянські коні”, “логічні бомби” тощо. Адміністратори ІС і користувачі повинні бути завжди готові до можливості проникнення шкідливого програмного забезпечення ІС і оперативно вживати заходи щодо виявлення його впровадження і ліквідації наслідків його атак.

В основу захисту від вірусів повинні бути покладені знання розуміння правил безпеки, належні засоби управління доступом до систем, зокрема:

- організація повинна проводити політику щодо встановлення тільки ліцензійного програмного забезпечення;
- антивірусні програмні засоби повинні регулярно оновлюватися і використовуватися для профілактичних перевірок (бажано щоденних);
- необхідно проводити регулярну перевірку цілісності критично важливих програм і даних. Наявність лишніх файлів і слідів несанкціонованого внесення змін потрібно реєструвати в журналі та розслідувати;
- дискети “невідомого походження” слід перевіряти на наявність вірусів до їх використання;
- необхідно суворо дотримуватись встановлених процедур повідомлення про випадки ураження ІС комп’ютерними вірусами і вживати заходи щодо ліквідації наслідків їх проникнення;
- слід мати плани забезпечення безперебійної роботи організації у разі вірусного зараження, у тому числі плани резервного копіювання всіх необхідних даних і програм та їх відновлень. Ці плани особливо важливі для мережевих файлових серверів, які підтримують велику кількість робочих станцій.

6.8. Контроль за станом безпеки інформаційних систем

Для ефективного захисту інформації в ІС організації, як правило, створюється підрозділ безпеки, на спеціалістів якого покладається вирішення таких основних задач:

- організація і підтримання контрольованого доступу користувачів до ресурсів ІС на всіх етапах її життєвого циклу;
- слідкування за станом безпеки ІС і оперативне реагування на несанкціоновані дії користувачів у даній системі.

У зв’язку з застосуванням додаткових засобів захисту інформації ***адміністратору безпеки належить виконувати такі операції:***

- встановлювати засоби захисту інформації на комп’ютери організації (установка і впровадження ЗЗІ);

- настроювати засоби захисту інформації шляхом надання прав доступу користувачам як до ресурсів комп'ютерів, так і до ресурсів мережі (експлуатація ЗЗІ);
- контролювати стан захищеності ІС шляхом оперативного моніторингу і аналізу системних журналів (контроль за станом безпеки ІС).

Адміністратору безпеки необхідно контролювати стан безпеки ІС як оперативно, шляхом стеження за станом захищеності комп'ютерів ІС, так і неоперативно – шляхом аналізу вмісту журналів реєстрації подій системи захисту інформації (СЗІ).

Використання сервера управління доступом для оперативного контролю за станом робочих станцій і роботою користувачів дозволяє відмовитись від постійної присутності в мережі адміністратора безпеки. У цьому випадку сервер управління доступом автоматично реєструє несанкціоновані дії, що відбуваються у мережі, і завжди володіє оперативною інформацією про стан станцій.

Збільшення кількості робочих станцій і використання програмних засобів з великою кількістю різноманітних компонентів призводять до істотного збільшення об'ємів журналів реєстрації подій СЗІ. Обсяг відомостей, що зберігаються в журналах, може настільки збільшитись, що адміністратор уже фізично не зможе повністю проаналізувати їх вміст за необхідний час.

Для полегшення роботи адміністратора безпеки необхідно реалізувати:

- оперативний контроль за станом робочих станцій мережі та роботою користувачів і за реєстрацією подій несанкціонованого доступу в спеціальному журналі;
- вибірку визначення подій (за іменем користувача, датою, часом події, її категорії тощо) з системних журналів;
- зберігання системних журналів кожної робочої станції за системою „день/місяць/рік" з автоматичним обмеженням строку їх зберігання. З закінченням установленого строку журнали знищуються;
- спеціальні можливості з обмеження переліку подій, що реєструються СЗІ;
- семантичне стиснення даних у журналі реєстрації, яке дозволяє збільшувати реєстровані події без істотної втрати їх інформативності;
- автоматична підготовка звітних документів установленої форми про роботу станцій мережі та наявних порушень, що дозволяє істотно понизити рутинне навантаження на адміністратора безпеки.

6.9. Сканери безпеки інформаційної системи

Сканер – це інструмент ефективної політики безпеки мережі. Він автоматизує роботи спеціалістів служби захисту, допомагаючи їм швидко перевірити сотні вузлів, у тому числі й тих, що знаходяться на інших територіях.

Мережа складається з каналів зв'язку, вузлів, серверів, робочих станцій, прикладного і системного програмного забезпечення, баз даних тощо. Всі ці компоненти потребують оцінювання ефективності їх захисту. ***Засоби аналізу захищеності досліджують мережу і ведуть пошук „слабких" місць, таких як:***

- „люки" в програмах (back door) і програми типу „троянський кінь";
- слабкі паролі;
- схильність до проникнення з незахищених систем;
- неправильна настройка міжмережевих екранів, WEB-серверів і баз даних.

