РУДИЙ Т.В.
ЖИВКО З.Б.
КУЛЕШНИК Я.Ф.
РУДА О.І.

ТЕХНОЛОГІЧНІ ЗАСОБИ БЕЗПЕКИ ЕКОНОМІЧНИХ СИСТЕМ

КУРС ЛЕКЦІЙ

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Львівський державний університету внутрішніх справ

Т.В. РУДИЙ, З.Б. ЖИВКО, Я.Ф. КУЛЕШНИК, О.І. РУДА

ТЕХНОЛОГІЧНІ ЗАСОБИ БЕЗПЕКИ ЕКОНОМІЧНИХ СИСТЕМ

Курс лекцій

Львів – 2017

ББК 32.973.2-018
Т38
УДК 004.056.5:658

Рекомендовано до друку Методичною радою
Львівського державного університету внутрішніх справ
Протокол № "8" від 21 березня 2017 р.

Р е ц е н з е н т и:
Я.І. СОКОЛОВСЬКИЙ, доктор технічних наук, професор, завідувач кафедри інформаційних технологій НЛТУ України;
Д.М. НЕСПЛЯК, кандидат фізико-математичних наук, доцент кафедри інформатики ЛьвДУВС.

Рудий Т.В.
Т38 Технологічні засоби безпеки економічних систем: курс лекцій. Вид. 2. Доп. і перероб. / Т.В. Рудий, З.Б. Живко, Я.Ф. Кулешник, О.І. Руда – Львів: Львівський державний університет внутрішніх справ, 2017. – 122 с.

У даному курсі лекцій висвітлено питання захисту державних інформаційних ресурсів у інформаційних системах, захисту інформації, яка становить комерційну таємницю, захисту інформації у електронних платіжних системах та алгоритми криптографічного захисту інформації. Детально розглянуті питання захисту потоків корпоративних даних у VPN-мережах.

Значну увагу приділено законодавчим аспектам у організації захисту інформації, які регламентують правила використання і оброблення інформації з обмеженим доступом та встановлюють ступінь відповідальності за порушення цих правил.

Рекомендовано для студентів економічних спеціальностей (напрямок підготовки 072 – ″Фінанси, банківська справа та страхування″), курсантів, практичних працівників слідчих підрозділів МВС.

УДК 004.056.5:658
ББК 32.973.2-018
© Т.В. Рудий, З.Б. Живко, Я.Ф. Кулешник, О.І. Руда. 2017
© Львівський державний університет внутрішніх справ, 2017

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС	– автоматизована система
БІ	– безпека інформації
ДСТСЗІ	– Департамент спеціальних телекомунікаційних систем та захисту інформації
ДТЗ	– допоміжні технічні засоби
ЕРС	– електрорушійна сила
ЗІ	– захист інформації
ЗМІ	– засоби масової інформації
ЗОТ	– засоби обчислювальної техніки
ЗТЗІ	– засоби технічного захисту інформації
ІБ	– інформаційна безпека
ІД	– інформаційна діяльність
ІзОД	– інформація з обмеженим доступом
ІО	– інформаційні об’єкти
ІС	– інформаційна система
ІТКС	– інформаційно-телекомунікаційна система
КВА	– контрольно-вимірювальна апаратура
КЗ	– контрольована зона
КРТ	– копіювально-розмножувальна техніка
КС	– комп’ютерна система
КСЗІ	– комплексна система захисту інформації
МЦБКЗ	– Міжвідомчий центр боротьби з комп’ютерною злочинністю
НД	– нормативний документ
НСД	– несанкціонований доступ
ОІД	– об’єкт інформаційної діяльності
ОТЗ	– основні технічні засоби
ПЕМВН	– побічні електромагнітні випромінювання і наведення
ПЗ	– програмне забезпечення
ПЗІ	– підрозділ захисту інформації
ПМА	– програма і методика атестування
РНБОУ	– Рада національної безпеки і оборони України
РСВ	– режимно-секретний відділ
СБУ	– служба безпеки України
СД	– службовий документ
СІ	– службова інформація
ССД	– служба службової документації
СУІБ	– система управління інформаційною безпекою
СУІБ	– система управління інцидентами інформаційної безпеки
ТД	– технічна документація
ТЗ	– технічне завдання
ТЗІ	– технічний захист інформації
ТКВІ	– технічні канали витоку інформації
ТУ	– технічні умови

CGI	–	Common Gateway Interface
DES	–	Data Encryption Standard
DNS	–	Domain Name System
ECC	–	Elliptic Curve Cryptography
EEPROM	–	Erectlically Erasable Programmable Read Only Memory
FTP	–	File Transfer Protocol
HTTP	–	HyperText Transfer Protocol
ISP	–	Internet Service Provider
MPLS	–	Multi Protocol Label Switching
NFS	–	Network File System
NSP	–	Network Service Provider
OSPF	–	Open Shortest Path First
PSTN	–	Public Switched Telephone Network
ROM	–	Read Only Memory
RIP	–	Routing Information Protocol
SCOS	–	Smart Card Operating System
SoD	–	Software on-Demand
SFS	–	SecureFast Packet Switch
VNet	–	SecureFast Virtual Networking
VNS	–	Virtual Network Server
VPN	–	Virtual Private Networks
WS	–	Work Station

ВСТУП

Інформаційні впливи на держави, суспільства, людей сьогодні часом бувають ефективнішими за політичні, економічні або військові. Впровадження сучасних інформаційних технологій, систем телекомунікації, кількісна зміна масштабів інформаційних взаємодій призвели до якісної зміни у підходах до розв’язання існуючих проблем і виникнення нових, яких не існувало на попередніх стадіях розвитку інформаційного суспільства.

Появилися нові проблеми також і у сфері інформаційної безпеки. У інформаційному суспільстві інформаційна безпека стає стратегічною категорією, складовою засадничих понять міжнародна безпека і національна безпека.

Інформаційна безпека має розглядатися у таких аспектах: соціально-економічного розвитку; збереження і захисту інформації; моніторингу та класифікації комп'ютерних і мережевих загроз; використання нових типів зброї та попередження інформаційних воєн.

У сучасній українській ринковій економіці обов'язковою умовою успіху в бізнесі, отримання прибутку та збереження у цілісності створеної організаційної структури є забезпечення економічної безпеки.

Однією з головних складових частин економічної безпеки є інформаційна безпека, яка досягається використанням комплексу методів та засобів захисту виробничої інформації від можливих зловмисних дій конкурентів з метою збереження її цілісності та конфіденційності.

Сьогодні злочинним шляхом використовується автоматизовані інформаційні системи насамперед у банківській сфері. Не є таємницею, що організовані злочинні угруповання мають у своїх ″штатах″ фахівців, які займаються розвідкою з використанням найсучасніших технологічних засобів для збирання важливої інформації про діяльність конкурентів, підприємств та фірм, які знаходяться у межах їх інтересів і, навіть, правоохоронних органів.

Укладачі у даному курсі лекцій багато уваги приділили висвітленню таких актуальних питань, як захист державних інформаційних ресурсів у інформаційно системах; захисту інформації, яка становить комерційну таємницю; захисту інформації у електронних банківських системах та алгоритми криптографічного захисту електронних платіжних карт.

Детально розглянуті питання захисту потоків корпоративних даних, що передаються відкритими мережами, аналізу загроз у VPN-мережах, які є не тільки "гарячою" темою для аналітиків, але привертають пильну увагу як надавачів мережевих послуг (Internet-провайдерів), так і корпоративних користувачів.

Важливим напрямком підвищення ефективності функціонування інформаційних систем підприємств є інтегрування з глобальною мережею Internet. У багатьох випадках завдяки, власне, ступеню інтегрування розв’язуються дві основні задачі. По-перше, об’єднуються територіально розподілені підсистеми ІС. По-друге, користувачам Internet забезпечується доступ до відкритої інформації ІС підприємств. Досить часто при розв’язанні обох задач використовується Web-сайт (Web-портал), який, крім того, відіграє представницьку роль підприємства у мережі Internet.

Практичний досвід показує, що функціонування Web-порталу значною мірою впливає на ефективність функціонування всієї ІС. Основою Web-порталу є Web-сервер, який забезпечує доступ користувачів із мережі Internet до Web-сторінок порталу підприємства.

Значну увагу приділено законодавчим аспектам у організації захисту інформації, які регламентують правила використання і оброблення інформації з обмеженим доступом та встановлюють міру відповідальності за порушення цих правил.

Загалом, незважаючи на позитивні зміни у законодавчому регулюванні інформаційних відносин обмеженість національного законодавства і відсутність єдиної правової бази у протидії порушенням безпеки ІС – одна з головних причин зростання кількості і високий рівень латентності злочинів пов’язаних з порушеннями інформаційної безпеки.

Важливою проблемою залишається і відсутність системного підходу до формування правової політики держави в інформаційній сфері.

З розвитком інформаційних технологій і систем захисту виникла потреба уніфікувати вимоги до їх проектування та впровадження забезпечивши необхідний рівень стандартизації. Одним з найважливіших напрямів цієї роботи є адаптування міжнародного стандарту ISO/IEC серії 27000.

Дотримання принципів стандартів ISO/IEC серії 27000 забезпечує керування і контроль доступом, розроблення та обслуговування апаратно-програмних комплексів, керування безперервністю інформаційних процесів. Відповідність вимогам стандартів ISO/IEC серії 27000 і дотримання національних правових норм з інформаційної безпеки є запорукою створення ефективної системи захисту інформації.

Усі пропозиції і зауваження просимо надсилати за адресою tarasrudyy@gmail.com, за що заздалегідь висловлюємо подяку.

ЛЕКЦІЯ 1.

ЕКОНОМІЧНІ ТА ІНФОРМАЦІЙНІ СИСТЕМИ

План

ВСТУП

В основі розвитку людського суспільства лежить виробництво матеріальних і духовних благ, інших цінностей, цілісна сукупність яких забезпечує умови життєдіяльності людини. Довільне суспільство, особливо сучасне високорозвинуте, є соціальною системою. Соціальна система – це складноорганізована, впорядкована цілісність, що включає окремих індивідів та соціальні спільноти, які об'єднані різноманітними зв'язками і взаємовідносинами, специфічними за своєю природою. Важливою підсистемою суспільства, основою соціальної системи є економічна система (ЕС).

У ході виробництва, розподілу, обміну та споживання благ між учасниками цих процесів складаються і постійно вдосконалюються різноманітні за своїм змістом економічні відносини. Останнє виявляється через економічну поведінку суб'єктів господарювання. Конкретна історична сукупність економічних відносин, що відповідає системі продуктивних сил і взаємодіє з нею, розвивається на основі дії як об'єктивних економічних законів, так і суб'єктивних чинників, визначає сутність ЕС суспільства.

1.1. Економічна система

У межах даного видання під терміном **економічна система** будемо розуміти сукупність усіх видів економічної діяльності людей у процесі їх взаємодії, спрямованої на: виробництво; обмін; розподіл; споживання товарів і послуг; на регулювання економічної діяльності.

Господарська діяльність в ЕС завжди виявляється організованою, скоординованою тим чи іншим чином, тому **економічна система** має складну структуру, яка утворюється в процесі взаємодії окремих елементів, якими є:

- продуктивні сили,
- техніко-економічні та організаційно-економічні відносини,
- виробничі відносини або відносини економічної власності,
- господарський механізм.

Отже, економічна система це сфера функціонування продуктивних сил і економічних відносин, взаємодія яких характеризує сукупність організаційних форм та видів господарської діяльності. Структурні ланки, що утворюють різноманітні ЕС, за своїм змістом неоднорідні. Вони поєднують у собі загальні та специфічні, основні та похідні, нові, що народжуються, та відмираючі старі, перехідні та проміжні економічні форми, кожна з яких функціонує на основі спільної для всієї системи і разом з тим власної логіки розвитку.

Характерними властивостями ЕС є цілісність, емерджентність, динамічність економічність процесів, невизначеність щодо розвитку економічних процесів.

В сучасних економічних умовах структурні елементи системи характеризуються динамізмом, мінливістю, суперечністю розвитку. Цим визначається необхідність структурної диференціації складових ланок економічної системи суспільства, без якої неможливо пізнати об'єктивні закони та принципи її функціонування. Довільна ЕС характеризується ієрархічністю, прагне набути стану цілісності та органічності. Ієрархія системи визначається місцем її елементів в соціальній структурі та механізмом їх субординації.

1.2. Взаємозв'язки елементів економічної системи

Тип взаємозв'язку елементів системи може бути ″вертикальним″ або ″горизонтальним″.

Вертикальна залежність виявляється у відносинах примусу, влади підкори, керованості підлеглості.

Горизонтальні зв'язки є партнерськими, добровільними, конкурентними. У соціальне орієнтованих економічних системах домінують саме партнерські взаємини.

Суб'єкти економічної системи. Особливе місце в становленні, функціонуванні та розвитку ЕС належить її суб'єктам як активній рушійній, перетворюючій силі. Кожний суб'єкт є носієм певних прав, обов'язків та відповідальності, які реалізує в процесі своєї функціональної діяльності.

Залежно від цього існують різноманітні класифікації економічних суб'єктів: індивід, колектив, держава; виробник (продавець), посередник, споживач (покупець); фізичні та юридичні особи; вітчизняні та іноземні; інституціональні (виробничі підприємства, банки, біржі) тощо.

Наявність не тільки необхідних, а й достатніх елементів для саморозвитку, самовідтворення, поліфункціональної діяльності системи характеризує її цілісність, самодостатність. Ознака органічності системи вказує на внутрішню, родинно-генетичну єдність, чистоту, нечужинність її елементів.

Органічність економічної системи. Чим більше в ЕС перехідних, змішаних явищ, форм та процесів, тим нижчий ступінь її органічності, чистоти. Таку тенденцію розвитку не слід розцінювати як однозначно негативну. Якщо в сучасних умовах взаємозалежність, взаємопереплетіння, конвергенція розвитку економічних систем збагачують, вдосконалюють одна одну це прогресивний процес. Економічна система характеризується різними сферами функціонування, рівнями господарювання її суб'єктів. Сучасна економічна система є не

сукупністю індивідуальних господарств одного рівня, а складною субординованою системою трьох рівнів, що взаємодіють.

Розвиненість, взаємодія та взаємодоповнення економічних рівнів є запорукою стійкості, динамічності та ефективної результативності системи. Здатність комплексно, адекватно і своєчасно реагувати на зміни навколишнього середовища свідчить про мобільність економічної системи. Це, в свою чергу, є запорукою як макро-, так і мікроекономічної рівноваги.

1.3. Компоненти економічної системи

Економічна система має три основні ланки, підсистеми:

1. Економічну структуру продуктивних сил суспільства.
2. Систему економічних відносин.
3. Механізм господарювання.

Продуктивні сили це система економічних чинників, які в процесі суспільного поділу праці забезпечують перетворення довкілля, створюють блага для задоволення потреб людини і суспільства, визначають рівень продуктивності суспільної праці.

Економічні відносини є сукупністю соціально-економічних та організаційно-виробничих зв'язків між господарюючими суб'єктами в процесі виробництва, розподілу, обміну та споживання матеріальних благ, послуг і доходів.

Механізм господарювання узгоджує функціонування і розвиток ланок економічної системи, приводить у відповідність продуктивні сили і економічні відносини. Він є сукупністю конкретних форм господарювання, організаційно-інституціональних систем, методів та важелів регулювання економічних процесів.

Механізм господарювання втілює дію як суб'єктивних, так і об'єктивних чинників. Вплив суб'єктивних чинників визначається цілеспрямованою діяльністю людини та її суспільних утворень.

Об'єктивні чинники означають незалежний від волі та свідомості людини, визначений дією економічних законів перебіг соціально-економічних процесів. Нехтування об'єктивними чинниками, керованість у своїх діях суб'єктивними бажаннями і довільними рішеннями окремих посадових осіб призводить до волюнтаризму, гальмує розвиток системи. Проте об'єктивні закони виявляють себе і реалізуються через діяльність людей, суспільних інституцій, держави. Чим вищий ступінь пізнання економічних законів, відповідності соціально-політичної та економічної практики їхнім вимогам, тим поступовішим і прогресивнішим є розвиток суспільної системи.

Отже, механізм господарювання є сукупністю форм організації та управління суспільними діями економічних суб'єктів, спрямованих на реалізацію економічних законів. Центральне місце в економічній системі належить людині. Як головна продуктивна сила, уособлення економічних відносин, суб'єкт і об'єкт господарської діяльності, носій і реалізатор економічних потреб та інтересів вона поєднує і узгоджує функціонування всіх ланок економічної системи. Місце людини в суспільній ієрархії, можливість і форми її самореалізації зумовлюють

характер ЕС. Поліструктурність і поліфункціональність людини визначають двоїстий характер продуктивних сил.

Економічні відносини. З одного боку, вони постають як натурально-речові, а з іншого як суспільні. З останніми пов'язане поняття технологічного способу виробництва, що відтворює поєднання засобів праці з організацією виробництва. Перехід від одного технологічного способу виробництва до іншого відбувається завдяки якісним змінам у характері засобів праці, прогресу науки і техніки. Відповідно до свого двоїстого характеру продуктивні сили суспільства функціонують і як техніка та технологія, і як суспільний організм. Специфіка процесу праці людей полягає в тому, що одночасно відбувається взаємодія їх з природою і між собою з приводу виробництва.

У структурі продуктивних сил людині та її праці належить центральне місце не лише як найактивнішій складовій частині, а й як безпосередньому джерелу матеріально-речових елементів, що входять до їх складу. Це надзвичайно важливе теоретичне положення було доведено ще представниками класичної школи політичної економії А. Смітом і Д. Рікардо. Матеріально-речові засоби виробництва розглядаються двоїсто як матеріалізація праці людини і як знаряддя цієї праці. Як головний елемент засобів виробництва останні можуть реалізувати свою суспільну корисність лише в процесі використання їх у предметній діяльності людини. Поза таким споживанням вони виступають як потенційні структурні елементи виробництва.

Продуктивні сили. Отже, за своїм змістом матеріально-речові продуктивні сили є органічним втіленням уречевленої й живої праці, функціональним поєднанням людини і засобів праці, що здійснюється у виробничому процесі. В ході виробничого споживання матеріально-речові продуктивні сили набувають нової якості перетворюються на продуктивну силу людини. Будь-який елемент матеріально-речових продуктивних сил завжди є безпосереднім продовженням природних сил людини, її енергетичного потенціалу. Використання енергії домашніх тварин і води, пари, електрики, токарного верстата, автоматизованих систем, транспортних засобів і сучасних комунікаційних структур, у тому числі космічних комплексів, слід розглядати як робочі органи людини, органічне продовження її фізичного уособлення та інтелекту.

У цьому розумінні продуктивні сили є не лише результатом втілення минулої праці людини, а й безпосереднім енергетичним потенціалом її праці. Коли розглядаються продуктивні сили у зв'язку з працею людини, йдеться про продуктивну силу не індивідуальної, а суспільної праці. Такий підхід має історичну основу, адже процес відокремлення людини від тваринного світу йшов як процес утвердження не окремо взятого індивіда, а як частки виробничого колективу, племені, роду, а потім і суспільства.

Констатація структурної двоїстості продуктивних сил суспільства має не тільки теоретичне, а й практичне значення. Проблема прискорення темпів зростання продуктивності праці не вичерпується розвитком техніки і технології. Виробничий досвід провідних зарубіжних фірм свідчить, що прямі інвестиції в основний капітал не завжди є визначальними. Є приклади, коли грошові вкладення зарубіжних фірм у живий капітал (людський фактор виробництва) та

організацію виробничого процесу (управління, систему постачання й реалізації готової продукції, маркетинг тощо) у кілька разів перевищують інвестиції безпосередньо в техніку і технологію. Це досить стабільна тенденція розвитку. За даними спеціального кон'юнктурного огляду, інвестиції 400 провідних корпорацій США у живий капітал та організацію виробничого процесу досягали в окремі роки повоєнного періоду понад 80 %. Зрозумілою стає інвестиційна політика, що склалася на Заході: вкладення в основний капітал, технічне і технологічне переоснащення виробництва може здійснюватися лише за умови створення відповідної організаційної структури і кваліфікаційного потенціалу виробничого персоналу всіх рівнів від робітника до президента виробничого об'єднання (корпорації). Потребує пріоритетної уваги перебудова організаційних ланок виробництва, без якої новітні техніка й технологія не дають необхідної віддачі, а в багатьох випадках навіть стають збитковими. Це підтверджує теоретичне положення про структурну двоїстість продуктивних сил суспільства при тому, що їхній матеріально-речовий зміст і заснована на суспільному поділі праці економічна форма їх організації діалектично єдині.