Технологія аналізу захищеності є дієвим методом реалізації політики мережевої безпеки перш ніж здійсниться спроба її порушення ззовні чи зсередини організації.

Сканери призначені для виявлення тільки відомих вразливостей, опис яких є у базі даних. У цьому вони подібні антивірусним системам, яким для ефективної роботи необхідно постійно оновлювати базу даних сигнатур. Функціонувати такі засоби можуть на мережевому рівні (network-based), рівні операційної системи (host-based) і рівні додатку (application-based). Найбільшого розповсюдження набули засоби аналізу захищеності мережевих сервісів і протоколів.

Крім виявлення вразливостей за допомогою засобів аналізу захищеності можна швидко визначати всі вузли корпоративної мережі, доступні у момент проведення тестування, виявити всі використовувані у ній сервіси і протоколи, їх настройки і можливості для несанкціонованої дії. Також ці засоби розробляють рекомендації та заходи, які дозволяють ліквідувати виявлені недоліки.

Існує два основних механізми, за допомогою яких сканер перевіряє наявність вразливості – сканування (scan) і зондування (proba).

Сканування – механізм пасивного аналізу, коли сканер пробує визначити наявність вразливості за побічними ознаками – без фактичного підтвердження її наявності. Цей метод найбільш швидкий і простий для реалізації. У термінах компанії ISS даний метод отримав назву „логічний висновок" (inference). За твердженням компанії Cisco, цей процес ідентифікує відкриті порти, знайдені на кожному мережевому пристрої, і збирає пов'язані з портами заголовки (banner), знайдені при скануванні кожного порту. Кожний отриманий заголовок порівнюється з таблицею правил визначення мережевих пристроїв, операційних систем і потенційних вразливостей. На основі проведеного порівняння робиться

висновок про наявність чи відсутність вразливості.

Зондування – механізм активного аналізу, який дозволяє пересвідчитися у наявності на аналізованому вузлі вразливості. Зондування виконується шляхом імітації атаки, яка використовує перевірювану вразливість. Цей метод більш повільний, ніж сканування, проте майже завжди точніший. У термінах компанії ISS даний метод отримав назву „підтвердження" (verification). За твердженням компанії Cisco, цей процес використовує інформацію, отриману в процесі сканування (логічного висновку) для детального аналізу кожного мережевого пристрою. У цьому процесі також використовуються відомі методи реалізації атак для того, щоб повністю підтвердити передбачувані вразливості та виявити інші вразливості, які не можуть бути виявлені пасивними методами, наприклад схильність до атак типу „відказ в обслуговуванні" ("denial of service").

Практично будь-який сканер проводить аналіз захищеності у п'ять етапів.

1. Збирання інформації про мережу. На даному етапі всі активні пристрої ідентифікуються у мережі і визначаються запущені на них сервіси і домени. У випадку використання систем аналізу захищеності на рівні операційної системи даний етап пропускається, оскільки на кожному вузлі, що аналізується встановлені відповідні агенти системного сканера.

2. Виявлення потенційних вразливостей. Сканер використовує описану базу даних для порівняння зібраних даних з відомими вразливостями за допомогою перевірки заголовків чи активних зондувальних перевірок. У деяких системах всі вразливості ранжуються за ступенем ризику. Наприклад, у системах Netsonar вразливості поділяються на два класи: мережеві та локальні. Мережеві вразливості (наприклад, ті, що діють на маршрутизатори) вважаються більш серйозними порівняно з вразливостями, характерними тільки для робочих станцій. Аналогічно і в Internet Scanner всі вразливості поділяються на три ступені ризику: високий (high), середній (Medium), низький (Low).

3. Підтвердження виявлених вразливостей. Сканер використовує спеціальні методи і моделює (імітує) визначені атаки для підтвердження факту наявності вразливостей на вибраних вузлах мережі.

4. Генерування звітів. На основі зібраної інформації система аналізу захищеності створює звіти, які описують виявлені вразливості. У деяких системах (наприклад, Internet Scanner і Netsonar) звіти створюються для різних категорій користувачів, починаючи з адміністраторів мережі і закінчуючи керівництвом компанії. Якщо перших більше цікавлять технічні деталі, то для керівництва компанії треба надати гарно оформлені з застосуванням графіків і діаграм звіти з мінімумом подробиць. Немаловажним аспектом є наявність рекомендацій для ліквідації виявлених проблем. І тут лідером є система Internet Scanner, яка для кожної

вразливості вміщує покрокові інструкції з ліквідації вразливостей, специфічні для кожної операційної системи. Часто звіти також містять посилання на FTP- чи Web-сервери, що мають patch і hotfix, які ліквідують виявлені вразливості.

5. Автоматична ліквідація вразливостей. Цей етап зрідка реалізується у мережевих сканерах, але широко застосовується у системних (наприклад, System Scanner). При цьому дана можливість може реалізуватись по-різному. Наприклад, у System Scanner створюється спеціальний сценарій (fix script), який адміністратор може запустити для ліквідації вразливості. Одночасно зі створенням цього сценарію, створюється і інший, який анулює зміни. Це необхідно, коли після ліквідації проблеми нормальне функціонування вузла було порушено. У інших системах можливості „відкату" не існує.