Специфіка економічної системи суспільства визначається соціально-економічними виробничими відносинами, які мають складну і багатогранну структуру, що ґрунтується на відносинах власності. Власність визначає суспільний спосіб поєднання робочої сили з засобами виробництва та відповідні стосунки між людьми з приводу привласнення матеріально-речових елементів і результатів виробничого процесу. Одночасно відносини власності зумовлюють історичну специфіку суспільства, його соціальну структуру, панівну систему політичної та економічної влади.

Соціально-економічні відносини є цілісною, структурно субординованою системою, що постійно розвивається від простого до складного. Основою цього процесу є розвиток продуктивних сил суспільства, їхньої матеріально-речової та економічної структури. При цьому виробничі відносини можуть відігравати двоїсту роль: двигуна, що стимулює і прискорює розвиток продуктивних сил, або сили, що гальмує цей розвиток. Водночас кожна система соціально-економічних відносин має й відносну самостійність, яка формується на основі свідомої діяльності людини, що бере участь у процесі виробництва, розподілу, обміну і споживання створюваних цінностей.

Отже, система соціально-економічних відносин формується і розвивається як система свідомо осмисленої функції людини, що органічно поєднує у своїй структурі об'єктивні й суб'єктивні чинники .

1.4. Класифікація економічних систем

Важливим питанням є класифікація економічних систем. ЕС складне, багатоструктурне і поліфункціональне соціально-економічне явище.

В економічній літературі визначають різні моделі, типи ЕС. Класифікація їх залежить від різних критеріїв. Головними з них є домінуюча форма власності, технологічний спосіб виробництва, спосіб управління і координування економічної діяльності тощо. Поділ економічних систем за переліченими озна-

ками є певною мірою умовним. Наприклад, поширеною є класифікація ЕС за технологічним способом виробництва, рівнем розвитку продуктивних сил.

Розрізняють: доіндустріальне суспільство (економічну систему, в якій домінує ручна праця); індустріальне суспільство, основою якого є машинна праця; постіндустріальне суспільство, що ґрунтується на автоматизованій праці, оснащеній комп'ютерною інформацією.

Однак ці системи суттєво розрізняються і механізмом господарювання, і домінуючим об'єктом власності, і різноманітністю суб'єктів економічної діяльності.

Багатокритеріальним є поділ ЕС на ринкові та адміністративно-командні системи.

Ринкова економіка. Основними характерними рисами ринкової економіки є такі: різноманітність форм власності при домінуванні приватної, панування товарно-грошових відносин, свобода підприємництва, конкурентний механізм господарювання, матеріальне стимулювання, вільне ціноутворення, що ґрунтується на взаємодії попиту і пропозиції, регулююча економічна роль держави, особиста свобода, домінування індивідуального інтересу тощо.

Адміністративна (командна, планова) економіка. Адміністративно-командна система заснована на пануванні державної власності, одержавленні народного господарства, відсутності конкуренції, директивному плануванні, неринкових господарських зв'язках, зрівняльному характері розподілу, ігноруванні законів товарно-грошового обігу, жорсткому ієрархічному підпорядкуванні суб'єктів господарювання, нерозвиненості або й відсутності ринкового менталітету тощо.

Останнім часом посилилися дискусії навколо понять ″змішана″ і ″перехідна″ економіка. Безперечно, це не тотожні поняття.

Змішана економічна система, яка характеризує сучасні розвинені країни, еволюціонувала з економіки чистого ринку, врахувала його недоліки і відмови.

Сучасні розвинені ЕС характеризуються різноманітністю форм власності та господарювання, якісними зрушеннями у відносинах приватної власності, конкурентному механізмі, значною економічною роллю держави, прогнозуванням соціально-економічних процесів тощо.

Перехідна економічна система характерна для країн, які звільняються від недоліків адміністративно-командної системи. В таких умовах трансформаційні процеси відбуваються суперечливо, бурхливо, з гострими соціально-економічними потрясіннями, кризовими явищами. Саме таке становище характерне для України, інших країн, що утворились на теренах колишнього СРСР.

Для жодної країни немає однозначних і загальновизнаних шляхів розвитку та безболісних рецептів досягнення добробуту і прогресу.

1.5. Інформаційні системи

Інформаційна система – сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів.

За ДСТУ 2392-94: Інформаційна система – комунікаційна система, яка забезпечує збирання, пошук, оброблення та пересилання інформації.

Таке визначення може бути задовільним тільки за найбільш узагальненої і неформальної точки зору і підлягає подальшому уточненню.

Основними чинниками, які впливають на впровадження інформаційних систем (ІС), є потреби організацій та користувачів, а також наявність відповідних засобів для їх формування. Найсуттєвіше на розвиток інформаційних систем вплинули досягнення в галузі інформаційних технологій загалом та телекомунікаційних систем, зокрема.

Причини, що спонукають організації впроваджувати ІС, з одного боку обумовлюються прагненням збільшити продуктивність повсякденних робіт чи усунути їх повторне проведення, а з іншого боку бажанням підвищити ефективність управління діяльністю організації за рахунок прийняття оптимальних та раціональних управлінських рішень.

Перша причина доволі прозора і для її реалізації достатньо впроваджувати стандартизовані системи обробки інформації. Успішне функціонування організації у значній мірі залежить від вдалого керівництва, яке базується на обґрунтуванні перспективних концепцій розвитку згідно з своєчасною, достовірною та повною інформацією, яку може поставляти відповідна ІС. Основне завдання ІС управління полягає у підпорядкуванні всіх внутрішніх процесів головним цілям організації. Для цього необхідно скоординувати процеси, пов'язані з діяльністю організації таким чином, щоб вони максимально забезпечували виконання поставлених задач в єдиному інформаційному полі. Тільки таким чином інформаційна озброєність організації починає безпосередньо впливати на ефективність її діяльності.

До основних напрямків автоматизації інформаційно-управлінської діяльності в організаційних структурах відносять:

- автоматизацію обробки документообігу, впровадження систем управління базами даних (СУБД), автоматизацію обміну інформацією через різноманітні види комунікацій (комп'ютерні мережі, телекомунікаційні системи);
- автоматизацію діяльності менеджерів на базі СУБД інформаційних систем, які надають підтримку в прийнятті управлінських рішень.

Впровадження ІС дозволяє менеджеру отримувати оперативний доступ до довільної нагромадженої інформації з тим, щоб в подальшому ефективно її використовувати для розв’язання поставлених задач (у сферах аудиту, маркетингу, фінансів, тощо)

1.6. ІС як складові системи управління

У науково-технічній літературі часто використовуються терміни ″система″, ″система управління″, ″автоматизована система управління″, ″інформаційна система″.

Слово ″система″ походить від грецького systema, що означає ціле, складене з частин чи множини елементів, зв'язаних один із одним і утворюючих певну цілісність, єдність.

Під системою розуміють сукупність зв'язаних між собою із зовнішнім середовищем елементів чи частин, функціонування яких спрямоване на одержання конкретного корисного результату.

Як приклад, можна назвати систему освіти, енергетичну, транспортну, економічну та інші системи.

Для системи характерні такі основні властивості:

- складність;
- подільність;
- цілісність;
- різноманіття елементів і різниця їх природи;
- структурованість.

Система, яка реалізовує функції управління, називається системою управління. Найважливішими функціями, які реалізуються цією системою, є прогнозування, планування, облік, аналіз, контроль та регулювання.

Управління пов'язане з обміном інформацією між компонентами системи, а також системи з навколишнім середовищем. У процесі управління одержуються відомості про стан системи в кожний момент часу, про досягнення (або не досягнення) заданої мети для того, аби впливати на систему і забезпечувати виконання управлінських рішень.

Оскільки здійснення управління виокремлюється в особливу функцію, тому на її виконанні спеціалізуються деякі елементи організацій. З огляду на це в межах організації можна виокремити керований процес (об'єкт управління) і керуючу частину (орган управління). Сукупність їх визначається як система управління.

Керуюча частина певним чином впливає на керований процес. Щоб керуюча частина могла здійснювати управління, їй необхідно зіставляти фактичний стан керованого процесу з метою управління, у зв'язку з чим керований процес впливає на керуючу частину. Взаємовплив обох частин здійснюється як передавання інформації. Таким чином, у системі управління завжди наявний замкнений інформаційний контур (рис. 1.1).

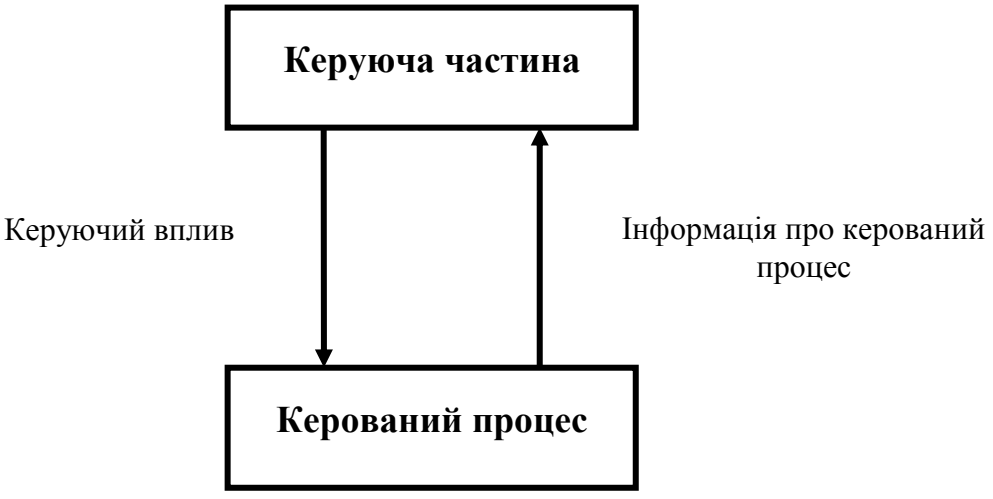


Рис. 1.1. Інформаційний контур

У межах інформаційного контуру існує і передається інформація про цілі управління, стан керованого процесу, про керуючі впливи. Інформаційний

контур разом із засобами збору, передавання, опрацювання і зберігання інформації, а також з персоналом, що здійснює ці дії над інформацією, утворить інформаційну систему даної організації.

Згідно з визначенням, поданим у Державному Стандарті України (ДСТУ), *інформаційна система* – це система, яка організовує накопичення і маніпулювання інформацією щодо проблемної сфери. Більш широко сутність ІС можна сформулювати так:

З позиції ділового бачення ІС – сукупність інформації, апаратно-програмних і технологічних засобів телекомунікацій, баз та банків даних, методів процедур оброблення даних, персоналу управління, які організовують процес збирання, передавання, оброблення і накопичування інформації, готування і прийняття ефективних управлінських рішень.

З технічної точки зору ІС може бути визначена як набір взаємозалежних компонентів, які збирають, оброблюють, зберігають і розподіляють інформацію, щоб підтримати процес прийняття управлінських рішень і управління організацією в цілому.

Із семантичної точки зору ІС – це сукупність різноманітних взаємопов'язаних або взаємозалежних відомостей про стан об'єкта управління та процеси, які відбуваються в ньому. Ці відомості виражені в показниках і інших інформаційних сукупностях, зібраних та оброблених за допомогою технічних засобів за визначеною методикою та заданими алгоритмами.

Місія ІС полягає в підготуванні і наданні інформації, необхідної для забезпечення ефективного управління всіма ресурсами підприємства.

До основних завдань ІС відносять:

- збір інформації з різних джерел;
- реєстрування, оброблення та подання інформації, яка характеризує стан виробництва й управління;
- розподіл інформації між керівниками, підрозділами та виконавцями відповідно до їх участі в управлінні.

Структурно ІС складається з таких компонентів (рис. 1.2):

- початкова інформація;
- система оброблення інформації;
- вихідна інформація.

До основних функцій ІС належать:

- *обчислювальна* (вчасне та якісне оброблення інформації в усіх аспектах, які забезпечують функціонування системи управління);
- *відстежувальна* (відстежування необхідної для управління зовнішньої і внутрішньої інформації);
- *запам'ятовувальна* (забезпечення постійного накопичення, система збереження і відновлення всієї необхідної інформації);
- *комунікаційна* (забезпечення передавання необхідної інформації в задані пункти);
- *інформаційна* (реалізування швидкого доступу, пошуку та подання необхідної інформації);

- *регулювальна* (здійснення інформаційного впливу на управління та його рівні у випадку відхилень фактичних значень від заданих);
- *оптимізаційна* (забезпечення оптимальних розрахунків у міру зміни критеріїв та умов функціонування об'єкта управління);
- *прогнозування* (визначення основних тенденцій, закономірностей і показників розвитку об'єкта управління);
- *аналітична* (визначення основних показників техніко-економічної діяльності об'єкта управління);
- *документувальна* (забезпечення отримання всіх обліково-звітних, та інших форм документів).

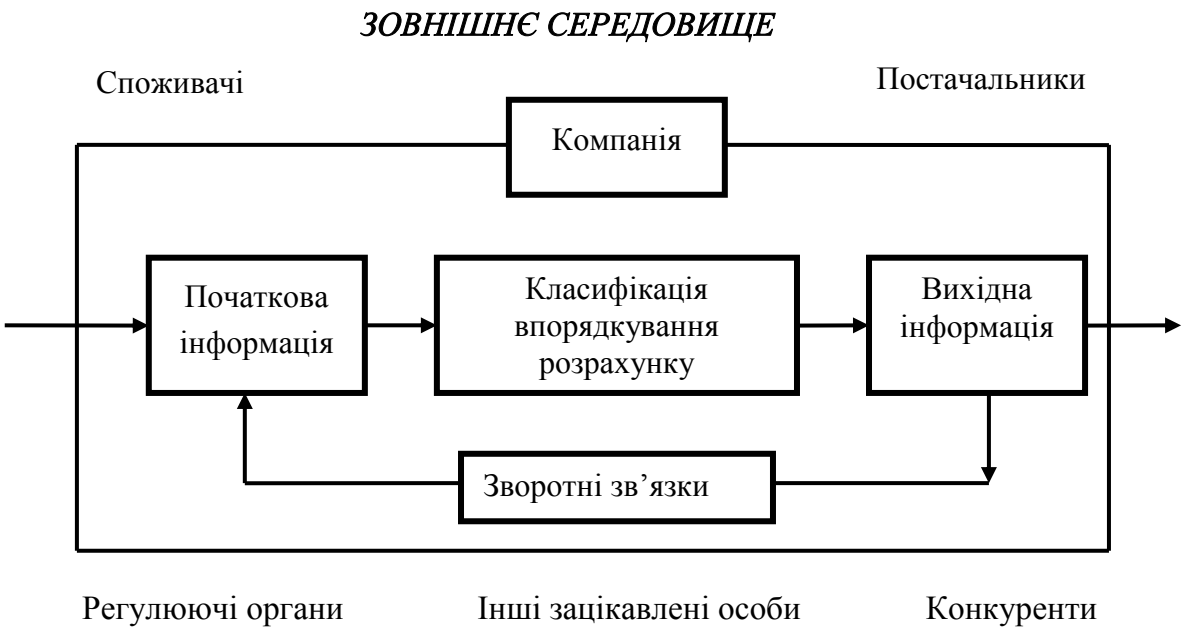


Рис. 1.2. Загальна схема ІС

1.7. Типова структура та склад ІС

Практично всі різновиди ІС незалежно від сфери їх застосування включають один і той самий набір компонентів (рис. 1.3):

- функціональні компоненти;
- компоненти системи опрацювання даних (СОД);
- організаційні компоненти.

При цьому, під функцією управління слід розуміти спеціальний постійний обов'язок однієї або декількох осіб, виконання якого забезпечує досягнення певного ділового результату.

Під функціональними компонентами мають на увазі систему функцій управління – повний набір (комплекс) взаємопов'язаних у часі й просторі робіт з управління, необхідних для досягнення поставлених перед підприємством цілей. Тобто, довільна складна управлінська функція розчленовується на ряд більш дрібних задач і, зрештою, доводиться до безпосереднього виконавця.

Природно, подані положення підкреслюють не тільки індивідуальний, а й груповий характер функції управління, а практичний результат утворюється не епізодично, а постійно.

Увесь процес управління підприємством зводиться або до лінійного управління підприємством або його структурним підрозділом, або до функціонального управління. Тому, декомпозиція ІС за функціональною ознакою (рис. 1.3) містить у собі виокремлення її окремих частин, які мають назву функціональних підсистем (функціональні модулі, бізнес-додатки), що реалізують систему функцій управління.

Функціональною ознакою зумовлюється призначення підсистеми, тобто те, для якої сфери діяльності вона призначена і які основні цілі, завдання і функції вона виконує. Функціональні підсистеми істотно залежать від предметної області (сфери застосування) ІС. Таким чином, задача повинна розглядатися як елемент системи управління, а не як елемент системи опрацювання даних.

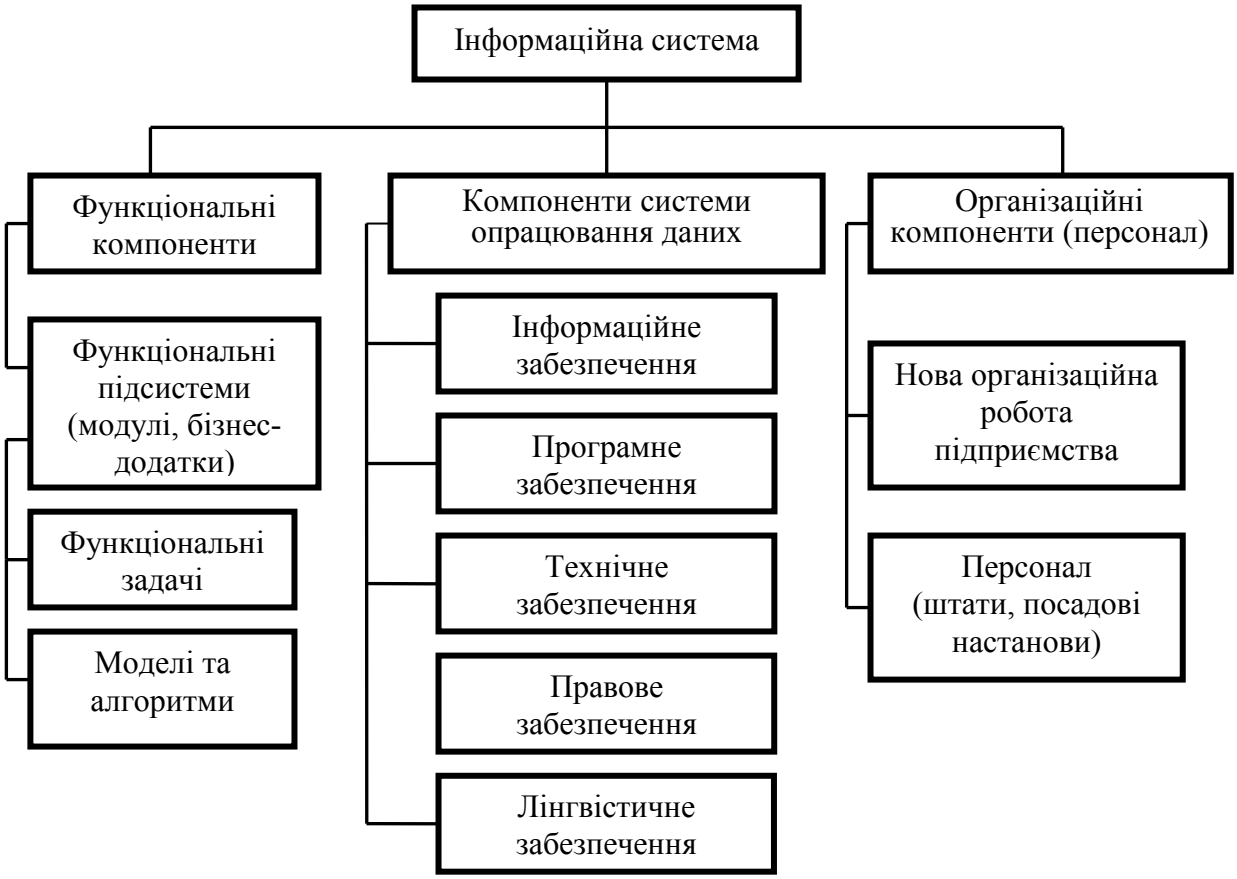


Рис. 1.3. Декомпозиція ІС

Вибір складу функціональних задач функціональних підсистем управління здійснюється з урахуванням основних фаз управління: планування; організації; мотивування і контролю.