У будь-якому випадку в адміністратора, що здійснює пошук вразливостей, є декілька варіантів використання системи аналізу захищеності:

- запуск сканування тільки з перевірками на потенційні вразливості (етапи 1, 2 і 4). Це дає попереднє ознайомлення з системами у мережі. Даний метод менш руйнівний, порівняно з іншими, і самий швидкий;
- запуск сканування з перевірками на потенційні та підтверджені вразливості. Цей метод може викликати порушення роботи вузлів мережі під час реалізації перевірок типу „exploit chek";
- запуск сканування за правилами для користувачів щодо пошуку конкретної проблеми.

Таким чином, для організації захисту інформації чи проведення аудиту (оцінки стану ІС на відповідність стандарту чи вимогам) існуючої автоматизованої системи потрібен штат висококваліфікованих спеціалістів в області інформаційної безпеки. Це може бути надто дорого і невигідно для організації, особливо невеликої. Для проведення досліджень і аудиту доцільно залучати сторонні консалтингові компанії, які мають великий досвід і штат професіоналів в області забезпечення і контролю стану інформаційної безпеки.

Контрольні питання

1. Охарактеризуйте основні напрямки захисту інформації в ІС.
2. Охарактеризуйте основні принципи політики безпеки.
3. Опишіть особливості видів політики безпеки.
4. Поясніть суть організаційно-режимних заходів захисту.
5. Охарактеризуйте основні групи організаційних заходів.
6. Охарактеризуйте особливості політики інформаційної безпеки організації при підключенні до Internet.
7. Опишіть загальний підхід до інвентаризації інформаційних

систем.

8. Охарактеризуйте принципи і напрямки проведення інвентаризації інформаційних систем.
9. Опишіть порядок контролю за роботою користувачів.
10. Розкажіть про можливості системи управління доступом до робочих місць в ІС.
11. Охарактеризуйте суть системи контролю надання привілеїв щодо доступу до інформації.
12. Поясніть суть вимог до системи управління паролями користувачів.
13. Охарактеризуйте засоби контролю доступу користувачів до сервісів.
14. Поясніть суть вимог до систем електронного документообігу.
15. Опишіть функції логічних засобів контролю (додатків) доступу до інформації в ІС.
16. Охарактеризуйте заходи контролю за використанням системних утиліт.
17. Обґрунтуйте необхідність дотримання спеціальних правил при наявності вразливих місць у захисті ІС.
18. Опишіть засоби управління доступом до ІС для захисту їх від вірусів.
19. Розкажіть про основні функції адміністратора безпеки.
20. Розкажіть про призначення та особливості застосування сканерів.
21. Опишіть варіанти використання системи аналізу захищеності скануванням.

Додаток 1

Таблиця1

Організація секретного діловодства

Складові частини діловодства	Функції забезпечення безпеки інформації під час роботи з документами	Способи виконання
1	2	3
Документування	1. Запобігання необґрунтованого виконання документів 2. Запобігання включення у документи надмірних конфіденційних відомостей 3. Запобігання необґрунтованого підвищення ступеня секретності документів 4. Запобігання необґрунтованого розсилання	1. Визначення переліку документів 2. Здійснення контролю за змістом документів і ступенем секретності їх змісту Визначення реального ступеню секретності відомостей, включених у документ 4. Здійснення контролю за розмножуванням і розсиланням документів
Облік документів	1. Запобігання втрати (викрадення) документів	1. Забезпечення реєстрації кожного документа і зручності його пошуку 2. Здійснення контролю за місцезнаходженням документа
Організація документообігу	1. Запобігання необґрунтованого ознайомлення з документами 2. Запобігання неконтрольованого передавання документів	1. Установлення системи дозволів доступу виконавців до документа 2. Установлення порядку прийому-передачі документів між співробітниками 3. Здійснення контролю за порядком роботи з документами

Продовження табл.1

1	2	3
Зберігання документів	1. Забезпечення цілісності документів	1. Виділення спеціального обладнання приміщень для зберігання документів, що виключають доступ сторонніх осіб 2. Установлення порядку допуску до справ 3. Здійснення контролю за вчасним і правильним формуванням справ
Знищення документів	1. Вилучення з документообігу документів, що втратили свою цінність	1. Установлення порядку підготовки документів на знищення 2. Забезпечення необхідних умов знищення 3. Здійснення контролю за правильним і вчасним знищенням документів
Перевірка наявності документів	1. Контроль наявності документів, виконання вимог їх опрацювання, обліку, виконання і здавання	1. Установлення порядку проведення перевірок наявності документів і порядку їх обробки

Додаток 2

Форма №1

Журнал обліку документів і видань з грифом “Комерційна таємниця”

Порядковий реєстраційний номер	Дата надходження і індекс документа		Звідки надійшов чи куди відправлений	Найменування документа і короткий зміст	Кількість листів		Кількість і номери примірників
					документа	додатка	
1	2		3	4	5	6	7

(продовження форми №1)

Резолюція чи кому направлений на виконання	Відмітка про взяття на контроль і термін виконання	Дата і розписка		Індекс (номер) справи, куди підшитий документ	Відмітка про знищення	Примітки
		про отримання	про повернення			
8	9	10	11	12	13	14

Форма №2

Карточка обліку вхідних (вихідних) документів та видань з грифом “КТ”

Реєстраційний номер і гриф	Дата реєстрації	Номер і дата надходження документа	Кількість листів	
			головного документа	додатка

Найменування відправника:

Короткий зміст:

Підшивка			Реєстрація додатка		
номер справи	номери листів	підписи про звірення, дата	вид	інв.№	підписи про звірення, дата

Відмітка про звірення наявності
Картка перевірена, всі
позиції закриті

_____
(підпис)

“____” _____20___р.

_____

(лицьова сторона)

Переміщення

Дата	Кількість основних додатків	Кому виданий чи куди відправле-ний	Розпис в отриманні чи № реєстра	Підписи про звірення, дата	Дата повернення	Розпис в отриманні чи відмітка про повернення

Для різних відміток:

(зворотна сторона)

Форма №3

Журнал обліку і розподілу видань з грифом “КГ”

Наймену-вання видання	Видано чи поступило			Розподіл			Повер-нення	Знищення
	звідки поступило і де віддру - ковано	вхід. № супровід-ного листа і дата	кількість і № примір-ників	куди і кому направлено (чи видано)	№ вихід. докум. (чи розписка в отриманні і дата)	кількість і № примір - ників	дата і № примір-ника	дата і № акта
1	2	3	4	5	6	7	8	9

Форма № 4

Карточка обліку справ і видань з грифом “КТ”, що видаються

Найменування справи чи видання				
№ справи, № примірників видань і кількість листів	Підрозділ і прізвище співробітника	**Розпис**		Примітки
		про отримання і дата	про повернення і дата	
1	2	3	4	5

Форма № 5

Журнал обліку службових видань з грифом “КТ”

Дата і № супровідного листа (накладної)	Звідки надійшло, назва і рік видання	Кількість примір-ників	№ примір-ників	Кому відправлено, дата і вихід. №	Кількість примір-ників	№ примір-ників	Відмітка про переоблік чи знищення
1	2	3	4	5	6	7	8

Додаток 3

Договірне зобов’язання

Я,_____

(прізвище, ім’я, по батькові)

оформляючись на роботу _____

(посада, підрозділ)

зобов’язуюсь:

а) у період роботи не розголошувати відомостей, що складають комерційну таємницю, які мені будуть довірені чи стануть відомі при виконанні службових обов’язків;

б) беззаперечно і акуратно виконувати вимоги наказів, інструкцій і положень щодо захисту комерційної таємниці, які відносяться до мене і з якими я ознайомлений (на);

в) не повідомляти усно чи у письмовій формі кому б то не було відомостей, що складають комерційну таємницю;

г) у разі звільнення не розголошувати і не використовувати для себе чи інших відомостей, що складають комерційну таємницю.

Я попереджений (на), що у разі порушення даного зобов’язання повинен (на) відшкодувати втрати чи буду притягнений (на) до дисциплінарної або кримінальної відповідальності згідно з діючим законодавством.

_____

(підпис)

Проінструктував

“ ” _____20___р.

Додаток 4

Комерційна таємниця
Екз.№

ДОГОВІР №
колективного підряду на комплексне режимне обслуговування підприємства

Справжній договір укладений між підприємством_____ в особі директора _____ і колективом служби безпеки_____ в особі заст. директора – начальника служби безпеки_____ про нижче наведене.

1. Служба безпеки бере на себе виконання нижче перелічених робіт для забезпечення безпеки і збереження комерційної таємниці підприємства:

1.1. Цілодобова охорона підприємства і контроль за дотриманням правил пожежної безпеки.

1.2. Виписування перепусток для співробітників підприємства.

1.3. Прийом осіб, що перебувають у відрядженні, виписування перепусток для них.

1.4. Виписування приписів для виконання завдань особам, що перебувають у відрядженні, і видача довідок про допуск.

1.5. Розробка номенклатури посад, які підлягають узгодженню із контрольними органами, і оформлення допусків.

1.6. Підготовка за поданням директора списку відомостей, що складають комерційну таємницю, наказів, інструкцій про збереження комерційної таємниці підприємства.

1.7. Надання послуг з передачі кореспонденції телетайпом, телексом, телефаксом та іншими системами зв'язку.

1.8. Прийом, облік та розсилання відкритої кореспонденції.

2. Директор підприємства зобов'язується:

2.1. За роботи, перелічені у дійсному договорі, здійснювати оплату із своїх фондів за відомістю на працівників служби безпеки у розмірі_____гривень щомісячно.