1.8. Компоненти системи опрацювання даних

Основна функція системи опрацювання даних – це реалізування таких типових операцій опрацювання даних:

- збір, реєстрація і перенесення інформації на фізичні носії;
- передавання інформації в місця її збереження й опрацювання;
- уведення інформації в ЕОМ, контроль уведення та компонування інформації у пам'яті комп'ютера;

- створення і ведення внутрішньомашинної інформаційної бази;
- опрацювання інформації на ЕОМ (накопичення, сортування коригування, вибірка, арифметичне і логічне опрацювання) для розв’язання функціональних задач системи (підсистеми) управління об'єктом;
- вивід інформації у вигляді сигналів для прямого управління технологічними процесами, інформації для зв'язку з іншими системами;
- організація, управління (адміністрування) обчислювальним процесом (планування, облік, контроль, аналіз реалізації ходу обчислень в обчислювальних мережах).

Система опрацювання даних (СОД) призначена для інформаційного обслуговування фахівців різних органів управління підприємства, які приймають управлінські рішення.

Виокремлення типових операцій опрацювання даних дозволили створити спеціалізовані програмно-апаратні комплекси, що їх реалізують (різні периферійні пристрої, оргтехніку, стандартні набори програм, у тому числі пакети прикладних програм – ППП за допомогою яких реалізують функціональні задачі ІС). Конфігурація апаратних комплексів утворює так звану топологію обчислювальних систем.

Практично всі системи опрацювання даних ІС незалежно від сфери застосування їх включають один і той самий набір складових (компонентів), які називаються видами забезпечення (рис. 1.3). Прийнято виділяти інформаційне, програмне, технічне, правове, лінгвістичне забезпечення.

Інформаційне забезпечення – це сукупність методів і засобів розміщення й організації інформації, що включають у себе системи класифікації і кодування, уніфіковані системи документування, раціоналізації документообігу та форми документів, методів створення внутрішньомашинної інформаційної бази ІС. Від якості інформаційного забезпечення значною мірою залежить достовірність і якість прийнятих управлінських рішень.

Програмне забезпечення – сукупність програмних засобів для створення та експлуатації СОД засобами обчислювальної техніки. До складу програмного забезпечення входять базові (загальносистемні) та прикладні (спеціальні) програмні продукти. Базові програмні засоби служать для автоматизації взаємодії людини і комп'ютера, організації типових процедур опрацювання даних, контролю і діагностики функціонування технічних засобів СОД.

Прикладне програмне забезпечення представляє собою сукупність програмних продуктів, призначених для автоматизації вирішення функціональних задач ІС. Вони можуть буті розроблені як універсальні засоби (текстові редактори, електронні таблиці, системи управління базами даних) і як спеціалізовані, тобто такі, що реалізують функціональні підсистеми (бізнес-процеси) об'єктів різної природи (економічні, інженерні, технічні)

Технічне забезпечення є комплексом технічних засобів, що застосовуються для функціонування системи опрацювання даних, і містить у собі пристрої, за допомогою яких виконуються типові операції опрацювання даних як поза ЕОМ (периферійні технічні засоби збору, реєстрації, первинного опрацювання

інформації, оргтехніка різного призначення, засоби телекомунікації і зв'язку), так і на ЕОМ різних класів.

Правове забезпечення – це сукупність правових норм, що регламентують створення і функціонування ІС. Правове забезпечення розробки ІС включає нормативні акти договірних взаємовідносин між замовником і розробником ІС, правове регулювання відхилень. Правове забезпечення функціонування СОД включає: умови надання юридичної чинності документам, отриманим із застосуванням обчислювальної техніки; права, обов'язки і відповідальність персоналу, в тому числі за своєчасність і точність опрацювання інформації; правила користування інформацією і порядок вирішення суперечок щодо її достовірності.

Лінгвістичне забезпечення – це сукупність мовних засобів що використовуються на різних стадіях створення та експлуатації СОД для підвищення ефективності розробки й забезпечення спілкування людини і ЕОМ.

Ергономічне забезпечення розглядають як сукупність методів і засобів, які використовуються на різних етапах розробки та функціонування ІС, призначене для створення оптимальних умов високоефективної і безпомилкової діяльності людини, спрямованої на якомога швидше освоєння цієї системи. До його складу входять: комплекс різноманітної документації, яка містить ергономічні вимоги до робочих місць, інформаційних моделей, умов діяльності персоналу, а також набір найдоцільніших способів реалізації цих вимог і здійснення ергономічної експертизи рівня їх реалізації; комплекс методів, навчально-методичної документації і технічних засобів, які забезпечують обґрунтованість вимог до рівня підготовки персоналу.

1.9. Організаційні компоненти ІС

Виділення організаційних компонентів у самостійний напрям зумовлюється особливою значущістю людського чинника (персоналу) в успішному функціонуванні ІС. Перш ніж упроваджувати дорогу систему опрацювання даних, має бути проведена величезна робота з упорядкування та удосконалення організаційної структури об'єкта; в противному разі ефективність ІС буде низькою.

Під *організаційними компонентами ІС* мають на увазі сукупність методів і засобів, що дозволяють удосконалити організаційну структуру об'єктів і управлінські функції, які виконуються структурними підрозділами; визначити штатний розклад і чисельний склад кожного структурного підрозділу; розробити посадові інструкції персоналу управління в умовах функціонування СОД.

Впровадження ІС сприяє удосконаленню організаційних структур, оскільки передбачає визначення розрахункової, тобто науково обґрунтованої, чисельності апарату управління за структурними підрозділами.

1.10. Класифікація ІС. Рівні ІС в організації

ІС можуть бути класифікованими за рядом характерних ознак.

За рівнем у системі державного управління: територіальні і галузеві; міжгалузеві; підприємств.

За рівнем інтелектуалізації: інформаційно-довідкові; інформаційно-пошукові; підтримки прийняття управлінських рішень; з використанням баз знань; експертні системи.

За ступенем централізації оброблення інформації: централізовані і децентралізовані;

За принципом інтегрування: багаторівневі з інтегруванням за рівнями управління та функціями управління; одноріневі.

За видами процесів: для наукових досліджень; для автоматизованого проектування; організаційного управління; управління виробничими процесами; управління технологічними процесами; навчальні.

За сферою діяльності: культурологічні; владні; науково-технічні; соціальні; фінансово-економічні; міжнародних організацій;

За режимом оброблення інформації: в режимі реального часу; в автономному режимі.

За рівнем у системі державного управління: загальнодержавні ІС призначені для вирішення найважливіших проблем національної економіки. тощо.

Територіальні (регіональні) ІС призначені для управління адміністративно-територіальними регіонами. Сюди належать ІС області, міста, району. Ці системи здійснюють оброблення інформації, яка необхідна для реалізування функцій управління регіоном, формування звітності і подання оперативних даних органам місцевого самоврядування.

Галузеві ІС управління призначені для галузей управління підвідомчими підприємствами. Галузеві ІС діють у промисловості, енергетиці, транспорті тощо. У них розв'язуються задачі інформаційного обслуговування апарату управління відповідних міністерств.

Міжгалузеві ІС є спеціалізованими системами функціональних органів управління національною економікою (планових, фінансових, статистичних та інших).

Централізовані ІС – накопичення і оброблення інформації здійснюється в єдиному центрі. Доступ інформаційних ресурсів ІС може здійснюватись віддалено.

Децентралізовані ІС побудовані за автономним принципом. Кожна ІС певного рівня обслуговує певне коло користувачів.

Оскільки організації мають різноманітні інтереси і структуру тому для їх обслуговування існують різні види ІС. Ніяка єдина система не може цілком забезпечувати потреби організації у всій інформації. Розглянемо види ІС, які складають основу організації.

Організація поділена на рівні: стратегічний; управлінський; знання й експлуатаційний. Далі ІС поділена на функціональні області типу продажу і маркетингу, виробництва, фінансів, бухгалтерського обліку і людських ресурсів.

Системи створюються, щоб обслуговувати ці різні організаційні інтереси. Організаційні рівні обслуговують чотири головних типии ІС: системи експлуатаційного рівня, системи рівня знань, системи управлінського рівня та стратегічні системи.

Системи експлуатаційного рівня підтримують операційних менеджерів, стежать за елементарними діями організації типу продажу, платежів, кредитування та ін. Основна мета систем на цьому рівні полягає в тому, щоб відповісти на типові питання і проводити потоки трансакцій через організацію.

Системи рівня знань підтримують працівників знання й оброблювачів даних в організації. Мета систем рівня знань полягає в тому, щоб допомогти діловій фірмі інтегрувати нове знання в бізнес і допомагати організації керувати потоком документів.

Системи рівня знань, особливо у формі робочих станцій і офісних систем, сьогодні є найбільш швидко зростаючими додатками в бізнесі.

Системи управлінського рівня розроблені, щоб обслуговувати контроль, управління, прийняття рішень і адміністративні дії середніх менеджерів. Вони визначають, чи добре працюють об'єкти, і періодично сповіщають про це. Наприклад, система управління переміщеннями повідомляє про переміщення загальної кількості товару, рівномірність роботи торговельного відділу і відділу, що фінансує витрати для службовців у всіх філіях компанії, відзначаючи, де фактичні витрати перевищують бюджети.

Системи стратегічного рівня – це інструмент допомоги керівникам вищого рівня, що готують стратегічні дослідження і тривалі тренди у фірмі й у діловому оточенні. Їхнє основне призначення - приводити у відповідність зміни в умовах експлуатації з існуючою організаційною можливістю. Який буде рівень зайнятості через п'ять років? Які тривалі промислові фінансові тренди і де наші підйоми і спади? Які вироби ми повинні робити через п'ять років?

ІС можуть також бути диференційовані функціональним чином. Головні організаційні функції типу продажу, виробництва, фінансів, бухгалтерського обліку і людських ресурсів обслуговуються власними інформаційними системами.

Типова організація має системи різних рівнів: експлуатаційного, управлінську, знання і стратегічну для кожної функціональної області. Наприклад, комерційна функція має комерційну систему на експлуатаційному рівні, щоб робити запис щоденних комерційних даних і обробляти замовлення.

Системи управлінського рівня відслідковують щомісячні комерційні дані всіх комерційних територій і доповідають про території, де продаж перевищує очікуваний рівень або падає нижче очікуваного рівня. Система прогнозу прогнозує комерційні тренди протягом п'ятирічного періоду – обслуговує стратегічний рівень.

Висновки: Економічна система – це об’єктивна єдність закономірно пов’язаних між собою явищ і процесів економічного життя. Вона характеризується багатогранністю, усі її елементи перебувають в органічному взаємозв’язку один з одним і не існують поза її межами. Функціональна подібність до живого організму надає елементам економічної системи органічної цілісності. Цим дана система відрізняється від інших так званих сумарних систем.

ЛЕКЦІЯ 2.

ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В ІС

План

Вступ.

2.1. Поняття політики безпеки ІС

2.2. Організація системи інформаційної безпеки підприємства

2.3. Класифікація загроз

2.4. Основні види загроз безпеці інформації

2.5. Основні форми захисту інформації.

2.6. Криптографічний захист інформації

ВСТУП

Під безпекою *інформаційної системи* розуміють її здатність протидіяти спробам нанесення збитків власникам та користувачам ІС методами створення різноманітних збуджуючих (навмисних і ненавмисних) впливів на неї. Природа впливів може бути різноманітною: спроба фізичного проникнення зловмисника, помилки персоналу, стихійні лиха (ураган, пожежа), вихід з ладу окремих ресурсів.

На сьогодні склалися *два підходи до забезпечення безпеки ІС*:

- *фрагментарний підхід*, сутність якого полягає у протидії строго визначеним загрозам за конкретних умов (спеціалізовані антивірусні засоби, автономні засоби шифрування тощо);
- *комплексний підхід*, який передбачає створення середовища оброблення інформації, що об’єднує різноманітні (правові, організаційні, програмно-технічні) заходи для протидії загрозам.

Комплексний підхід, як правило, використовується для захисту великих ІС. У цьому випадку необхідно забезпечити виконання наступних заходів:

- організаційні заходи з контролю за персоналом, який має високий рівень повноважень на дії в ІС (програмісти, адміністратори баз даних ІС);
- організаційні та технічні заходи з резервування стратегічно важливої інформації;
- організаційні заходи з відновлення працездатності ІС у випадку виникнення нештатних ситуацій;
- організаційні та технічні заходи з управління доступом у приміщення, в яких знаходяться програмно-технічні засоби;
- організаційні та технічні заходи з фізичного захисту приміщень, в яких знаходяться програмно-технічні засоби і носії даних, від стихійних лих, масових безладів тощо.

2.1. Поняття політики безпеки ІС

У 1985 році Національним центром інформаційної безпеки Міністерства оборони США була опублікована, так звана, ″Помаранчева книга″ (″Критерії оцінки достовірності обчислювальних систем Міністерства оборони″). У ній були подані основні положення, за якими американське оборонне відомство визначало ступінь захищеності інформаційно-обчислювальних систем. У

систематизованому вигляді подано основні поняття, рекомендації і класифікація за видами загроз безпеці ІС і методи захисту від них. У подальшому книга перетворилась у збірку науково-обґрунтованих норм і правил, які описують системний підхід для забезпечення безпеки електронних інформаційних систем та їх елементів, і стала настільною книгою для фахівців у галузі захисту інформації. Запропонована у ″Помаранчевій книзі″ методологія за своєю сутністю стала загальноприйнятою, а її основні положення внесені до національних стандартів різних країн.

Системний підхід згідно з ″Помаранчевою книгою″ вимагає: прийняття принципових рішень у галузі безпеки на основі моніторингу поточного стану ІС; прогнозування можливих загроз і аналізу пов’язаного з ними ризику для ІС; планування заходів з запобігання виникнення критичних ситуацій; планування заходів виходу з критичних ситуацій.

Одне з основних понять, введених у ″Помаранчевій книзі″, це політика безпеки. *Політика безпеки* – це сукупність норм, правил і методик, на основі яких у подальшому базується діяльність ІС в галузі оброблення, зберігання і розподілення критичної інформації. При цьому під ІС розуміють не тільки апаратно-програмний комплекс, але і обслуговуючий персонал.

Політика безпеки формується на основі аналізу поточного стану і перспективи розвитку ІС, можливих загроз і визначає: мету, задачі та пріоритети системи безпеки; галузь дії окремих підсистем; гарантований мінімальний рівень захисту; обов’язки персоналу із забезпечення захисту; санкції за порушення захисту.

Якщо виконання політики безпеки проводиться не повною мірою або непослідовно, тоді ймовірність порушення ЗІ різко зростає. Під *захистом інформації* розуміють комплекс заходів, який забезпечує:

- збереження конфіденційності інформації – запобігання ознайомлення з інформацією неуповноважених осіб; збереження інформації – запобігання пошкодженню або знищенню інформації внаслідок свідомих дій зловмисника, помилок персоналу, стихійного лиха; прозорість, тобто наявність системи безпеки не повинна створювати перешкод для нормальної роботи ІС.

Впровадження політики безпеки неможливе без аналізу ризику. Аналіз ризику підвищує рівень поінформованості про слабкі та сильні сторони захисту, створює базу для прийняття рішень, оптимізує розмір витрат на захист, оскільки більша частина ресурсів спрямовується на блокування загроз, які можуть принести найбільшу шкоду.

Аналіз ризику складається з наступних основних етапів:

1. Опис складу ІС – апаратних засобів, програмного забезпечення, даних, документації, персоналу.
2. Визначення слабких місць – з’ясовуються слабкі місця за кожним елементом ІС з оцінкою ймовірних джерел загроз.
3. Оцінювання ймовірності реалізування загроз.
4. Оцінювання очікуваних розмірів втрат – цей етап складний, оскільки не завжди можливе кількісне оцінювання даного показника.
5. Аналіз можливих методів і засобів захисту.

6. Оцінювання виграшу від прийнятих заходів. Якщо очікувані втрати більші від допустимого рівня, необхідно посилити заходи безпеки.

Аналіз ризику завершується прийняттям політики безпеки і складанням плану захисту з обов'язковими наступними розділами:

1. Поточний стан. Опис статусу системи безпеки на момент формування плану.
2. Рекомендації. Вибір основних засобів захисту, які реалізують політику безпеки.
3. Відповідальність. Перелік відповідальних працівників і зон відповідальності.
4. Розклад. Визначення порядку роботи механізмів захисту, в тому числі і засобів контролю.

2.2. Організація системи інформаційної безпеки підприємства

Основним питанням початкового етапу впровадження системи ІБ підприємства є призначення відповідальних осіб за безпеку і розмежування сфер їх впливу. Як правило, ще на етапі початкової постановки завдань з'ясовується, що за цей аспект ІБ підприємства відповідати дуже складно. Системні програмісти і адміністратори схильні відносити цю задачу до компетенції загальної служби безпеки, тоді як остання вважає, що це питання знаходиться в компетенції фахівців з ІС.

При розв'язанні завдань розподілу відповідальності за безпеку ІС підприємства необхідно враховувати наступні положення: ніхто, крім керівництва, не може прийняти основоположні рішення в галузі політики ІБ; ніхто, крім фахівців, не зможе забезпечити правильне функціонування системи ІБ; жодна зовнішня організація або група фахівців життєво не зацікавлена в економічній ефективності впровадження заходів безпеки.

Організаційні заходи безпеки ІС безпосередньо або опосередковано пов'язані з адміністративним управлінням і відносяться до рішень та дій, які застосовуються керівництвом для створення таких умов експлуатації, що зведуть до мінімуму слабкість системи захисту. Дії адміністрації можна регламентувати наступними напрямками: заходи фізичного захисту ІС; регламентування технологічних процесів; регламентування роботи з службовою інформацією; регламентування процедур резервування; регламентування внесення змін; регламентування роботи персоналу і користувачів; підбір та підготовка кадрів; заходи контролю і спостереження.

На практиці найчастіше використовуються наступні *категорії інформації*.

Важлива інформація – незамінна та необхідна для функціонування ІС інформація, процес відновлення якої після знищення неможливий або дуже трудомісткий і пов'язаний з великими матеріальними витратами, а її помилкове застосування або модифікування призводить до значних втрат.

Корисна інформація – необхідна для функціонування ІС інформація, яка може бути відновлена без великих матеріальних витрат, при чому її модифікування або знищення призводить до відносно невеликих втрат.

Конфіденційна інформація – інформація, доступ до якої для частини персоналу або сторонніх осіб небажаний, оскільки може спричинити матеріальні та моральні втрати.

Відкрита інформація – це інформація, доступ до якої відкритий для всіх.

Керівництво повинно приймати рішення про те, хто і яким чином буде визначати ступінь конфіденційності та важливості інформації. На жаль, у нашій державі ще не повністю сформоване законодавство, щоб розглядати інформацію як товар та регламентувати права інтелектуальної власності на ринку інтелектуального продукту, як це робиться в світовій практиці.

2.3. Класифікація загроз

Під загрозою безпеці розуміють потенційні дії або події, які можуть безпосередньо або опосередковано нанести втрати – призвести до розладу, спотворення або несанкціонованого використання ресурсів ІС, включаючи інформацію, яка зберігається, передається, обробляється, а також програмні та апаратні засоби.

Не існує єдиної загальноприйнятої класифікації загроз, хоча розроблено багато її варіантів. Подамо перелік подібних класифікацій: за метою реалізування загроз; за принципом дії загроз на ІС; за характером впливу загроз на ІС; за причиною виникнення помилки захисту; за способом дії атаки на об’єкт; за об’єктом атаки; за використовуваними засобами атаки; за станом об’єкту атаки.

Загрози прийнято поділяти на *випадкові* (або ненавмисні) і *навмисні*. Джерелом *випадкових загроз* можуть бути помилки в програмному за безпеченні, виходи з ладу апаратних засобів, неправильні дії користувачів або адміністрації ІС тощо. *Навмисні загрози*, на відміну від випадкових, призначені нанести максимальну шкоду ІС і, в свою чергу, поділяються на пасивні і активні.

Пасивні загрози, як правило, спрямовані на несанкціоноване використання інформаційних ресурсів ІС, не впливаючи при цьому на її функціонування. Пасивною загрозою є, наприклад, спроба отримання інформації, яка поширюється каналами передавання даної ІС, шляхом підслуховування.

Активні загрози передбачають порушення нормального функціонування ІС шляхом цілеспрямованого впливу на її апаратні, програмні та інформаційні ресурси.

До активних загроз відносяться, наприклад, активне знищення або радіоелектронне заглушення ліній зв’язку ІС, вивід з ладу сервера або операційної системи, спотворення відомостей у базах даних або системної інформації ІС тощо. Джерелами активних загроз можуть бути безпосередні дії зловмисників, програмні віруси.

2.4. Основні види загроз безпеці інформації

До *основних загроз безпеці інформації* в ІС відносяться: розкриття службової інформації; компрометація інформації; несанкціоноване використання ресурсів ІС; помилкове використання ресурсів ІС; несанкціонований обмін інформацією; відмова від інформації; відмова в обслуговуванні.

Засобами реалізування *загрози розкриття службової інформації* може бути НСД до баз даних ІС, прослуховування каналів ІС тощо. У кожному випадку

отримання інформації, яка є власністю деякої особи (або групи), наносить її власникам суттєву шкоду.

Компрометація інформації, як правило, здійснюється шляхом внесення несанкціонованих змін у бази даних ІС, в результаті чого її користувач змушений відмовитись від неї або витратити додаткові зусилля та кошти для виявлення змін і відновлення істинних відомостей. У випадку використання скомпрометованої інформації користувач може прийняти неправильні рішення з усіма наслідками, які звідси випливають.

Несанкціоноване використання ресурсів ІС, з однієї сторони, є засобом розкриття або компрометації інформації, а з іншої – має самостійне значення, оскільки, навіть не маючи відношення до користувацької або системної інформації, може нанести певні збитки абонентам або адміністрації ІС. Обсяги збитків можуть змінюватися в широких межах – від скорочення поступлення фінансових ресурсів до повного виходу ІС з ладу.

Помилково санкціоноване використання ресурсів ІС теж може призвести до знищення, розкриття або компрометації вказаних ресурсів. Така загроза найчастіше всього є наслідком помилок програмного забезпечення.

Несанкціонований обмін інформацією між абонентами ІС може призвести до отримання одним із них відомостей, доступ до яких йому заборонений, що за своїми наслідками рівнозначне розкриттю інформації.

Відмова від інформації полягає в невизнанні адресатом або відправником цієї інформації фактів її отримання або відправлення. Це, зокрема, може послужити аргументованим приводом до відмови однією з сторін від раніше укладеної угоди (фінансової, торговельної, дипломатичної тощо) ″технічним шляхом″, формально не відмовившись від неї, але тим самим може нанести іншій стороні значні матеріальні збитки.

Відмова в обслуговуванні – це дуже суттєва і достатньо розповсюджена загроза, джерелом якої є сама ІС. Подібна відмова особливо небезпечна в ситуаціях, коли затримка з наданням ресурсів ІС абоненту може призвести до тяжких для нього наслідків. Наприклад, відсутність у абонента даних, необхідних для прийняття рішень, може бути причиною його нераціональних або неоптимальних дій.

2.5. Основні форми захисту інформації

У загальній системі забезпечення безпеки захист інформації відіграє значну роль. Виділяють наступні підходи в організації ЗІ: правовий; фізичний; управління доступом; криптографічне закриття.

До правових способів захисту інформації відносяться Закони України, законодавчі акти, які регламентують правила використання і оброблення інформації обмеженого доступу і встановлюють міру відповідальності за порушення цих правил.

Фізичні способи захисту інформації ґрунтуються на запровадженні перешкод для зловмисника, закриваючи шлях до захищеної інформації (сувора система допуску на територію або в приміщення з апаратурою, носіями інформації). Ці способи захищають тільки від зовнішніх зловмисників і не захищають

інформацію від тих осіб, які володіють правом доступу до неї. Нагромаджена статистика свідчить, що 75 % порушень здійснюють працівники цієї ж організації.

Під управлінням доступом розуміють ЗІ шляхом регулювання доступу до всіх ресурсів ІС (технічних, програмних, елементів баз даних). Регламентується порядок роботи користувачів і персоналу, право доступу до окремих файлів у базах даних тощо.

У відповідності з встановленою класифікацією даних, користувачів, апаратури, приміщень відповідальні за безпеку розробляють багаторівневу підсистему управління доступом, яка повинна виконувати такі завдання: ідентифікувати користувачів, персонал, ресурси ІС шляхом присвоювання кожному об'єкту персонального ідентифікатора (коду, імені); автентифікувати, встановлювати достовірність об'єктів за поданими відомостями (паролі, ключі, коди та інші ознаки); проводити авторизацію (перевіряти повноваження) запитів суб'єкта у відповідності до встановленого регламенту роботи; організовувати роботу у відповідності із загальним регламентом; протоколювати звернення до захищених компонентів ІС; реагувати на несанкціоновані дії (затримка або відмова в обслуговуванні, спрацювання сигналізації).

Комплексний розгляд питань забезпечення безпеки ІС знайшов відображення у, так званій, *архітектурі безпеки*, в рамках якої розрізняють загрози безпеці, а також послуги (служби) і механізми її забезпечення.

Служби безпеки, на концептуальному рівні, специфікують напрями нейтралізування загроз. У свою чергу, вказані напрями реалізуються механімами безпеки. У рамках ідеології ″взаємодії відкритих інформаційних систем″ служби і механізми безпеки можуть використовуватися на довільному з рівнів еталонної моделі взаємодії відкритих систем (OSI): фізичному, канальному, мережевому, транспортному, сеансовому, представницькому, прикладному.

Перед розглядом служб безпеки слід звернути увагу на ту обставину, що протоколи інформаційного обміну поділяються на два типи: віртуального з'єднання і дейтаграмні. У відповідності з вказаними протоколами прийнято ділити мережі на віртуальні і дейтаграмні. У перших передавання інформації між абонентами організовується віртуальним каналом і проходить у три етапи (фази): створення (встановлення) віртуального каналу, передавання повідомлення і знищення віртуального каналу (роз'єднання). При цьому повідомлення розбивається на блоки (пакети), які передаються в порядку їх розташування у повідомленні. *У дейтаграмних мережах* блоки повідомлень передаються від відправника до адресата незалежно один від одного і різними маршрутами, в зв'язку з чим порядок доставлення блоків може не відповідати порядку їх розташування у повідомленні. *Віртуальна мережа* відтворює принцип організації телефонного зв'язку, тоді як дейтаграмна – поштового. Ці два підходи визначають деякі розбіжності в складі і особливостях служб безпеки.

2.6. Криптографічний захист інформації

У ІС найефективнішими є криптографічні способи ЗІ, які характеризуються найвищим рівнем захисту. Для цього використовуються програми крип-

тографічного перстворення (шифрування) та програми захисту юридичної значимості документів (цифровий підпис). Шифрування забезпечує засекречування і використовується в ряді інших сервісних служб. Шифрування може бути симетричним і асиметричним. *Симетричне шифрування* базується на використанні одного і того ж секретного ключа для шифрування і дешифрування.

Асиметричне шифрування характеризується тим, що для шифрування використовується один ключ, а для дешифрування – інший, секретний. При цьому наявність і навіть знання загальнодоступного ключа не дозволяє визначити секретний ключ. Для використання механізмів криптографічного закриття інформації в ІС необхідна організація спеціальної служби генерування ключів і їх розподіл між абонентами.

Подамо короткий перелік деяких найвідоміших алгоритмів шифрування:

1. *Метод* DES (Data Encryption Standard), який є федеральним стандартом США, розроблений фірмою IBM та рекомендований для використання Агентством національної безпеки США. Алгоритм криптографічного захисту відомий і опублікований. Він характеризується такими властивостями: високим рівнем захисту даних проти дешифрування і можливого модифікування даних; простотою розуміння; високим ступенем складності, який робить його розкриття дорожчим від отримуваного прибутку; методом ЗІ, який базується на ключі і не залежить від ″таємності″ механізму алгоритму; економічністю у реалізуванні та ефективним у швидкодії алгоритмом. Разом з тим йому притаманний ряд недоліків: малий розмір ключа; окремі блоки, які містять однакові дані, будуть виглядати однаково, що є погано з точки зору криптографії.

2. *Російський стандарт шифрування даних* ГОСТ 28147–89. Єдиний алгоритм криптографічного перетворення даних для великих ІС. Не накладає обмежень на ступінь секретності інформації. Володіє перевагами алгоритму DES і у той же час позбавлений від його недоліків. Крім того, в стандарт закладений метод, який дозволяє зафіксувати невиявлене випадкове або навмисне модифікування зашифрованої інформації. Однак, загальним його недоліком є складність програмного реалізування.

3. *Метод з відкритим ключем* (RSA). Шифрування проводиться першим відкритим ключем, розшифрування – іншим, секретним ключем. Метод надзвичайно перспективний, оскільки не вимагає передавання ключа шифрування іншим користувачам. Фахівці вважають, що системи з відкритим ключем зручніше застосовувати для шифрування даних, які передаються, ніж при збереженні інформації. Існує ще одна галузь використання даного алгоритму – цифрові підписи, які підтверджують справжність документів та повідомлень, що передаються. Проте і він є недосконалим. Його недоліком є недостатньо вивчений алгоритм. Не існує строгого доведення його надійності математичними методами.

Потрібно мати на увазі, що ніякий окремо взятий організаційний захід або найпотужніший технічний засіб захисту не забезпечить достатнього рівня безпеки. Успіх справи залежить від комплексного застосування різних засобів і методів у створенні структури ЗІ з кількома рубежами і в постійному їх удосконаленні.

ЛЕКЦІЯ 3.

ЗАГАЛЬНІ ПРИНЦИПИ ЗАХИСТУ ІНФОРМАЦІЇ У БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

План

Вступ.
3.1. Особливості захисту інформації у банківських ІС
3.2. Захист інформації в електронних платіжних системах
3.3. Алгоритми шифрування в електронних картах

ВСТУП

В умовах широкого застосування сучасних інформаційних технологій, наявності засобів обміну інформацією розширюються можливості її витоку та несанкціонованого доступу до неї зі злочинною метою. Особливо уразливими сьогодні залишаються незахищені системи зв'язку, в тому числі КМ. Інформація, яка циркулює у них, може бути незаконно модифікована, викрадена або знищена.

За статистичними даними, в промислово розвинених країнах середні збитки від одного злочину в сфері інформаційних технологій становлять приблизно $ 450 тис., а щорічні сумарні втрати в США і Західній Європі сягають $ 100 млрд. і $ 35 млрд., відповідно. В останні десятиріччя зберігалася стійка тенденція до зростання збитків, пов'язаних із злочинністю в сфері ІТ.

3.1. Особливості захисту інформації у банківських інформаційних системах

Найбільшу небезпеку для банків представляє інформаційна незахищеність, тому при вирішенні даної проблеми банку необхідно враховувати те, що однією з головних умов стабільного функціонування кожного банку є обмін інформацією. Розглянемо питання інформаційної безпеки детальніше.

З метою протидії злочинам у сфері ІТ або зменшення збитків від них необхідно фахово вибирати заходи і засоби ЗІ від витоку та несанкціонованого доступу до неї.

Актуальність даної проблеми пов'язана із зростанням можливостей ІТ. Розвиток засобів, методів і форм автоматизації процесів оброблення інформації і масове застосування комп'ютерів роблять інформацію набагато більш уразливою. Основними чинниками, які сприяють підвищенню її уразливості, є:

- збільшення обсягів інформації, яка накопичується, зберігається та обробляється за допомогою комп'ютерів;
- зосередження в базах даних інформації різного призначення і різної приналежності;
- розширення кола користувачів, які мають безпосередній доступ до ресурсів ІС та масивів даних;
- ускладнення режимів роботи технічних засобів ІС;
- обмін інформацією в локальних та глобальних мережах, у тому числі на великих відстанях.

У всіх аспектах забезпечення ЗІ основним елементом є аналіз можливих дій щодо порушення роботи банківських ІС, тобто дій, що підвищують уразливість інформації, яка обробляється в ІС, призводять до її витоку, випадкового або навмисного модифікування, знищення.

Випадкові загрози включають у себе помилки персоналу, перебої у роботі технічних засобів та програмного забезпечення, а також події, які не залежать від людини, наприклад, природні явища або стихійні лиха. Заходи захисту від них – в основному організаційні.

До помилок апаратних та програмних засобів відносяться пошкодження комп'ютерів і периферійних пристроїв (магнітних, оптичних носіїв тощо), помилки в прикладних програмах. До помилок через неуважність, які досить часто виникають під час технологічного циклу оброблення, передавання або зберігання даних, відносяться помилки користувача, оператора або програміста, втручання під час виконання програм, пошкодження носіїв інформації.

Навмисні загрози можуть реалізуватися учасниками процесу оброблення інформації (внутрішні) і "хакерами" (зовнішні).

За частотою виявлення навмисні загрози можна розташувати в такому порядку:

- копіювання і крадіжка програмного забезпечення;
- несанкціоноване модифікування даних;
- зміна або знищення даних на довільних носіях;
- саботаж;
- крадіжка інформації;
- несанкціоноване використання ресурсів ІС;
- несанкціоноване використання банківських ІС;
- НСД до інформації високого рівня таємності.

Втручання у роботу банківської автоматизованої системи – довільні зловмисні дії, які впливають на оброблення інформації в ІС, тобто на всю сукупність операцій (зберігання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійнюються за допомогою технічних і програмних засобів, включаючи обмін через канали передавання даних.

Втручання у роботу ІС може бути і у формі впливу на канали передавання інформації як між технічними засобами її оброблення і зберігання всередині ІС, так і між окремими ІС, внаслідок чого інформація, яка передається, знищується або модифікується.

Знищення інформації – втрата інформації, внаслідок чого інформація в ІС перестає існувати для фізичних і юридичних осіб, які мають право власності на неї в повному або обмеженому обсязі. Як знищення, втрату інформації треба розглядати і її блокування, тобто припинення доступу до інформації користувачам ІС.

Модифікування інформації – зміна змісту, порушення цілісності, в тому числі і часткове знищення інформації.

Навмисні дії щодо порушення роботи ІС призводять до безпосереднього розкриття або зміни даних.

Особу, яка здійснює несанкціоновану дію з метою підвищення уразливості інформації, називаємо зловмисником. Дії зловмисника можна розділити на чотири основні категорії:

1. *Переривання* – припинення нормального оброблення інформації, наприклад, внаслідок руйнування обчислювальних засобів (рис. 3.1. б.) Відзначимо, що переривання може мати серйозні наслідки навіть у тому випадку, коли сама інформація ніяких впливів не зазнає.

2. *Крадіжка, розкриття* – читання або копіювання інформації з метою отримання даних, які можуть бути використані зловмисником або третьою стороною (рис. 3.1. в.).

3. *Модифікування* (зміна) інформації (рис. 3.1. г.).

4. *Руйнування* – безповоротна зміна інформації, наприклад, стирання даних з довільного носія) (рис. 3.1. д.).

Вибір засобів ЗІ в банківських ІС – складна задача, при розв'язанні якої потрібно враховувати різні можливі дії щодо порушення роботи такої системи, вартість реалізування різних засобів захисту і наявність численних зацікавлених сторін.

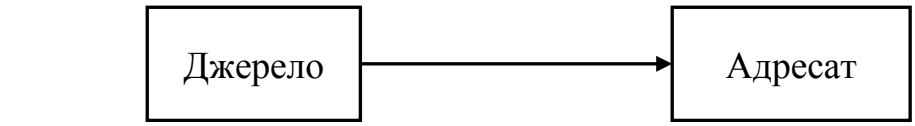
Одним із найважливіших видів інформації в банку є гроші в електронному вигляді, тому основою ЗІ в банківських ІС є захист електронного грошового обігу. Крім цього, інформація в банківських ІС становить значний інтерес для великої кількості людей та організацій – клієнтів банку. Ця інформація має обмежений доступ і банк несе відповідальність за забезпечення надійного рівня її захисту перед клієнтами та державою.

Банківські служби безпеки велику увагу приділяють питанням фізичного захисту. Питання інформаційної безпеки залишаються у компетенції служб супроводу і впровадження програмного забезпечення. Кваліфікованих розробників програмного забезпечення і системних програмістів у таких службах багато, але фахівців в області систем інформаційної безпеки практично немає.

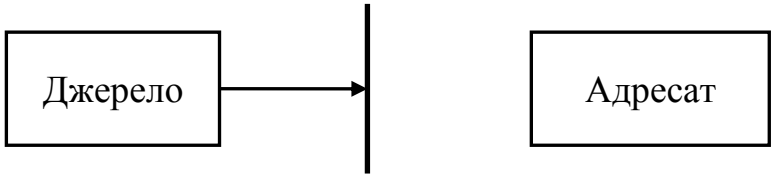
Рівень відповідності програмного забезпечення, яке розробляється, функціональним задачам банку можна оцінювати по різному. Однак, у всіх цих систем є загальний недолік – відсутня комплексна система захисту інформації, вони не сертифіковані на кваліфікаційні вимоги безпеки, а існуючі засоби і методи ЗІ в таких системах, як правило, зарубіжного виробництва або розроблені самостійно програмістами банку.

Розглянемо питання, пов'язані з наданням існуючими програмними системами послуг у області ЗІ. Відзначимо, що засоби розроблення програмного забезпечення є різноманітними: починаючи від C++, Clarion і закінчуючи потужними засобами проектування ІС – CASE-засобами, розподіленими базами даних і мережевими системами.

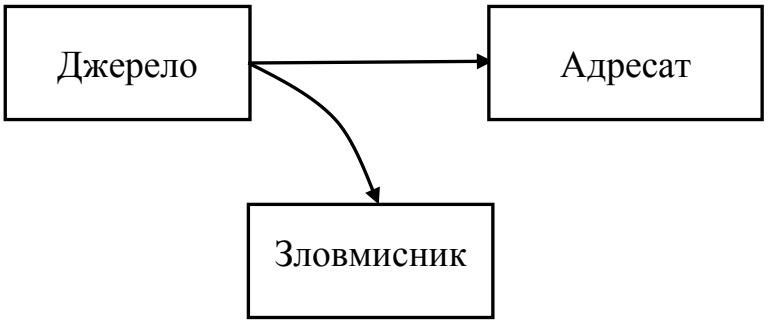
Розробники ретельно продумують інтерфейсні зв'язки всередині системи і спілкування з користувачем, опрацьовують алгоритми пришвидшеного пошуку в базах даних, структуру файлів. Отримана в результаті такого проектування система виконує добре продумані і чітко реалізовані функції, але дані зберігаються в форматах, які легко читаються довільним редактором текстів, або ж їх можна конвертувати в інші, поширеніші формати даних.