2.2. Приймати роботи за актом, затвердженим директором_____і заст. директора – начальником служби безпеки_____.

2.3. Зобов'язати співробітників пілприємства виконувати всі режимні вимоги, передбачені інструкцією щодо забезпечення збереження комерційної таємниці.

2.4. При визначенні грифу документів керуватися обмежувальними переліками відомостей, обов'язковими для виконавців.

2.5. Негайно представляти у службу безпеки відомості про вступ у зв'язок з інофірмами.

3. Дійсний договір укладається на календарний рік з 01.01.200 р. до 31.12.200 р., друкується у двох примірниках, кожний примірник зберігається у директора____ і у службі безпеки.

Директор підприємства

_____

" "_____200__р.

Заст. директора –
начальник служби
безпеки

_____

" "_____200__р.

АКТ
про виконання робіт за договором №

" "_____200__р.

Комісія у складі представника підприємства_____ в особі його директора _____ і представника колективу безпеки в особі заст. директора – начальника служби безпеки_____ провели роботу щодо встановлення фактичного виконання колективом служби безпеки договору №_____ колективного підряду на комплексне режимне обслуговування_____ за 200___р.

У результаті перевірки комісія встановила, що всі роботи за договором у _____200____р. виконані якісно, у повному об'ємі і у встановлені терміни.

До акту додається відомість на виплату.

Директор підприємства

_____

" "_____200__р.

Заст. директора –
начальника служби
безпеки

_____

" "_____200__р

Додаток 5
Таблиця 1

Заходи, що спрямовані на запобігання розголошенню конфіденційної інформації

Способи розголошення	Особливості	Організаційні заходи	Організаційно-технічні заходи
1	2	3	4
		Загально-організаційні заходи:	
		1. Перелік відомостей, що становлять комерційну таємницю	
		2.Зобов'язання співробітників про нерозголошення комерційних секретів	
		3. Моніторинг за лояльністю співробітників 4. Міри відповідальності за розголошення конфіденційної інформації	
		5. Охорона будинків, приміщень і місць зберігання документів	1. Використання технічних засобів контролю приміщень, сховищ документів
Відкрите залишення конфіденційних документів	1. На робочому столі	1. Розташування робочого місця, що виключає або обмежує можливість спостереження за документами	1. Використання штор, фіранок, драпувань
	2. На екрані ПЕОМ і в засобах колективного користування		1. Використання програмних засобів гасіння інформації з регламенту

Продовження табл.1

1	2	3	4
	3. У квартирі	1. Заборона на роботу з конфіденційною інформацією вдома	
	4. В автомашині	1. Суворий контроль за перевезенням документів	
Передавання конфіденційної інформації	1. Каналами електрозв'язку	1. Використання заходів приховання змісту	1. Використання технічних засобів захисту інформації
		2. Скорочення часу передавання інформації	2. Використання маскіраторів, скремблерів, засобів шифрування й електронного підпису в системах зв'язку і телекомунікацій
		3. Використання методів прихованого ведення сеансів зв'язку	
	2. При розробленні й опрацюванні документів	1. Розроблення документів у спеціальних зошитах і блокнотах	1. Розроблення документів на ПЕОМ із дотриманням вимог захисту конфіденційної інформації
Повідомлення, оголошення	1. На ділових зустрічах (переговорах)	1. Чітка регламентація тематики переговорів 2. Проведення переговорів у спеціальних приміщеннях 3. Обмеження на запис інформації учасниками переговорів (спец.блокноти)	1. Запис (аудіо або аудіо/відео) переговорів з метою наступного аналізу їхньої конфіденційності

Продовження табл.1

1	2	3	4
	2. При діловому листуванні	1. Контроль змісту листів	1. Шифрування тексту документів 2. Застосування пристроїв таємного фіксування незаконного доступу до документів
	3. На семінарах, симпозіумах, у пресі та інших засобах масової інформації	1. Дотримання вимог конфіденційності	
	4. На виставках, у рекламі	1. Ретельний аналіз і відбір інформаційних матеріалів і демонстраційних виробів	
		2. Суворий інструктаж співробітників з метою дотримання режиму конфіденційності	
Пересилання	1. Каналами поштового зв'язку	1. Шифрування документів 2. Застосування спеціальних конвертів, що виключають проникнення до документів 3. Опечатування конвертів і упакувань 4. Пересилання спецзв'язком або кур'єрами 5. Попереднє оповіщення адресата про	1. Використання технічних засобів шифрування документів

Продовження табл.1

1	2	3	4
		відправлення документів 6. Повідомлення адресата про відповідальність за розголошення конфіденційних відомостей	
		7. Посланцем (знайомий, попутник)	
Опублікування	1. У дисертаційних дослідженнях, пресі та інших ЗМІ	1. Попередній контроль опублікованих матеріалів	
		2. Перелік відомостей, дозволених до опублікування у відкритій пресі	
Особисте спілкування	1. На зустрічах	1. Дотримання вимог про нерозголошення конфіденційної інформації	
	2. При телефонних переговорах	1. Заборона ведення приватних переговорів з використанням службових телефонів	1. Запис переговорів зі службових телефонів на магнітофон
			2. Використання апаратури закриття телефонних переговорів
Втрата документів	1. На роботі	1. Суворий облік і контроль за розробленням, використанням і зберіганням документів конфіденційного характеру 2. Службове розслідування	