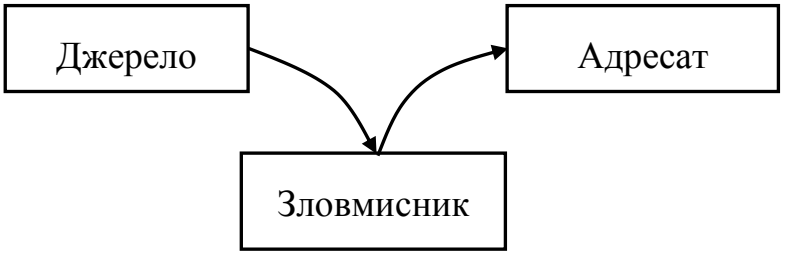
а)



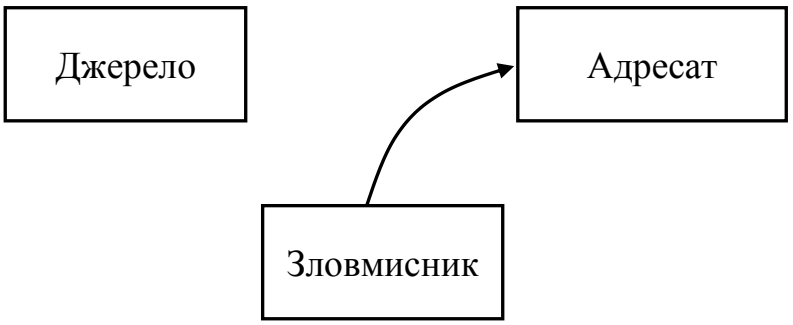
б)



в)



г)



д)

Рис. 3.1. Схеми механізмів порушення цілісності інформації зловмисником: а) нормальний обмін інформацією; б) переривання; в) крадіжка, розкриття; г) модифікування; д) фальсифікування

У цьому випадку в ІС забезпечений високий рівень надійності оброблення і зберігання, а також фізичної цілісності даних, але рівень безпеки інформації є надто низьким. При інсталюванні такого програмного продукту в банку потрібні серйозні заходи організаційного і технічного характеру для досягнення необхідного рівня захищеності інформації.

Як висновок, треба відзначити, що кваліфікований підхід до побудови системи ЗІ в банківських ІС має на увазі конкретну оцінку ймовірності виявлення кожної загрози у конкретній банківській системі.

Таким чином, кожному банку, в залежності від конкретних умов його роботи, потрібна персональна система ЗІ. Побудова такої системи можлива лише на аудиторських умовах спеціально залученими фахівцями і фірмами, які мають ліцензію на вказаний вид діяльності.

Розглянувши загальні принципи ЗІ в банківських ІС, доцільно відзначити, що комплексний ЗІ в банківських АС має в своїй основі використання фізичних, законодавчих, організаційних та програмно-технічних засобів захисту. Такі засоби повинні забезпечувати ідентифікування та автентифікування користувачів, розподіл повноважень доступу до системи, реєстрацію та облік спроб НСД. Організаційні заходи ЗІ в банківських ІС, як правило, спрямовані на чіткий розподіл відповідальності під час роботи персоналу з інформацією, створення декількох рубежів контролю, запобігання навмисному або випадковому знищенню та модифікуванню інформації.

3.2. Захист інформації у електронних платіжних системах

За останні тридцять років людська цивілізація зазнала значних змін. Цей феномен переходу від постіндустріального до інформаційного суспільства торкнувся всіх галузей науки, техніки, та інших сфер діяльності.

Зрозуміло, що такий стан речей має вплив і на найдавнішу з комерційних галузей – торгівлю. По-перше високі часові вимоги вимагають укладати угоди за дуже короткий термін. Комунікаційні засоби розширюють ринки збуту для продавців, збільшують пропозицію для покупців та пришвидшують обіг коштів. По-друге в інформаційному суспільстві виник новий вид товару – інформація.

Треба відзначити, що електронні засоби не змінюють сутності комерційної угоди її основних атрибутів, вони лише додають нові можливості. Ці можливості можна використовувати як за усталеними правилами, так і всупереч таким правилам. Тобто, електронне середовище відкриває як нові можливості для торгівлі, так і нові можливості для різних зловживань.

Історія розвитку засобів електронної комерції фактично є історією пізнання простої істини – із зростанням потужності обчислювальних засобів зростали можливості зловмисників, що, в свою чергу, вимагало побудови систем захисту від зловживань.

Виходом з цієї ситуації є використання системи електронної комерції з інтегрованою підсистемою захисту. Політика безпеки має бути однією з основних складових частин системи починаючи ще з етапу проектування.

Гостро стоїть проблема аутентифікування суб’єктів комерційних відносин. На сьогодні не існує єдиного стандарту на способи побудови систем електронної комерції. Під час проектування таких систем авторами закладається ненадійна система безпеки, часто через недостатньо надійне аутентифікування сторін. Відсутність систем сертифікування ключів (а це є загальновизнаним надійним методом аутентифікування) відкриває простір для численних зловживань

(наприклад, відкриття фіктивних електронних магазинів, які ″продають повітря″).

У цивілізованому світі існує кілька систем розповсюдження сертифікатів відкритих ключів засобами електронних криптосистем, наприклад, VeriSign – але використання таких систем є надто дорогим і практично недоступне для організацій України. Очевидно, що в Україні є актуальною потреба створення аналогічних систем.

3.2.1. Огляд та аналіз існуючих засобів систем електронної комерції

Переважна більшість систем електронної комерції, які забезпечують достатній рівень захищеності користувачів, є закритими системами. Це, по-перше, наражає користувачів на ризик атаки з боку власника або оператора такої системи (з використанням ″люків″ або інших засобів зниження стійкості захисту користувача в системі, які відомі тільки власникам або розробникам системи). По-друге – це фактично унеможливлює створення аналогічної системи з використанням чужого досвіду побудови.

Для створення системи, в якій достеменно не буде різних ″запасних виходів″ та будь-яких інших способів обходу засобів безпеки, треба повністю спроектувати та відтворити цю систему. При цьому, починаючи від етапу проектування, враховувати інтегровані підсистеми захисту.

Крім технічних аспектів існують також правові. Однак, треба наголосити, що відсутність законів України, які регулювали б проблеми, що пов'язані з електронними документами, відповідальністю за шахрайства в цій галузі діяльності, значно ускладнюють ситуацію з розвитком новітніх технологій, у тому числі електронної комерції.

Серед існуючих систем електронної комерції можна виділити такі основні групи:

- замовлення товару через мережу Internet з оплатою ″класичними″ засобами;
- купівля товару через мережу Internet з оплатою за допомогою існуючих платіжних систем (платіжні картки, у тому числі мікропроцесорні, home banking тощо);
- купівля товару через мережу Internet з оплатою за допомогою власних платіжних систем.

Перший метод фактично не реалізовує систему електронної комерції у повному обсязі – адже така система має надавати можливість укласти та виконати угоду лише своїми засобами (тут вважаємо, що платіжна система входить як складова частина до системи електронної комерції).

Останній з перелічених методів не дає такої гнучкості, яку надає система з використанням різних існуючих платіжних засобів. Але саме такі системи на сьогодні є найрозповсюдженішими у світі і в Україні. Треба наголосити, що велику кількість таких систем було створено без урахування суворих вимог до захищеності та безпеки – наприклад, багато систем використовують аутентифікування з використанням пароля, що є цілком неприпустимим у системі з ризиками фінансових втрат.

Таким чином ці системи є потенційно небезпечними для участі у них як з боку продавця, так і з боку покупця.

Оператором системи може бути довільна організація, яка займатиметься підтримкою діяльності системи. Ця організація повинна стежити за цілісністю ієрархії розповсюдження сертифікатів відкритих ключів, підтримувати всі сервіси роботи із сертифікатами. Також необхідно постійно дотримуватись вимог забезпечення безпеки системи та провадити заходи з дотримання політики безпеки всіма учасниками системи.

Система має забезпечувати захищеність кожного учасника:

- покупець має бути впевненим, що продавець є дійсно продавцем і в змозі виконати свою частину угоди – доставити товари, надати послуги тощо;
- продавець має бути впевненим в тому, що покупець є здатним на оплату наданих товарів або послуг.

Таку впевненість може надати суворе аутентифікування сторін – тоді продавець буде впевненим, що покупець платить із свого гаманця, а не з вкраденої кредитної картки, яку от-от заблокують, при цьому покупець може бути впевненим в тому, що він має справу з магазином, який пройшов реєстрацію та отримав відповідні дозволи у держави або уповноважених органів.

Система має реалізовувати політику безпеки, яка базується на *моделі взаємної недовіри*. Це водночас забезпечує безпеку кожного з учасників системи і чітко розмежовує відповідальність за можливі втрати внаслідок порушення політики безпеки.

3.2.2. Аналіз способів захисту мікропроцесорних карт

Основне призначення електронної комерції – надати можливість покупцям вибирати, оформляти замовлення і здійснювати покупки товарів та отримувати послуги в будь-який час за допомогою мереж загального користування, в тому числі мережі Internet.

Потрібно сформувати велику розгалужену систему, яка дозволила б створити електронний магазин навіть небагатій організації та забезпечити статус покупця будь-кому, хто має доступ до мережі Internet.

На шляху реалізування такої системи постає багато проблем.

Перша проблема – це мільйони користувачів. Отже, систему потрібно реалізувати за допомогою ієрархічної архітектури, що дозволить створити кілька центрів з підтримки системи з кількістю клієнтів у десятки, сотні тисяч – це реальні показники для сучасних ІС середнього рівня. Також це дозволить легко масштабувати систему – адже можна буде не лише додавати кінцевих користувачів, а й нові вузли довільного рівня. Це забезпечиить використання деревоподібної моделі розповсюдження сертифікатів, яка є надійнішою.

Друга проблема – просте інтегрування нової системи в існуючу мережу Internet та пов’язаних з цим сервісів. Так, нова система має доповнювати службу WWW, за допомогою якої зараз створено мільйони сайтів.

Таким чином, продавці мають можливість використовувати усі створені дотепер засоби візуального подання інформації в мережі Internet (в рамках протоколу http), а механізми електронної комерції будуть лише доповненнями.

Третя проблема – це джерело довіри в системі. Деревоподібна структура системи забезпечить використання ієрархічної моделі розповсюдження довіри, але потрібно обрати корінь такої ієрархії. Логічно було б функції джерела довіри покласти на державну установу.

3.2.3. Система безпеки мікропроцесорних карт

Електронні карти появилися у повсякденному житті в 70-х роках XX ст. Вже у 1970 р. японський винахідник Арімура запатентував пластикову карту, яка містила одну або декілька електронних схем для генерування необхідних сигналів.

Переломним моментом у галузі електронних карт можна вважати 1974 р., коли Морено запатентував незалежний електронний об'єкт з ″пам'яттю″. Однак, у 1976 р. Булл у співпраці з фірмою Motorolla розробив першу карту без мікропроцесора. У 1978 р. появилася перша карта з вмонтованим мікропроцесором. Лише в 1985 р. фірмі Philips вперше вдалося імплементувати в своїх картах симетричний алгоритм DES, а шість років пізніше – асиметричний алгоритм RSA завдяки введенню до карти копроцесора, який пришвидшував виконання арифметичних операцій, CORSAIR (Computing RSA In Rush).

У 1995 р. фірма Philips випустила карту з копроцесором FAME (The Fast Akcelerator for Modular Exponentiation). Завдяки цьому процесору появилась можливість виконання складних обчислень з метою збільшення рівня безпеки. Модернізацією процесора FAME був копроцесор FAMEX (The Fast Accelerator for Modular Exponentiation eXtended), який є ще більш швидкодіючим і дозволяє виконувати криптографічні операції з більшими ключами. У табл. 3.1 подано час операцій генерування і верифікації підпису з використанням копроцесора FAMEX.

Таблиця 3.1

Час виконання операції генерування та верифікації підпису з використанням копроцесора FAMEX

Довжина ключа RSA	Час генерування підпису, мс	Час верифікації підпису, мс
512 bit	< 40	< 95
1024 bit	< 160	< 400
2048 bit	< 1100	< 6400 m

Електронна і магнітна карти. Електронні та магнітні карти можуть лише зберігати дані. Різниця між ними полягає в тому, що пам'ять в електронних картах може використовуватися до моменту введення нових даних на місце існуючих, в той час як магнітні базуються на технології однократного запису і багатократного зчитування.

Мікропроцесорні карти. Мікропроцесорні карти або так звані інтелігентні (Smart Cards) – це карти, які крім пам'яті мають вмонтовані процесори. Їх можна порівняти з малими переносними комп'ютерами, які живляться від зчитувачів і не мають таких пристроїв як дисплей, клавіатура або ″мишка″.

До характерних ознак цих карт належать:

- різноманітне застосування – одна карта може використовуватися для багатьох послуг, які можуть бути між собою пов’язані або незалежні;
- безпека даних – доступ до них контролюється процесором і може бути наданий при виконанні певних умов.

На сьогодні в мікропроцесорах використовується 8-ми та 16-ти бітова пам’ять EEPROM обсягом 64 Кб. Мікропроцесор контролює зчитування і запис даних, що розміщені в пам’яті, а користувач для отримання доступу до них повинен подати відповідний ключ доступу – PIN. Мікропроцесор може також контролювати кількість невдалих спроб доступу і після перевищення встановленого ліміту спроб доступу повністю блокувати доступ до даних. Завдяки мікропроцесору можна керувати і поділяти пам’ять, а це робить карту багатофункціональною для різноманітних напрямків застосуваня.

Мікропроцесорні карти повинні містити постійну пам’ять ROM, в якій записана необхідна для функціонування процесора операційна система. Пам’ять в картах цього типу поділяється на три зони:

- вільного зчитування – тут записана інформація один раз під час виготовлення карти (інформація про власника карти: ім'я, прізвище, термін дії карти, її номер);
- конфіденційна – розміщені там дані записані тільки раз і не змінюються протягом терміну використання карти, а доступ до цих даних можливий лише після введення відповідного ключа;
- робоча – переховувані там дані можна змінювати протягом усього терміну використання карти.

Існує дуже багато типів електронних карт. Однак їх можна згрупувати за спільними характеристиками. Електронні карти класифікуються з урахуванням способу захисту від несанкціонованого доступу (НСД).

Спосіб захисту даних від НСД залежить від ″інтелігентності″ електронної карти. Власне за цією ознакою карти поділяють на три групи.

1. *Звичайні карти* (Dumb Cards).

Ці карти володіють пам’яттю, функцією запису і зчитування, але не мають жодних функцій контролю доступу. Комунікація із зовнішніми пристроями є загалом синхронна. Сучасніші моделі цих карт містять пам’ять EEPROM обсягом від 256 байтів до кілька десятків кілобайтів.

2. *Карти з вмонтованою логікою* (Wired Logic Cards).

У цих картах міститься елемент контролю доступу з наперед запрограмованими функціями. У залежності від способу реалізування доступу з цієї групи можна виокремити кілька типів карт. Пам’ять EEPROM поділяється за адресами на кілька зон. Зчитування є можливим у кожній зоні, однак в призначеній лише для зчитування області не можна здійснити запису. Карти цього типу використовуються в публічному телефонному зв’язку або для ідентифікування.

3. *Інтелігентні карти* (Smart Cards).

Карти з цієї групи містять мікропроцесор, що відкрило нові можливості для керування розміщеною в картах пам’яттю. У пам’яті можуть бути записані як дані, так і виконувана програма. Значною перевагою є те, що мікропроцесор дозволяє асинхронну комунікацію зі зчитувачем, що зумовлює збільшення рівня

безпеки системи. З точки зору комунікацій із засобами зчитувачів карти можна поділити на дві групи:

1. *Контактні карти*.

Карти цього типу є найбільш розповсюджені і популярні. Зчитувач має нескладну механічну будову (рис. 3.2).

Карти, як і зчитувач, повинні мати очищені контакти, а карта повинна бути точно розміщена у зчитувачі. Таке з'єднання забезпечує трансмісію даних до подальших пристроїв системи, а також передає живлення до електронної схеми, вмонтованої в карту. Карти цього типу використовуються тоді, коли операції повинні бути здійснені досить швидко. Розмір цих карт не відрізняється від стандартних, єдина відмінність полягає в товщині карти, яка знаходиться в межах від 0,76 мм (кредитна карта) до 3 мм.

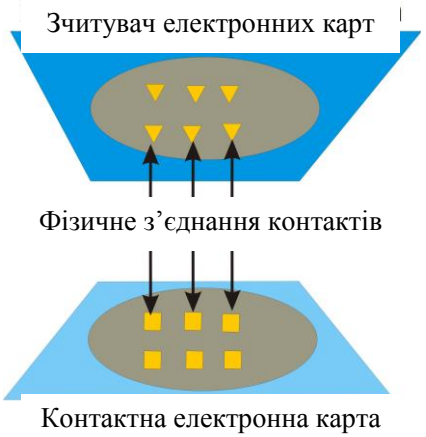


Рис. 3.2. Спрощена схема ″контактна електронна карта – зчитувач″

Трансмісія даних і живлення здійснюється за допомогою комунікаційних засобів, вмонтованих у карту (рис. 3.3).

Основні переваги застосування безконтактних електронних карт:

- великий термін дії та складність підробки;
- незначні експлуатаційні витрати;
- зручний спосіб користування;
- стійкість зчитувачів до пошкоджень;
- значна швидкість трансмісії даних (до 100 Кб/с);
- короткий час здійснення довільної операції (ідентифікування, зчитування, запис).

2. *Безконтактні карти*.

Способи живлення карт поділяються на дві групи, а саме – на активні карти, які для живлення використовують вмонтовану батарею, та пасивні карти, які отримують енергію живлення від зовнішніх пристроїв через зовнішнє електромагнітне поле. Щодо активних карт, то батареї повинні періодично замінюватися і вони є чутливішими до змін атмосферних умов, ніж контактні карти. Недоліком пасивних карт є обмежений діапазон дії щодо живлення. Перевагою активних карт є більший термін експлуатації.

Діапазон охоплення. Діапазон дії карти є надзвичайно важливим, оскільки визначає умови роботи всієї системи. Існує багато карт, які повинні бути розміщені досить близько від зчитувача, навіть на відстані кілька міліметрів.

Однак є карти, діапазон дії яких є значно більший, зокрема декілька сантиметрів, декілька десятків сантиметрів (так званий середній діапазон) або навіть більше одного метра (довгий та ультрадовгий діапазони). Карти з великим діапазоном вимагають застосування батареї. Комунікація зі зчитувачем відбувається за допомогою радіохвиль. Карти з коротким діапазоном живляться за допомогою енергії радіохвиль, які випромінюються радіозчитувачем.

Запис і зчитування. Карти за цією ознакою поділяються на дві групи:

- тільки для зчитування (Read Only), які використовуються для віддаленого ідентифікування людей, тварин або предметів;
- для зчитування і запису, які мають застосування, подібне до контактних карт.

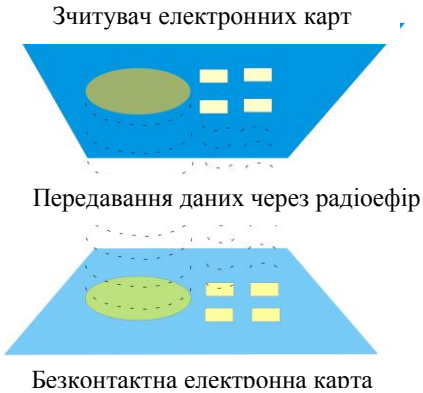


Рис. 3.3. Спрощена схема ″безконтактна електронна карта – зчитувач″

Робоча частота. Карти можуть працювати на низьких, середніх та високих частотах. Вибір частоти залежить від призначення карти. Низькі частоти використовуються для роботи на малих відстанях і коли не вимагається швидка трансмісія даних.

Використовувані на сьогодні карти в системах радіоідентифікування функціонують на трьох частотах: низькій (125 КГц); середній (13,56 МГц); високій (2,45 ГГц).

Застосування електронних карт. Електронні карти мають широке застосування в повсякденному житті. Нижче подані основні напрями та установи, де використовуються електронні карти:

- транспортна комунікація (безконтактні карти для оплати за проїзд міським транспортом та автострадою);
- моторизація (системи аутентифікування автомобілів, їх захисту – Car Immobilizer використовується зараз як стандартна опція в багатьох моделях автомобілів);
- банківська система (кредитні карти, Internet карти, які виконують функції безготівкових трансакцій);
- мережі мобільного зв’язку (карти SIM, малі за розміром карти, на яких може бути записано багато інформації, при цьому існує можливість запису та усування з них даних);
- комерційні станції TV (системи декодування сателітного сигналу);

- охорона здоров’я (системи ідентифікування пацієнта, запис набутих хвороб);
- електронний підпис;
- автентифікування (входи до установ, фірм, цивільних установ, ідентифікування в ІС);
- освіта (у системах ідентифікування студентів, у бібліотечній системі).

Будова електронних карт. У електронних картах використовуються три основні архітектури в залежності від того, чи це карти з пам’яттю, процесорні або безконтактні. Будова і архітектура карт цих типів наступна:

1. *Карти з пам’яттю*. Ця карта (рис. 3.4) містить лише модулі пам’яті:

- ROM (Read Only Memory), яка записується під час виготовлення карти і служить тільки для зчитування;
- EEPROM (Erectlically Erasable Programmable Read Only Memory), яка надається до багатократного електричного усування та запису даних.

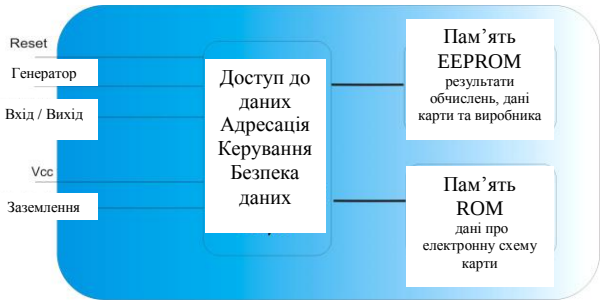


Рис. 3.4. Блок-схема карти з пам’яттю

Беручи до уваги простоту виготовлення, карти з пам’яттю і надалі є найчастіше використовувані. Наявність модуля безпеки і блоку автентифікування забезпечується захист виконання операцій.

Надаваний при кожній операції ідентифікаційний код (PIN) обмежує доступ до даних, які містяться в пам’яті EEPROM, а після декількаразового (найчастіше триразового) помилкового введення – блокує доступ до неї. Верифікація автентичності відбувається за допомогою методу "Challenge-response", який полягає у підтвердженні відгуку карти на імовірнісний виклик.

2. *Процесорні карти*. Ці карти (рис. 3.5) крім модулів пам’яті містять також процесор, операційну систему, ряд допоміжних модулів та контакти, які є вмонтованим модулем для комунікацій зі зчитувачами. Використовуються три типи модулів пам’яті: RAM, ROM, і EEPROM. Операційна система SCOS (Smart Card Operating System) зберігається в пам’яті ROM, оскільки це найбезпечніший спосіб захисту від її модифікування.

Процесор керує виконанням задач операційної системи та заімплементованими завданнями. До трьох головних додаткових модулів належать модулі обнулення, синхронізації та комунікації. Карта може бути також доповнена модулями захисту перед її електричним знищенням.

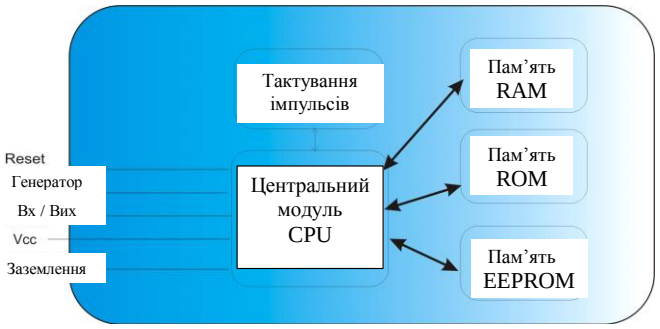


Рис. 3.5. Блок-схема мікропроцесорної карти

3. *Безконтактні карти*.

Безпровідні карти своєю будовою докорінно відрізняються від традиційних контактних карт. Для комунікації зі зчитувачами використовуються не контакти, а радіопристрої, причому дані пересилаються радіоефіром.

Крім згаданих вище модулів будова безконтактних карт є надзвичайно схожою до будови процесорних карт (оскільки це є власне процесорна карта, а єдина відмінність полягає у згаданому способі комунікації).

3.3. Алгоритми шифрування в електронних картах

Алгоритми шифрування, які використовуються в електронних картах, можна поділити на дві основні групи за типом використаного криптографічного алгоритму. Найпопулярніші серед них подані нижче.

Симетричне шифрування: алгоритм DES; алгоритм 3DES; алгоритм IDEA; алгоритм RC5; алгоритм AES.

Асиметричне шифрування: RSA; ECC; DSS.

Алгоритм шифрування у безконтактних картах. Найрозповсюдженішими безконтактними картами є карти, які виготовляються фірмою Philips, яка розробила два стандарти для своїх карт: MIFARE та HITAG. Найчастіше використовуються карти MIFARE з огляду на їх більшу швидкодію при трансмісії даних та підвищену безпеку.

Для шифрування даних використовується ряд алгоритмів.

Алгоритм DES – один з перших алгоритмів, який використовується в електронних картах. Уперше його використала фірма Philips в електронних картах у 1985 р. На сьогодні його застосовують у модифікованій версії алгоритмів, тому слід детальніше висвітлити принцип його функціонування.

Шифрування полягає у початковій перестановці бітів 64-х бітового блоку в 16-ти циклах шифрування і кінцевій перестановці. Для опису алгоритму DES використані такі позначення:

L і R – послідовність бітів (ліва і права);

LR – конкатенація послідовностей L і R, тобто така послідовність бітів, довжина якої дорівнює сумі довжин L і R;

$\oplus$ – функція за модулем 2 на 48-ми бітовому векторі даних;

A – вхідний блок.

Принцип функціонування алгоритму DES. З явного вхідного текстового файлу зчитується 64-ох бітовий блок A. Першим кроком є перестановка цих бітів згідно з таблицею початкової перестановки IP. Ці перестановки можна записати

як A_0=IP(A). Отриману послідовність бітів A_0 поділяють на дві однакові послідовності: L_0 – ліві біти; R_0 – праві біти.

Наступним етапом є здійснення ітераційного процесу шифрування. Допустимо, A_i – результат i-ої ітерації:

$$A_i = L_iR_i, \tag{3.1}$$

$$L_i = R_{i-1},\ i = 1, 2, ..., 16, \tag{3.2}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i),\ i = 1, 2, ..., 16, \tag{3.3}$$

де: $f(R_{i-1}, k_i)$ – функція шифрування.

У останньому 16-му циклі отримуємо послідовності R_{16} та L_{16}.

Алгоритм шифрування завжди закінчується відновленням позиції бітів за допомогою оберненої матриці перестановок IP^{-1}. Це необхідно для того, аби використовувати цей самий алгоритм як для шифрування, так і для дешифрування. Схема шифрування алгоритму подана на рис. 3.6.

Алгоритм обчислення функції f. Для обчислення функції f використовуються: функція розширення E, тобто розширення від 32 бітів до 48 бітів; функція підстановок S_j, j = 1, 2,…, 8, тобто перетворення 6-ти бітового числа у 4-ох бітове; функція перестановок P, тобто перестановка бітів у 32-ти бітовій послідовності.

Алгоритм створення ключа. У кожній ітерації використовується інший новий ключ K_i довжиною 48 бітів. Ключ K_i обчислюється на підставі ключа шифрування K. Ключ K є 64-ох бітовим блоком з 8-ми бітами контролю парності, які розміщені на позиціях 8, 16, 24, 32, 40, 48, 56, 64.

Алгоритм 3DES. Цей алгоритм є своєрідною модифікацією алгоритму DES. Відмінність між ними полягає в тому, що повідомлення шифруються три рази алгоритмом DES: зашифровується першим ключем; розшифровується другим ключем; зашифровується третім ключем, зокрема,

$$c = E_3(D_2(E_1(m))). \tag{3.4}$$

Дешифрування в другій фазі не впливає на суму алгоритму, але дозволяє застосувати алгоритм 3DES у режимі компатибільності з алгоритмом DES – ключем першим і другим або другим і третім приймаємо такий самий ключ, а останнім – звичайний ключ, як в алгоритмі DES:

$$c = E_3(D_1(E_1(m))) = E_3(m), \tag{3.5}$$

$$c = E_3(D_3(E_1(m))) = E_1(m). \tag{3.6}$$

Алгоритм 3DES використовує режими роботи та блоки такої самої довжини, як алгоритм DES.

Алгоритм RSA. В цьому алгоритмі випадково Генерується досить велике число – ключ явний, який використовується для обчислення іншого великого числа – приватного ключа за допомогою достатньо складних маремати чних функцій. Користувачі застосовують ці ключі для шифрування документів, які висилаються до них двома і більше особами, та для розшифрування документів після їх отримання.

Схема шифрування/дешифрування алгоритму RSA подана на рис 3.7.

Сам алгоритм можна подати наступним чином:

- вибираються два великі прості числа p, q;
- перемножуємо їх n=p×q;
- обчислюємо φ(n)=(p–1)(q–1);
- вибирають випадкове число 1<e<φ(n), яке є простим відносно φ(n);
- використовуємо ключі: явний (публічний) і приватний.

З метою безпечного шифрування та дешифрування слід виконати такі вимоги:

- числа p і q повинні мати по ~100 цифр;
- числа p і q не можуть бути дуже близькими одне від другого.

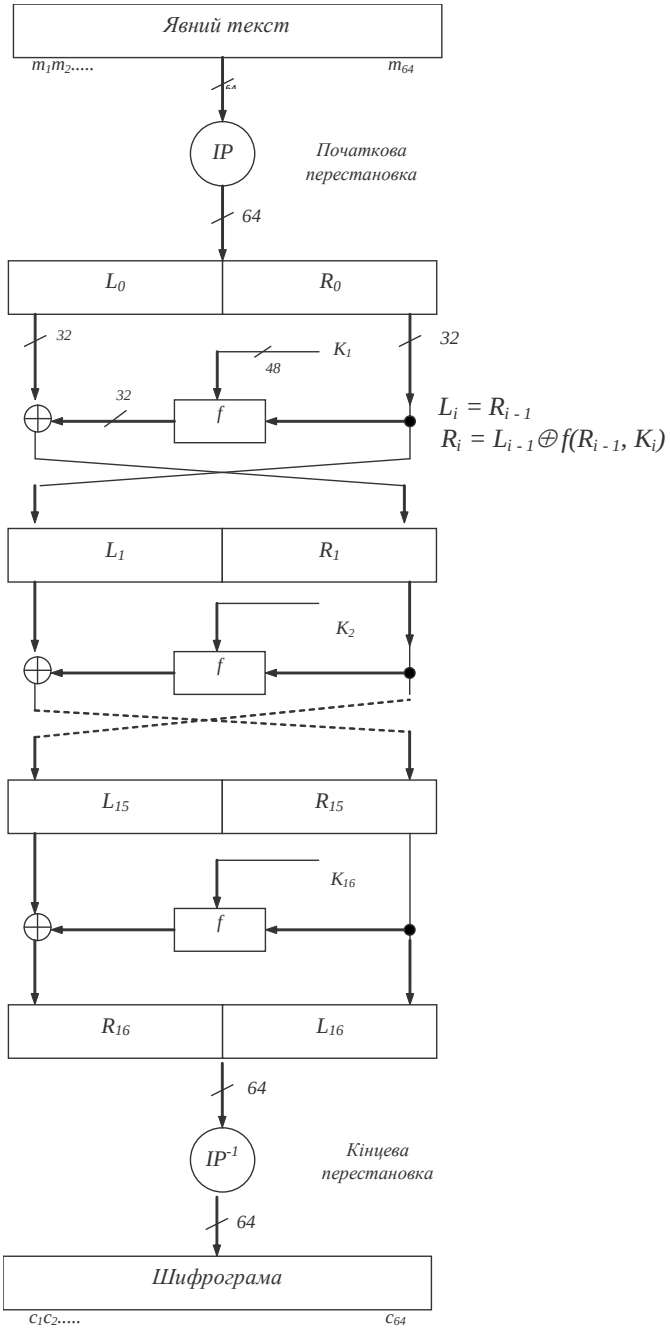


Рис. 3.6. Схема шифрування алгоритму DES

Алгоритм DSS. Алгоритм DSS – це поточна назва, але якщо йде мова про особливості, то це стандарт цифрових підписів. Ґрунтується він на методі верифікації особи, яка висилає інформацію, та інтегральності переданих даних. Стандарт базується на двох алгоритмах:

- алгоритм Діффі-Хелмана, який призначений лише для узгодження приватного ключа між особами, які надають і отримують інформацію, але не може бути використаний для безпосереднього шифрування даних. Цей алгоритм полягає в обчисленні дискретної експоненційної функції і дискретного логарифму;
- алгоритм SHA – це алгоритм безпечного хешування, яке в криптографії має два значення: змішувати і стискувати. У першому значенні вживається для безпечного шифрування текстів (наприклад, в алгоритмі RSA), а в другому – для отримання на підставі тексту певного унікального числа, яке використовується для створення цифрового підпису. Найчастіше використовується така версія, яка характеризується тим, що здійснення операцій в одну сторону є простим, а в іншу – надзвичайно складним. Мова тоді йде про односпрямовану функцію хешування, а відповідний алгоритм має назву SHA-1.

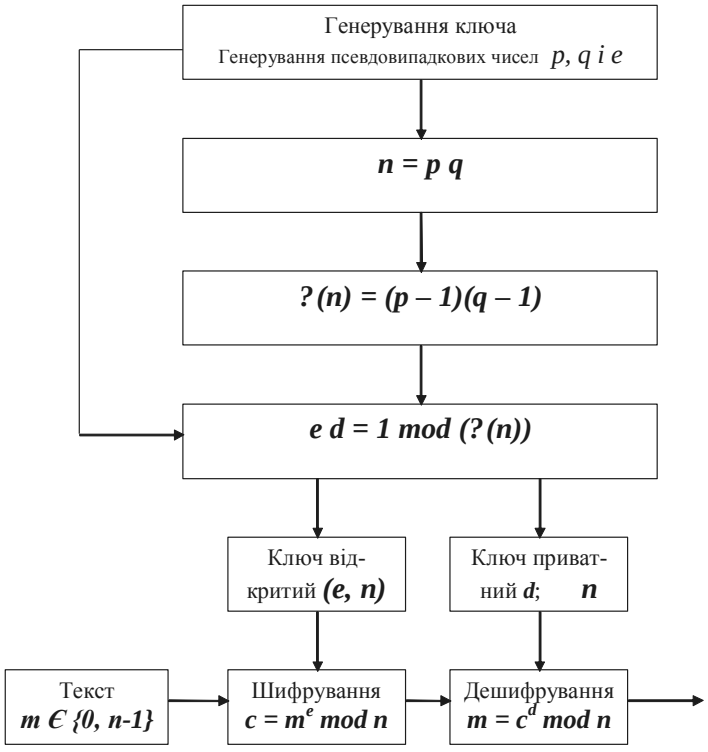


Рис. 3.7. Схема шифрування/дешифрування алгоритму RSA

Алгоритм ECC. Алгоритм ECC (Elliptic Curve Cryptography) базується на еліптичних кривих. Останні дозволяють використовувати менші ключі, що є дуже важливим у банківській справі з огляду на процесори карт.

Беручи до уваги високу швидкодію алгоритму ECC при шифруванні і згадані невеликі ключі, його часто застосовують у безпровідній комунікації, а отже – у безконтактних картах. Для унаочнення переваг цього алгоритму можна сказати, що ключ двійковою довжиною від 150 до 350 знаків, забезпечує таку

саму криптографічну стійкість, як ключ від 600 до 1400 і більше знаків в інших криптографічних системах.

Розглянемо загальні поняття еліптичних кривих. Загальне рівняння еліптичної кривої можна подати у вигляді

$$y^2 = x^3 + ax + b. \tag{3.7}$$

З точки зору криптографії маємо нову криптологічну систему на підставі еліптичних кривих.

Додавання точок P і Q (рис. 3.8):

1. P+0=0+P=P для всіх P ε E (E – еліптична крива);
2. Якщо P=(x, y) ε E, тоді P+(–P)=0 , де – P=(x, –y);
3. Допустимо, $P=(x_1, y_1)$, $Q=(x_2, y_2)$ ε E де – P≠–Q. Тоді $P+Q=(x_3, y_3)$, причому $x_3=\lambda_2 - x_1 - x_2 \pmod p$, $y_3=\lambda (x_1 - x_3) - y_1 \pmod p$,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p \text{ якщо } P \neq Q, \tag{3.8}$$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \pmod p \text{ якщо } P = Q. \tag{3.9}$$

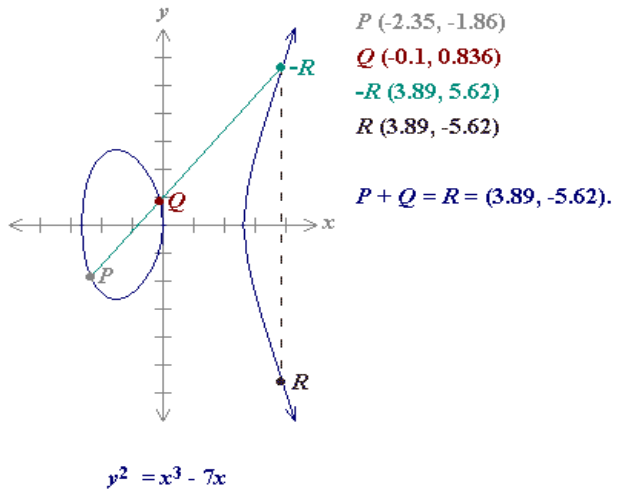


Рис. 3.8. Додавання точок P і Q на еліптичній кривій

Вимоги до алгоритмів. Крім очевидних вимог, таких як неможливість розшифрування доступними засобами, обчислювальна складність алгоритму повинна бути такою, щоб поміститися в пам’яті карти. При цьому вмонтований процесор повинен здійснити обчислення за короткий проміжок часу.

Декілька обмежень, які накладаються на алгоритми, розроблювані для використаня в електронних картах: засоби пам’яті (RAM – 0,5 … 1 Кб; ROM – 50 Кб); швидкість передавання даних; список розпоряджень процесора і копроцесора; можливість генерування ключа приватного і явного (так звана імплементація тестів сильних чисел).

Стосовно вимог безпеки можна використати приклад обчислень для алгоритму RSA. Приймаючи ключ 1024-бітовий, отримуємо, що для зламання шифру потрібні сотні тисяч років навіть для сучасних суперпродуктивних комп’ютерів.

ЛЕКЦІЯ 4.

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

План

Вступ.

4.1. Визначення і аналіз загроз на об'єктах інформаційної діяльності підприємства

4.2. Технічний захист інформації на об'єктах інформаційної діяльності державних підприємств України

4.3. Організаційно-правові принципи захисту ІС на основі міжнародних стандартів

ВСТУП

Об'єктом технічного захисту є інформація, яка становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, яка є державною власністю або передана державі у володіння, користування, розпорядження.