Продовження табл.1

1	2	3	4
	2. За межами роботи	1. Заборона на винесення службових документів за межі організації без належних заходів захисту 2. Службове розслідування	
Безконтрольне розроблення документів	1. Необґрунтоване виготовлення документів	1. Регламентація складу конфіденційних документів	
	2. Включення у звичайні документи відомостей конфіденційного характеру	1. Контроль за змістом документів	
		2. Контроль за ступенем таємності документів	
Безконтрольний документообіг	1. Необґрунтоване розсилання документів	1. Контроль розмноження й розсилання документів	
	2. Необґрунтоване ознайомлення з конфіденційними документами співробітників	1. Контроль ознайомлення співробітників з конфіденційними документами з урахуванням системи розмежування допуску	

Продовження табл.1

1	2	3	4
		2. Контроль передачі документів виконавцям	
		3. Контроль за порядком роботи з конфіденційними документами	
Безконтрольне зберігання та знищення документів		1. Забезпечення збереження документів	
		2. Своєчасне знищення документів	1. Використання технічних засобів механічного знищення документів
Безконтрольний прийом вхідної кореспонденції	1. Суворий облік вхідних документів		
	2. Своєчасне доведення документів, що надійшли, до керівництва та виконавців		

Додаток 6
Таблиця 1

Заходи щодо захисту інформації від витоку технічними каналами

Способи (канали)	Особливості	Організаційні	Організаційно-технічні
1	2	3	4
Візуально-оптичні	1. При звичайному освітленні й у складних умовах (сутінки, ніч)	1. Розширення зони безпеки 2. Контроль можливості встановлення спостереження 3. Використання особливостей місцевості	1. Використання захисних засобів (штори, захисні плівки, спеціальне скло) 2.Використання засобів маскування
Акустичні	1. Пряме поширення звуку в закритих об'ємах	1. Ведення конфіденційних переговорів у спеціальних захищених приміщеннях	1. Устаткування приміщень засобами захисту переговорів від витоку інформації акустичними каналами
	2. Пряме поширення звуку на відкритому просторі	1. Обмеження ведення конфіденційних переговорів на відкритому просторі	
		2. Використання місцевих предметів і умов при веденні конфіденційних переговорів	
	3. Поширення звуку у твердих середовищах (структурний звук)	1. Виявлення можливості утворення каналів витоку інформації у твердих середовищах (стіни, повітроводи, комунікації)	1. Будівельно-конструкційні заходи, що виключають можливість утворення акустичних каналів

Продовження табл.1

1	2	3	4
Електромагнітні	1. За рахунок мікрофонного ефекту в технічних засобах	1. Вживання заходів, що виключають можливість утворення каналу витоку інформації за рахунок мікрофонного ефекту 2. Забезпечення контрольованої зони безпеки	1. Установка апаратних засобів захисту від витоку інформації за рахунок мікрофонного ефекту
	2. За рахунок магнітної складової електромагнітного поля	1. Забезпечення контрольованої зони безпеки	1. Екранування апаратур і приміщень 2.Заземлення апаратур
	3. За рахунок паразитної генерації підсилювачів	1. Контроль наявності паразитної генерації підсилювачів різного призначення у виділених приміщеннях	1. Екранування і заземлення технічних засобів і приміщень
	4. Коло живлення електронних систем	1. Використання мереж живлення, що не мають виходу за межі контрольованої зони	1. Розбирання електричних кіл
	5. Коло заземлення	1. Обов'язкове використання самостійних контурів заземлення для виділених приміщень	1. Регулярне вимірювання опору заземлення на відповідність нормативним вимогам

Продовження табл.1

1	2	3	4
	6. За рахунок взаємного впливу проводів і ліній зв'язку	1. Виключити паралельний пробіг телефонних проводів і ліній зв'язку, якими ведеться передача конфіденціальної інформації	Використання екранованих кабелів. Використання різних прийомів прокладки проводів, що послаблюють взаємний вплив
	7. За рахунок високочастотного нав'язування	1. Дослідження можливостей утворення каналів витоку інформації за рахунок УЧ - нав'язування	
	8. Волоконно-оптичними каналами зв'язку	1. Контроль можливого утворення каналів витоку волоконно-оптичними каналами	1. Суворе виконання вимог щодо дотримання заходів захисту від витоку інформації
Матеріально-речовинні	1. Безконтрольний вихід відходів виробництва за межі території підприємства	1. Суворий контроль і обмеження (виключення) виходу відходів виробництва за межі території підприємства	1. Виключення відходів як вторинної сировини 2. Утилізація відходів
	2. Безконтрольний вихід відходів інформаційних технологій за межі території підприємства	1. Організація знищення інформації на технічних носіях	