4.1. Визначення і аналіз загроз на об'єктах інформаційної діяльності підприємства

Технічний захист інформації здійснюється поетапно: перший етап – визначення і аналіз загроз; другий етап – розроблення системи ЗІ; третій етап – реалізування плану ЗІ; четвертий етап – контроль за функціонуванням та керуванням системою ЗІ.

На першому етапі здійснюється ґрунтовний аналіз об'єктів ТЗІ, ситуаційного плану, умов функціонування підприємства, оцінювання ймовірності прояву загроз та очікуваних збитків від їх реалізування, підготування даних для формування виокремленої моделі загроз.

Джерелами загроз може бути діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб. Опис загроз і схематичне подання шляхів їх здійснення формують модель загроз.

Загрози можуть здійснюватися: технічними каналами побічних електромагнітних випромінювань і наведень (ПЕМВН), акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали; каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації; НСД шляхом під'єднання до апаратури та ліній зв'язку, маскуванням під зареєстрованого користувача, подоланням заходів захисту для використання інформації або нав'язуванням хибної інформації, застосуванням закладних пристроїв або програм та вкоріненням комп'ютерних вірусів.

4.1.1. Розроблення плану захисту інформації

На другому етапі ТЗІ розробляється план, який містить організаційні, первинні технічні та основні технічні заходи захисту інформації з обмеженим доступом, визначити зони безпеки інформації.

Організаційні заходи регламентують порядок інформаційної діяльності (ІД) з урахуванням норм і вимог ТЗІ для всіх періодів життєвого циклу ІД.

Первинні технічні заходи передбачають ЗІ блокуванням загроз без використання засобів ТЗІ.

Основні технічні заходи передбачають ЗІ з використанням засобів забезпечення ТЗІ.

Заходи захисту інформації повинні: бути адекватними до загроз; бути розробленими з урахуванням можливих збитків від реалізування загроз і вартості захисних заходів та обмежень, які вносяться ними; забезпечувати задану ефективність ЗІ на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

Рівень ЗІ означується системою кількісних та якісних показників, які забезпечують вирішення завдання ЗІ на основі норм та вимог ТЗІ. Мінімально необхідний рівень ЗІ забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі. Порядок розрахунку та інструментального визначення зон безпеки, реалізування заходів ТЗІ, розрахунку ефективності захисту та порядок атестування технічних засобів забезпечення ІД, робочих місць (приміщень) встановлюються нормативними документами системи ТЗІ.

4.1.2. Реалізування плану захисту інформації

На третьому етапі ТЗІ слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту ІзОД, установити необхідні зони безпеки інформації, провести атестування технічних засобів забезпечення ІД, технічних засобів ЗІ, робочих місць (приміщень) на відповідність вимогам безпеки інформації.

ТЗІ передбачає застосування захищених програм і технічних засобів забезпечення ІД, програмних і технічних засобів ЗІ та контролю ефективності захисту, які мають сертифікат відповідності вимогам нормативних документів або дозвіл на їх використання від уповноваженого Кабінетом Міністрів України органу, а також застосуванням спеціальних інженерно-технічних споруд, засобів і систем.

Засоби ТЗІ можуть функціонувати автономно або сумісно з технічними засобами забезпечення ІД у вигляді окремих пристроїв або вмонтованих у них складових елементів. Склад засобів ТЗІ, перелік їх постачальників, а також послуг з інсталювання, налаштування та обслуговування визначаються особами, які володіють, користуються і розпоряджаються ІзОД самостійно або за рекомендаціями фахівців з ТЗІ згідно з нормативними документами системи ТЗІ.

Надання послуг з ТЗІ, атестування та сервісне обслуговування засобів ТЗІ можуть здійснювати юридичні і фізичні особи, які мають ліцензію на право проведення цих робіт.

4.1.3. Організація проведення обстеження об’єктів інформаційної діяльності підприємства

Метою обстеження об’єктів ІД підприємства є вивчення його ІД, визначення об`єктів захисту – ІзОД, виявлення загроз, їхній аналіз та формування окремої моделі загроз.

Обстеження повинно бути проведено комісією, склад якої визначається відповідальною за ТЗІ особою і затверджується наказом керівника підприємства.

У ході обстеження необхідно:

- провести аналіз умов функціонування об’єктів інформаційної діяльності (ОІД) підприємства, їх розташування на місцевості (ситуаційного плану) для визначення можливих джерел загроз;
- дослідити засоби забезпечення ІД, радіус дії яких виходить за межі контрольованої території;
- передбачити вивчення схем засобів і систем життєзабезпечення ОІД (електроживлення, заземлення, автоматизації, пожежної та охоронної сигналізації), а також інженерних комунікацій та металоконструкцій;
- дослідити інформаційні потоки, технологічні процеси передавання, одержання, використання, розповсюдження і зберігання інформації та провести необхідні вимірювання;
- визначити наявність та технічний стан засобів ТЗІ;
- перевірити наявність на ОІД нормативних документів, які забезпечують функціонування системи ЗІ, організацію проектування будівельних робіт з урахуванням вимог ТЗІ, а також нормативної та експлуатаційної документації, яка забезпечує ІД;
- виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів і провідників;
- визначити технічні засоби і системи, застосування яких не обґрунтовано службовою або виробничою необхідністю і які підлягають демонтуванню;
- визначити технічні засоби, які потребують переобладнання (перемонтування) та встановлення засобів ТЗІ.

За результатами обстеження слід скласти акт, який повинен бути затверджений керівником підприємства.

Матеріали обстеження необхідно використовувати під час розроблення окремої моделі загроз, яка повинна включати:

- генеральний та ситуаційний плани підприємства, схеми розташування засобів і систем забезпечення ІД, а також інженерних комунікацій, які виходять за межі контрольованої території;
- схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів НСД до ІзОД;
- оцінювання збитків, які передбачаються від реалізування можливих загроз.

4.1.4. Організація розроблення системи захисту інформації

На підставі матеріалів обстеження та окремої моделі загроз необхідно визначити головні задачі ЗІ і скласти технічне завдання (ТЗ) на розроблення системи ЗІ.

Технічне завдання повинно включати такі основні розділи:

- вимоги до системи ЗІ;
- вимоги до складу проектної та експлуатаційної документації;
- етапи виконання робіт;

- порядок внесення змін і доповнень до розділів ТЗ;
- вимоги до порядку проведення випробування системи захисту.

Основою функціонування системи захисту інформації є план ТЗІ, який повинен містити такі документи:

- перелік розпорядчих, організаційно-методичних, нормативних документів з ТЗІ, а також настанови щодо їхнього застосування;
- настанови про порядок реалізування організаційних, первинних та основних технічних заходів захисту;
- настанови, які встановлюють обов`язки, права та відповідальність персоналу;
- календарний план ТЗІ.

ТЗІ і план з ТЗІ розробляють фахівці з ТЗІ, узгоджують із зацікавленими підрозділами (організаціями). Затверджує їх керівник підприємства.

4.1.5. Реалізування організаційних заходів захисту інформації

Організаційні заходи ЗІ – комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне розв’язання задач ЗІ шляхом регламентуваня діяльності персоналу і порядку функціонування засобів (систем) забезпечення ІД та засобів (систем) ТЗІ.

У процесі розроблення і реалізування організаційних заходів потрібно:

- визначити окремі задачі захисту ІзОД;
- обґрунтувати структуру і технологію функціонування системи ЗІ;
- розробити і впровадити правила реалізування заходів з ТЗІ;
- визначити і встановити права та обов`язки підрозділів та осіб, які беруть участь в обробленні ІзОД;
- придбати засоби ТЗІ та нормативні документи і забезпечити ними ОІД підприємства;
- встановити порядок впровадження захищених засобів оброблення інформації, програмних і технічних засобів ЗІ, а також засобів контролю;
- встановити порядок контролю за функціонуванням системи ЗІ та за її якісними характеристиками;
- визначити зони безпеки інформації;
- встановити порядок проведення атестування системи ЗІ, її елементів і розробити програми атестаційного випробування;
- забезпечити керування системою ЗІ.

Оперативне розв’язання задач з ТЗІ досягається організацією керування системою ЗІ, для чого необхідно:

- вивчати й аналізувати технологію оброблення ІзОД у процесі ІД;
- оцінювати схильність ІзОД до впливу загроз у конкретний момент часу;
- оцінювати очікувану ефективність застосування засобів ТЗІ;
- здійснювати збирання, оброблення та реєстрацію даних, які відносяться до ТЗІ;
- розробляти і реалізовувати пропозиції щодо коригування плану ТЗІ в цілому або окремих його елементів.

4.1.6. Первинні технічні заходи захисту інформації

У процесі реалізування первинних технічних заходів потрібно забезпечити:

- блокування каналів витоку інформації;
- блокування НСД до інформації або її носіїв;
- перевірку справності та працездатності технічних засобів забезпечення ІД.

Блокування каналів витоку інформації може здійснюватися:

- демонтуванням технічних засобів, ліній зв'язку, сигналізації та керування, енергетичних мереж, використання яких не пов'язано з життєзабезпеченням ОІД та обробленням ІзОД;
- видаленням окремих елементів технічних засобів, які є середовищем поширення полів та сигналів з приміщень де циркулює ІзОД;
- тимчасовим від’єднанням технічних засобів, які не беруть участі в обробленні ІзОД, від ліній зв'язку, сигналізації, керування та енергетичних мереж;
- застосуванням способів та схемних рішень із ЗІ, які не порушують основних технічних характеристик засобів забезпечення ІД.

Блокування НСД до інформації або її носіїв може здійснюватися:

- створенням умов роботи в межах встановленого регламенту;
- унеможливленням використання програмних, програмно-апаратних засобів, які не пройшли перевірки (випробування).

Перевірку справності та працездатності технічних засобів і систем забезпечення ІД необхідно здійснювати відповідно до експлуатаційних документів.

Виявлені несправні блоки й елементи можуть сприяти витоку або порушенню цілісності інформації і підлягають негайній заміні (демонтуванню).

4.1.7. Основні технічні заходи захисту інформації

У процесі реалізування основних технічних заходів захисту потрібно:

- встановити засоби виявлення загроз і перевірити їхню працездатність;
- встановити захищені засоби оброблення інформації, засоби ТЗІ та перевірити їхню працездатність;
- застосувати програмні засоби захисту в блоках обчислювальної техніки, автоматизованих системах, здійснити їхнє загальне тестування і тестування на відповідність вимогам захищеності;
- застосувати спеціальні інженерно-технічні споруди, засоби (системи).

Вибір засобів ТЗІ зумовлюється фрагментарним або комплексним способом ЗІ.

Фрагментарний захист забезпечує протидію певній загрозі. Комплексний захист забезпечує одночасну протидію безлічі загроз.

Засоби виявлення загроз застосовують для сигналізації та сповіщення власника (користувача, розпорядника) ІзОД про витік інформації або порушення її цілісності. Засоби ТЗІ застосовуються автономно або спільно з технічними засобами забезпечення ІД для пасивного або активного приховування ІзОД.

Для пасивного приховування застосовують фільтри-обмежувачі, лінійні фільтри, спеціальні абонентські пристрої захисту та електромагнітні екрани.

Для активного приховування застосовують вузькосмугові й широкосмугові генератори лінійного та просторового зашумлення.

Програмні засоби застосовуються для забезпечення:

- ідентифікування та автентифікування користувачів, персоналу і ресурсів системи оброблення інформації;
- розмежування доступу користувачів до інформації, засобів обчислювальної техніки і технічних засобів ІС;
- цілісності інформації та конфігурації ІС;
- реєстрації та обліку дій користувачів;
- маскування оброблюваної інформації;
- реагування (сигналізації, від'єднання, зупинення робіт, відмови у запиті) на спроби несанкціонованих дій.

Спеціальні інженерно-технічні споруди, засоби та системи застосовуються для оптичного, акустичного, електромагнітного та іншого екранування носіїв інформації.

Розміщення, монтування та прокладання спеціальних інженерно-технічних засобів і систем, у тому числі систем заземлення та електроживлення засобів забезпечення ІД, слід здійснювати відповідно до вимог нормативних документів з ТЗІ.

4.1.8. Контроль за функціонуванням та керування системою захисту інформації

Контроль за функціонуванням системи ТЗІ на об'єктах ІД підприємства здійснюється з метою визначення й удосконалення стану ТЗІ в підрозділах підприємства, щодо яких здійснюється ТЗІ, виявлення та запобігання порушенням з ТЗІ в ІС та об'єктах.

Контроль стану ТЗІ в підрозділах підприємства організовується відповідно до планів, затверджених керівниками відповідних органів, шляхом проведення перевірок. Перевірки стану ТЗІ здійснюються безпосередньо комісіями, на які покладається забезпечення ТЗІ.

Перевірки поділяються на *комплексні*, *цільові* (тематичні) та *контрольні*.

Під час комплексної перевірки вивчається та оцінюється стан ТЗІ у підрозділах підприємства, щодо яких здійснюється ТЗІ.

Під час цільової (тематичної) перевірки вивчаються окремі напрямки ТЗІ, перевіряється виконання рішень (розпоряджень, наказів, вказівок) органів державної влади з питань ТЗІ в підрозділах, щодо яких здійснюється ТЗІ, виконання завдань або провадження діяльності в галузі ТЗІ, за відповідними дозволами та ліцензіями, суб'єктами системи ТЗІ.

Під час контрольної перевірки перевіряється усунення недоліків, які були виявлені під час проведення попередньої комплексної або цільової перевірки. Зазначені перевірки можуть бути планові та позапланові, з попередженням та раптові.

Позапланова перевірка здійснюється за вказівкою керівництва підприємства в разі виникнення потреби визначення повноти та достатності заходів з ТЗІ за наявності відомостей щодо порушень виконання вимог нормативно-правових актів з питань ТЗІ.

При проведенні перевірки стану ТЗІ контролю підлягають організаційні, організаційно-технічні, технічні заходи з ТЗІ у виділених приміщеннях, ІС і об'єктах, повнота та достатність робіт з атестування виділених приміщень.

Необхідно провести аналіз функціонування системи ЗІ, перевірку виконання заходів з ТЗІ, контроль ефективності захисту, підготувати та оприлюднити дані для керування системою ЗІ.

Керування системою ЗІ полягає в адаптуванні заходів з ТЗІ до поточного завдання ЗІ. За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізуються у найкоротший термін.

Контроль організаційних заходів з ТЗІ у підрозділах підприємства включає перевірку:

- переліку відомостей, які підлягають ТЗІ;
- окремої моделі загроз для ІС або об'єкту;
- плану контрольованої зони органу, щодо якого здійснюється ТЗІ;
- переліку виділених приміщень органу, щодо якого здійснюється ТЗІ, ІС та об'єктів;
- проведення категоріювання виділених приміщень та об'єктів.

Контроль організаційно-технічних і технічних заходів щодо ТЗІ у виділених приміщеннях, ІС та об'єктах, повноти та достатності робіт з атестування виділених приміщень включає перевірку відповідності виконання цих заходів до нормативно-правових актів з питань ТЗІ.

Організаційно-технічні й технічні заходи з ТЗІ у виділених приміщеннях, ІС та об'єктах, роботи з атестування виділених приміщень виконуються власними силами або суб'єктами підприємницької діяльності в галузі ТЗІ.

За результатами комплексної перевірки комісією складається акт перевірки стану та ефективності заходів з ТЗІ, а цільової та контрольної перевірки – довідка за довільною формою. Ознайомлення керівника суб'єкта системи ТЗІ з актом (довідкою) здійснюється під розпис.

Керівник підрозділу зобов'язаний ужити невідкладних заходів щодо усунення недоліків і реалізування пропозицій комісії відповідно до вимог нормативно-правових актів з питань ТЗІ.

Порушення встановлених норм та вимог з ТЗІ, виявлені під час проведення перевірок, поділяються на три категорії:

- перша – невиконання норм та вимог з ТЗІ, внаслідок чого створюється реальна можливість порушення конфіденційності, цілісності й доступності інформації або її витоку технічними каналами;
- друга – невиконання норм та вимог з ТЗІ, внаслідок чого створюються передумови для порушення конфіденційності, цілісності і доступності інформації або її витоку технічними каналами;
- третя – невиконання інших вимог з ТЗІ.

У разі виявлення порушення першої категорії вживають такі заходи:

- голова комісії негайно доповідає керівництву підприємства для прийняття рішення про припинення робіт, які проводились з порушенням норм і вимог ТЗІ, та про факт порушення;
- здійснюються заходи з усунення порушень у терміни, погоджені з підрозділом, на який покладено ТЗІ;
- в установленому порядку організовується розслідування причин, які призвели до порушень, з метою недопущення їх у подальшому і притягнення осіб, які допустили порушення нормативно-правових актів з питань ТЗІ до відповідальності згідно із законодавством України.

Дозвіл на відновлення робіт, під час виконання яких були виявлені порушення норм і вимог ТЗІ першої категорії, дає керівник підприємства за погодженням з підрозділом, на який покладено ТЗІ, після усунення порушень і перевірки достатності й ефективності вжитих заходів.

Керівництво підприємства зобов'язано надавати комісії повну інформацію стосовно впроваджених заходів з ТЗІ та сприяти проведенню їх перевірки.

4.1.11. Порядок контролю за станом технічного захисту інформації

Метою контролю є виявлення можливих технічних каналів витоку інформативного (небезпечного) сигналу (проведення спецдосліджень), вироблення заходів, які забезпечують його приховування, оцінювання достатності й ефективності вжитих заходів захисту, оперативний контроль за станом технічного захисту каналів витоку інформативного сигналу.

Технічний канал витоку вважається захищеним, якщо сигнал не перевищує встановленого нормативною документацією відношення ″інформативний сигнал/шум″.

Пристрої захисту і захищені технічні засоби вважаються справними, якщо їх параметри відповідають вимогам експлуатаційних документів.

Контроль за виконанням організаційних та підготовчих технічних заходів щодо ЗІ здійснюється візуальним оглядом каналів прокладання провідників і кабелів, які виходять за межі об`єкту захисту, а також технічних засобів захисту та захищеної техніки.

У ході перевірки визначаються:

- наявність електромагнітного зв`язку між лініями основних технічних засобів (ОТЗ) та допоміжних технічних засобів (ДТЗ);
- наявність виходів ліній зв`язку, сигналізації, годинофікації, радіотрансляції за межі виділених приміщень;
- наявність незадіяних ОТЗ, ДТЗ, провідників, кабелів;
- можливість від’єднання ОТЗ на період проведення конфіденційних переговорів або важливих нарад;
- рознесення джерел електромагнітних та акустичних полів на максимально можливу відстань у межах виділених приміщень;
- виконання заземлення апаратури, яке виключає можливість утворення петель з провідників та екранів;
- рознесення кабелів електроживлення ОТЗ та ДТЗ з метою виключення наведень небезпечних сигналів;

- виконання розведення кіл електроживлення екранованим або скрученим кабелем;
- наявність можливості від’єднання електроживлення ОТЗ під час знеструмлення мережі;
- відхилення параметрів електроживлення від норм, заданих в технічних умовах (ТУ), під час виникнення несправностей у колах живлення.

У процесі проведення спецдосліджень, перевірки ефективності технічних заходів захисту підлягають інструментальному контролю ОТЗ і лінії зв`язку.

У ході контролю перевіряються електромагнітні поля інформативних сигналів довкола апаратури та кабельних з`єднань ОТЗ, наявність інформативних сигналів у колах, провідниках електроживлення та заземлення ОТЗ та ДТЗ.

Під час спецдосліджень визначається радіус, за межами якого відношення ″інформативний сигнал/шум″ є меншим від гранично допустимої величини. Проводяться вимірювання і розрахунок параметрів інформативного сигналу, виявляється можливість його витоку каналами ПЕМВН, визначаються фактичні значення його параметрів у каналах витоку, проводиться порівняння фактичних параметрів з нормованими.