Додаток 7
Таблиця 1

Заходи щодо припинення несанкціонованого доступу до джерел конфіденційної інформації

Способи розголошення	Особливості	Організаційні	Організаційно-технічні
1	2	3	4
Ініціативне співробітництво	1. Умови, що провокують ініціативне співробітництво	1. Виключення умов, що сприяють ініціативному співробітництву 2. Аналіз і контроль соціальних умов у трудових колективах 3. Вивчення співробітників, потенційно здатних до ініціативного співробітництва	1. Використання технічних засобів контролю соціально-морального клімату
Схилення до співробітництва	1. Шантаж, залякування, підкуп	1. Вивчення співробітників, що складають інтерес для конкурентів і злочинних груп	
Випитування, вивідування	1. Провокування до розмов співробітників на службові теми на роботі, у громадських місцях, на відпочинку тощо	1. Навчання й виховання кадрів у напрямку суворого дотримання вимог щодо захисту комерційних секретів	1. Використання портативних магнітофонів для контролю записів і наступного аналізу щодо виявлення зловмисних дій
	2. Вивідування при веденні телефонних розмов		1. Використання спеціальних магнітофонів для запису й аналізу зловмисних дій

Продовження табл.1

1	2	3	4
Підслухо-вування	1. Підслуховування конфіденційних розмов керівництва й співробітників у приміщеннях	1. Ведення конфіденційних розмов у спеціальних приміщеннях	1. Устаткування приміщень шумопоглинальними засобами 2. Постановка акустичних перешкод
	2. Підслуховування конфіденційних переговорів в автотранспорті	1. Заборона ведення конфіденційних переговорів в автотранспорті	1. Використання засобів постановки акустичних перешкод
	3. Підслуховування конфіденційних розмов на відкритій місцевості	1. Інформування співробітників про можливості використання зловмисниками спрямованих мікрофонів 2.Ведення переговорів з використанням маскувальних властивостей місцевості	
Візуальне спостереження	Використання зловмисником візуальних засобів спостереження за станом і діяльністю підприємства (організації)	1. Використання штор, завісок, драпувань	1. Використання спеціального скла
	2. Використання зловмисником оптичних засобів спостереження		
Розкрадання	1. Первинних документів	1. Суворий облік і контроль розробки, руху й знищення документів	

Продовження табл.1

1	2	3	4
	2. Носіїв конфіденційної інформації		1. Суворий облік і контроль руху технічних носіїв інформації організаційно-технічними заходами
	3. Проміжних документів 4. Вихідних документів		
	5. Виробничих відходів	1. Сувора регламентація правил збору й знищення відходів	1. Установка спеціальних ящиків для відходів виробництва
Копіювання	1. Копіювання документів	1. Регламентація й облік розробки, розмноження й розсилання конфіденційних документів	
		2. Копіювання даних і програм на ЕОМ	1. Сувора регламентація технологій обробки інформації
			2. Облік і реєстрація режимів роботи та видачі документів
Підробка (модифікація)	1. Підробка ділових документів	1. Суворий контроль виготовлення, обліку та розсилання документів	1. Використання спеціальних засобів підтвердження дійсності документів (спеціальне чорнило, фарби тощо.)
	2. Підробка фінансових документів 3. Підробка персональних документів	1. Використання спеціальних методів виготовлення персональних документів	

Продовження табл.1

1	2	3	4
Знищення (псування, руйнування)	1. Документів	1. Виключення несанкціонованого доступу до конфіденційних документів	1. Використання спеціальних сейфів для зберігання конфіденційних документів
	2. Продукції	1. Забезпечення заходів щодо охорони і захисту продукції в місцях її знаходження	
	3. Програмного забезпечення	1. Забезпечення заходів щодо розмежування доступу до програмного забезпечення	1. Використання програмно-апаратних методів захисту програм і масивів даних від неправомірного впливу
Незаконне підключення до ліній і систем зв'язку	1. Контактне	1. Використання прихованих комунікацій 2. Охорона місць можливого підключення	1. Контроль ліній і систем зв'язку на наявність підключень 2. Використання екранованих кабелів
	2. Безконтактне	1. Використання прихованих комунікацій 2. Охорона місць можливого підключення	1. Використання екранованих кабелів
Перехоплення	1. Перехоплення інформації, переданої системами радіозв'язку	1. Використання методів потайного ведення сеансів зв'язку 2. Заборона ведення переговорів конфіденційного характеру	1. Використання технічних засобів засекречування інформації

Продовження табл.1

1	2	3	4
	2. Перехоплення інформації за рахунок побічних електромагнітних випромінювань і наведень	1. Проведення заходів щодо виключення утворення побічних електромагнітних випромінювань	1. Використання способів ослаблення ПЕМВІН 2. Екранування приміщень
Негласне ознайомлення	1. З документами 2. З інформацією на екранах ПЕОМ	1. Організація роботи з документами, що виключає можливість ознайомлення з їхнім змістом	
Фотографування	1. Документів	1. Організація роботи з документами, що виключає можливість ознайомлення з їх змістом	
	2. Продукції		
Збір і аналітична обробка		1. Розробка системи заходів щодо приховання конфіденційної інформації	
		2. Чітко організована робота з дезінформування зловмисників	

Література

1. Закон України „Про інформацію” від 02.10.1992р. - №2657-XII.
2. Закон України „Про науково-технічну інформацію” від 25.06.1993р. - №3322-XII.
3. Закон України „Про державну таємницю” від 21.01.1994р. - №3855XII.
4. Закон України „Про Концепцію Національної програми інформатзації” від 04.02.1998р. - №75/98-ВР.
5. Закон України „Про захист інформації в автоматизованих системах” від 05.07.1994р. - №80/94-ВР.
6. Закон України „Про стандартизацію” від 17.05.2001р. - №2408-III.
7. Закон України „Про ліцензування певних видів господарської діяльності” від 01.06.2000р. - №1775-III.
8. Ліцензійні умови провадження господарської діяльності, пов’язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації (затверджено наказом Державного комітету України з питань регуляторної політики та підприємництва від 29.12.2000р. - № 89/67).
9. Закон України „Про охорону прав на промислові зразки” від 15.12.1993р. - 3688-XII (із змінами і доповненнями станом на 01.01.2004р.).
10. Закон України „Про охорону прав на знаки для товарів і послуг” від 15.12.1993р. - №3689-XII (із змінами і доповненнями станом на 01.01.2004р.).
11. Закон України „Про електронні документи та електронний документообіг” від 22.05.2003р. - №851-IV.
12. Закон України „Про електронний підпис” від 22.05.2003р. - № 852-IV.
13. Постанова Кабінету Міністрів України „Про затвердження Концепції технічного захисту інформації в Україні” від 08.10.1997р. - №1126.
14. Концепція стратегії і тактики боротьби з комп’ютерною злочинністю в Україні (проект). - К.: 2001. - 61с.
15. Положення про Державний комітет України з питань державних секретів та технічного захисту інформації (затв. Указом Президента України від 05.11.1996р. - №1047/96).
16. Положення про технічний захист інформації в Україні (затв. Постановою КМУ від 09.09.1994р. - №632).
17. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні поняття, - К.: Держстандарт України, 1996. - 8 с.
18. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. - К.: Держстандарт України, 1996. - 11 с.

19. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Терміни та визначення. - К.: Держстандарт України, 1996. - 16 с.
20. Правила обов'язкової сертифікації засобів обчислювальної техніки (затв. наказом Держстандарту України від 25.06.1997р. - №366).
21. Правила обов'язкової сертифікації технічних засобів охоронної та охоронно-пожежної сигналізації (затв. наказом Держстандарту України від 10.04.1997р. - №191).
22. Бармен Скотт. Разработка правил информационной безопасности. Пер. с англ. - М.: „Вильямс", 2002. - 208 с.
23. Вертузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу. Навч. посібник /За ред. С.Г. Лаптева. - К.: Вид-во Європ. ун-ту, 2001. - 321 с.
24. Голубєв В.О., Гавловський В.Д., Цимбалюк В.С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. Навч. посібник /за заг. ред. доктора юридичних наук, професора Р.А. Калюжного. - Запоріжжя: ГУ „ЗІДМУ", 2002. - 292 с.
25. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. - К.: „ТЧД" „ДС", 2001. - 688 с.
26. Конеев И.Р., Беляев А.В. Информационная безопасность. - СПб.: БХВ-Петербург, 2003. - 752 с.
27. Медведев Н.Г., Москалюк Д.В. Аспекты информационной безопасности виртуальных частных сетей. Учебное пособие. - К.: Изд-во Европ. ун-та, 2002. - 95 с.
28. Ситник В.Ф. та ін. Основи інформаційних систем: Навчальний посібник. - К.: КНЕУ, 2001. - 420 с.
29. Ярочкин В.И. Информационная безопасность. Учебное пособие. - М.: Международ. отношения, 2000. - 400 с.

Навчальне видання

Володимир Андрійович Лужецький
Леонід Іванович Северин
Юрій Петрович Гульчак
Андрій Дмитрович Кожухівський

Основи організаційного захисту інформації

Навчальний посібник

Оригінал-макет підготовлено Севериним Л. І.

Редактор Т. О. Старічек

Навчально-методичний відділ ВНТУ
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м.Вінниця, Хмельницьке шосе, 95, ВНТУ

Підписано до друку
Формат 29,7 х 42 I/4
Друк різографічний
Тираж прим.
Зам. №

Гарнітура Times New Roman
Папір офсетний
Ум. друк. арк.

Віддруковано в комп'ютерному інформаційно-видавничому центрі
Вінницького національного технічного університету
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м.Вінниця, Хмельницьке шосе, 95