У випадку перевищення допустимих значень розробляються захисні заходи, використовуються засоби захисту (екранування джерел випромінювання, встановлення фільтрів, стабілізаторів, засобів активного захисту).

Після проведення спецдосліджень, вироблення та впровадження засобів захисту проводиться контроль за ефективністю застосованих технічних засобів захисту.

Результати контролю оформляються актом, складеним у довільній формі, який підписується перевіряючим та затверджуються керівником підприємства.

4.2. Захист інформації на об’єктах інформаційної діяльності державних підприємств України

4.2.1. Організаційно-правові заходи щодо охорони державної таємниці

Для охорони державної таємниці впроваджуються:

- єдині вимоги до виготовлення, користування, збереження, передавання, транспортування та обліку матеріальних носіїв таємної інформації;
- дозвільний порядок провадження органами державної влади діяльності, пов'язаної з державною таємницею;
- обмеження оприлюднення, передавання іншій державі або поширення іншим шляхом таємної інформації;
- обмеження перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів та технічних засобів, які належать до них;
- режим таємності органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, які провадять діяльність, пов'язану з державною таємницею;
- спеціальний порядок допуску, доступу громадян до державної таємниці;
- технічний та криптографічний захисти таємної інформації.

4.2.2. Категоріювання об'єктів інформаційної діяльності

Категоріюванню підлягають об'єкти, в яких обговорюється, наявна, пересилається, приймається, перетворюється, накопичується, обробляється, відтворюється і зберігається ІзОД.

Категоріювання об’єктів визначається Тимчасовим положенням з категоріювання об’єктів (ТПКО-95), затвердженим наказом Державної служби України з питань технічного захисту інформації від 10 липня 1995 р. № 35.

Цей нормативний документ призначений для організування робіт з категоріювання об'єктів. Його положення поширюються на центральні і місцеві органи державної виконавчої влади, місцеві Ради народних депутатів та їх органи, на військові частини всіх військових формувань, на підприємства, установи й організації всіх форм власності, представництва України за кордоном і громадян, які володіють, користуються та розпоряджаються ІзОД.

Власники СІ, яка не є власністю держави, положення цього документу застосовують на свій розсуд.

До об’єктів, які підлягають категоріюванню, відносяться:

- ІС та засоби обчислювальної техніки (ЗОТ), які функціонують і проектуються;
- технічні засоби, які призначені для роботи з ІзОД та не відносяться до ІС, за винятком тих, що засновані на криптографічних методах захисту;
- приміщення, призначені для проведення нарад, конференцій, обговорень тощо з використанням ІзОД;
- приміщення, в яких розміщені технічні засоби, призначені для роботи з ІзОД, у тому числі й засновані на криптографічних методах захисту.

Категоріювання проводиться з метою застосування обґрунтованих заходів щодо технічного захисту ІзОД, яка циркулює на об`єктах, від витоку каналами ПЕМВН, а також акустичних (віброакустичних) полів.

Встановлюються чотири категорії об'єктів залежно від *правового режиму доступу до інформації*, яка циркулює у них:

- до першої категорії відносяться об'єкти, в яких циркулює інформація, що містить відомості, які становлять державну таємницю, для якої встановлено гриф таємності ″Особливої важливості″;
- до другої категорії відносяться об’єкти, в яких циркулює інформація, що містить відомості, які становлять державну таємницю, для якої встановлено гриф таємності ″Цілком таємно″;
- до третьої категорії відносяться об'єкти, в яких циркулює інформація, що містить відомості, які становлять державну таємницю, для якої встановлено гриф таємності ″Таємно″, а також інформація, що містить відомості, які становлять іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству й державі;
- до четвертої категорії відносяться об'єкти, в яких циркулює СІ.

4.2.3. Порядок проведення робіт з категоріювання об'єктів

Для проведення робіт з категоріювання ОІД підприємства наказом керівника підприємства призначається комісія. У наказі визначається мета

створення комісії, її склад, об'єкти, які підлягають категоріюванню, терміни подання результатів.

Комісія з категоріювання визначає:

- вищий гриф таємності інформації, яка циркулює на об'єкті;
- підставу для категоріювання (первинне, планове, з огляду на зміни).

За результатами роботи комісії складаються акти довільної форми, в яких подаються зазначені відомості, раніше встановлена категорія та прийняте рішення про категоріювання. Акти затверджуються керівником підприємства.

Повторне категоріювання об'єкту проводиться у випадку зміни грифа таємності інформації, яка циркулює на об'єкті, і (або) умов розміщення технічних засобів, але не рідше одного разу на 5 років.

4.2.4. Засекречування та розсекречування матеріальних носіїв інформації

Перелік посад, які дають право посадовим особам надавати матеріальним носіям таємної інформації грифи таємності, затверджується керівником органу державної влади, що провадить діяльність, пов'язану з державною таємницею.

Засекречування матеріальних носіїв інформації здійснюється шляхом надання відповідному документу, виробу або іншому матеріальному носію інформації грифа таємності.

Реквізити кожного матеріального носія таємної інформації мають містити гриф таємності, який відповідає ступеню таємності інформації, встановленому рішенням державного експерта з питань таємниць, – ″Особливої важливості″, ″Цілком таємно″, ″Таємно″, дату та термін засекречування матеріального носія таємної інформації, який встановлюється з урахуванням передбачених ст. 13 Закону України ″Про державну таємницю″ термінів дії рішення про віднесення інформації до державної таємниці, підпис, його розшифрування та посаду особи, яка надала зазначений гриф, а також посилання на відповідний пункт (статтю) Зводу відомостей, які становлять державну таємницю.

Якщо реквізити, зазначені у частині другій цієї статті, неможливо нанести безпосередньо на матеріальний носій таємної інформації, вони мають бути зазначені у супровідних документах.

Забороняється надавати грифи таємності, передбачені цим Законом, матеріальним носіям іншої таємної інформації, яка не становить державної таємниці або конфіденційної інформації.

Ступені таємності науково-дослідних, дослідно-конструкторських і проектних робіт, які виконуються в інтересах забезпечення національної безпеки та оборони держави, встановлюються державним експертом з питань таємниць, який виконує свої функції у сфері діяльності замовника, разом з підрядником.

4.2.5. Звід відомостей, які становлять державну таємницю

Звід відомостей, які становлять державну таємницю, формує і публікує в офіційних виданнях СБ України на підставі рішень державних експертів з питань таємниць.

На підставі та у межах Зводу відомостей, які становлять державну таємницю, з метою конкретизування та систематизування даних про секретну

інформацію підприємства можуть створюватися розгорнуті переліки відомостей, що становлять державну таємницю.

Розгорнуті переліки відомостей, які становлять державну таємницю, не можуть суперечити Зводу відомостей, що становлять державну таємницю.

У разі включення до Зводу відомостей, які становлять державну таємницю, або до розгорнутих переліків цих відомостей інформації, що не відповідає категоріям і вимогам, передбачених ст. 8 Закону України ″Про державну таємницю″, або порушення встановленого порядку віднесення інформації до державної таємниці зацікавлені громадяни та юридичні особи мають право оскаржити відповідні рішення у суді. З метою недопущення розголошення державної таємниці судовий розгляд скарг може здійснюватися на закритих засіданнях відповідно до Закону України ″Про державну таємницю″.

4.3. Організаційно-правові принципи захисту ІС на основі міжнародних стандартів

Аналіз літературних джерел дає підстави стверджувати, що у процесі проектування, створення і експлуатування систем ЗІ є суттєві недоліки, які знижують ефективність їх функціонування. Необхідно обґрунтувати розроблення організаційно-правових засад ЗІ, які визначать стратегію, тактику системи ЗІ, а також враховує динаміку зміни загроз інформаційним активам ІС.

Однак, чинне законодавство України в інформаційній сфері не враховує вимог міжнародних стандартів, які надають більш широкий спектр послуг та профілів захищеності.

Дотримання принципів стандартів ISO/IEC серії 27000 забезпечує керування і контроль доступом, розроблення та обслуговування апаратно-програмних комплексів, керування безперервністю інформаційних процесів. Відповідність вимогам стандартів ISO/IEC серії 27000 і дотримання національних правових норм з ІБ є запорукою створення ефективної системи ЗІ.

Інкорпорацію законодавства України та структуру нормативно-правових актів України у галузі технічного захисту інформації обов’язкових до виконання, на рівні правової доктрини, можна подати наступним чином:

- Конституція України;
- Закони України;
- укази та розпорядження Президента України;
- постанови та розпорядження Кабінету Міністрів України;
- нормативно-правові акти Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації (ДССЗТЗІ) України;
- міжнародні угоди України з питань технічного захисту інформації, згода на обов'язковість виконання яких надана Верховною Радою України.

Регулятивно-правову основу забезпечення ЗІ у ІС підрозділів НП України становлять: Конституція України; Постанова Верховної Ради України ″Про концепцію національної безпеки України″; Закони України ″Про інформацію″, ″Про науково-технічну інформацію″, ″Про державну таємницю″, ″Про захист інформації у інформаційно-телекомунікаційних системах″, ″Про доступ до публічної інформації″, ″Про захист персональних даних″, Постанова Кабінету Міністрів

України ″Про затвердження правил захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах″.

В Україні розроблено серію нормативних документів системи технічного захисту інформації, основним з яких є НД ТЗІ 2.5-004-99 ″Критерії оцінки захищеності інформації комп'ютерних систем від несанкціонованого доступу″. Цей документ використовується при проектуванні та створенні комплексних систем захисту інформації (КСЗІ) державних інформаційних ресурсів, а також ІС, в яких обробляється інформація з обмеженим доступом, вимога щодо захисту якої визначено законом.

Однак, довільна використовувана при проектуванні КСЗІ методологія повинна бути сумісною з основними сучасними стандартами, такими як ISO/IEC серії 27000.

Тому, організаційно-правові засади системи ЗІ в ІС підрозділів НП України повинні формуватися відповідно до рекомендацій міжнародних стандартів та з дотриманням положень чинного законодавства України. Такими стандартами є: ISO/IEC 27001:2013 Інформаційні технології. Методи захисту. Системи менеджменту інформаційною безпекою; ISO/IEC 27002:2005 Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою; ISO/IEC 27003:2010 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації; ISO/IEC 27004:2009 Інформаційні технології. Методи захисту. Вимірювання; ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки; ISO/IEC 27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем менеджменту інформаційною безпекою.

У світовій практиці паралельно з розвитком технічних систем ЗІ розвивався напрямок стандартизації у частині менеджменту інформаційної безпеки. Результатом стало затвердження міжнародного стандарту ISO/IEC 27001:2005, а пізніше ISO/IEC 27001:2013. Впровадження системи менеджменту інформаційною безпекою (СМІБ). Стандарт дозволяє правильно організувати процес захисту інформаційних активів і управління ризиками для цих активів. Для контролю якості процесу менеджменту інформаційної безпеки було запроваджено інститут сертифікування. Сертифікат має міжнародний статус.

Неможливо обійти увагою новий стандарт ISO/IEC 27035:2011 Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки, який надає практичні рекомендації з виявлення, реєстрування і оцінювання випадків порушення інформаційної безпеки у ІС.

Він допоможе реагувати на інциденти ІБ, зокрема, вводити відповідні інструменти контролю для їхнього запобігання та відновлення у випадку реалізування загроз, покращувати загальний підхід до проектування технічних систем ЗІ.

Інтегрування системи управління інцидентами інформаційної безпеки у КСЗІ дає ряд переваг:

- підвищення загального рівня інформаційної безпеки;

- зменшення негативних наслідків реалізування загроз та часу відновлення штатних режимів функціонування ІС;
- посилення акценту на попередження інцидентів інформаційної безпеки;
- призначення пріоритетів і збору даних;
- внесок в обґрунтування рішень щодо формування бюджету та ресурсів;
- надання додаткової інформації для розроблення політики інформаційної безпеки та супровідної документації.

В Україні тільки перша версія ISO/IEC 27001:2005 частково отримала статус державного стандарту. Питання його практичного застосування залишається актуальним. Стандарт з урахуванням галузевих особливостей є обов'язковим у банківській сфері – СОУ Н НБУ 65.1 СУІБ 1.0: 2010.

Наявна правова колізія, коли міжнародні стандарти ISO/IEC серії 27000 в Україні не адаптовані, а ″Критерії оцінки захищеності інформації комп'ютерних систем від несанкціонованого доступу″ 1999 року є давно застарілими (ІТ та технології ЗІ, на відміну від чинного законодавства, інтенсивно розвивалися) і вона має тенденцію до загострення за найгіршим сценарієм.

Спробуємо з’ясувати головні причини виникнення такої ситуації. Отже, замовник своїми силами або із залученням підрядників розробляє технічне завдання (ТЗ) на КСЗІ, погоджує його з ДССЗЗІ, а потім, на підставі ТЗ проектує, реалізовує КСЗІ за допомогою сукупності організаційних, програмно-апаратних та інженерних засобів і вводить у дослідну експлуатацію. Далі, на підставі отриманої заявки ДССЗЗІ визначає компанію-ліцензіата, яка виступає організатором державної експертизи КСЗІ. Організатор експертизи, володіє штатом кваліфікованих експертів, розробляє програму та методику експертних випробувань, проводить їх і подає результати своєї роботи у вигляді проекту експертного висновку на розгляд експертної ради з питань технічного захисту інформації ДССЗЗІ. У разі позитивного рішення КСЗІ отримує атестат відповідності вимогам системи технічного захисту інформації.

Існуючій системі проектування КСЗІ притаманний і ряд інших недоліків. Так, для ІС з різною архітектурою, різними вимогами щодо забезпечення ЗІ, що ґрунтуються, в тому числі, і на різних категоріях доступу до інформації, існують стандартні функціональні профілі захищеності, тобто деякі фіксовані набори послуг безпеки. У той же час, розробник КСЗІ при формуванні ТЗ самостійно визначає об'єкти захисту, на які ці послуги поширюються. Експерти з ДССЗЗІ, в процесі узгодження ТЗ, перевіряють специфікації послуг, однак складно визначити рівень адекватності висунутих вимог до умов функціонування існуючих ІС.

Наступний етап контролю за відповідністю ТЗ створеній КСЗІ – експертиза. Зазвичай, експертиза полягає лише у перевірці якості реалізування заявлених послуг безпеки в ІС та комплектність документації на КСЗІ. Практично ніколи експертами якість впровадженої КСЗІ не перевіряється тестуванням на НСД до активів ІС. По-перше, цього не вимагає нормативно-правова база, а по-друге для проведення таких робіт потрібен високий фаховий рівень експертів.

Недостатнє бюджетне фінансування при закупівлі відповідних програмно-технічних засобів захисту накладає додаткові обмеження на технічну складову КСЗІ в ІС підрозділів НП України.

Фахівці можуть розробити та запровадити ідеальний варіант КСЗІ, відповідні служби та експерти виконають усі необхідні експертизи та заходи з атестування, а відсутність кваліфікованих фахівців зведе нанівець усі попередні зусилля. Для забезпечення якісного функціонування КСЗІ необхідно терміново переглянути посадові оклади працівникам Служби захисту інформації, щоб залучити потрібних фахівців.

У всіх аспектах забезпечення ЗІ основним елементом є аналіз можливих загроз щодо порушення роботи ІС, тобто загроз, які підвищують уразливість інформації, призводять до її витоку, випадкового або навмисного компрометування, знищення. Розглядаючи загальні принципи ЗІ в ІС, доцільно відзначити, що комплексний ЗІ в ІС має у своїй основі використання організаційних та програмно-апаратних засобів ЗІ. Такі засоби повинні забезпечувати ідентифікування та автентифікування користувачів, розподіл повноважень доступу до активів ІС, реєстрування та облік спроб НСД.

ЛЕКЦІЯ 5.

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

План

Вступ.

5.1. Захист інформації від витоку технічними каналами

5.2. Захист інформації під час використання засобів копіювально-розмножувальної техніки

ВСТУП

Інформація з обмеженим доступом у процесі ІД, основними видами якої є одержання, використання, поширення та зберігання інформації, може зазнавати впливу загроз її безпеці, у результаті чого може відбутися витік або порушення цілісності інформації. Схильність ІзОД до впливу загроз визначає її *вразливість*. Здатність системи ЗІ протистояти впливу загроз визначає *захищеність* ІзОД.

Зміст та послідовність робіт з протидії загрозам або з їх нейтралізування повинні відповідати етапам функціонування системи ЗІ і сутність яких зводиться до: проведення обстеження підприємства; розроблення і реалізування організаційних, первинних технічних, основних технічних заходів з використанням засобів ТЗІ; приймання робіт з ТЗІ; атестування засобів (систем) забезпечення ІД на відповідність вимогам нормативних документів з ТЗІ.

Порядок проведення робіт з ТЗІ або окремих їхніх етапів установлюється наказом (розпорядженням) керівника підприємства.

Роботи повинні виконуватися під керівництвом фахівців з ТЗІ. Для участі в роботах, надання методичної допомоги, оцінювання повноти та якості реалізування заходів ЗІ можуть залучатися фахівці з ТЗІ інших організацій, які мають ліцензію органу, уповноваженого Кабінетом Міністрів України.

5.1. Захист інформації від витоку технічними каналами

Об’єкт, мету та завдання ТЗІ визначають і встановлюють особи, які володіють, користуються, розпоряджаються ІзОД у межах прав і повноважень, наданих законами України, підзаконними актами та нормативними документами системи ТЗІ.

Середовищем поширення носіїв ІзОД можуть бути лінії зв’язку, сигналізації, керування, енергетичні мережі, кінцеве і проміжне обладнання, інженерні комунікації та споруди, загороджувальні будівельні конструкції, а також світлопроникні елементи будинків і споруд (отвори), повітряне, водне та інші середовища, грунт, рослинність тощо. Витік або порушення цілісності ІзОД (спотворення, модифікування, руйнування, знищення) можуть бути результатом реалізування загроз безпеці інформації.

Технічному захисту підлягає ІзОД, носіями якої є поля і сигнали, які утворюються в результаті роботи технічних засобів пересилання, оброблення, зберігання, відтворення інформації ОТЗ, а також ДТЗ. До ОТЗ відносяться:

- засоби і системи телефонного, телеграфного (телетайпного), директорського, гучномовного, диспетчерського, внутрішнього, службового та технологічного зв`язку;

- засоби і системи звукопідсилення, звукозапису та звуковідтворення;
- пристрої, що утворюють дискретні канали зв`язку: абонентська апаратура із засобами відтворення та сигналізації, апаратура підвищення достовірності пересилання, каналоутворювальна техніка;
- апаратура перетворення, оброблення, пересилання і приймання відеоканалів, які містять факсимільну інформацію.

ОТЗ можуть бути захищеними і незахищеними. До ДТЗ і систем відносяться:

- засоби і системи спеціальної охоронної сигналізації (на відкриття дверей, вікон та проникнення до приміщення сторонніх осіб), пожежної сигналізації (з давачами, які реагують на дим, світло, тепло, звук);
- система дзвінкової сигналізації (виклик секретаря, вхідна сигналізація);
- контрольно-вимірювальна апаратура;
- засоби і системи кондиціонування (давачі температури, вологості, кондиціонери);
- засоби і системи провідної радіотрансляційної мережі та приймання програм радіомовлення і телебачення (абонентські гучномовці системи радіомовлення та сповіщення, радіоприймачі та телевізори);
- засоби і системи годинофікації;
- засоби і системи електроосвітлення та побутового електрообладнання (світильники, люстри, настільні та стаціонарні вентилятори, електронагрівальні прилади, холодильники, паперорізальні машини, провідна мережа електроосвітлення);
- електронна та електрична оргтехніка.

ДТЗ можуть бути захищеними і незахищеними.

Елементами ОТЗ та ДТЗ можуть бути зосереджені випадкові антени (апаратура та її блоки) або розподілені випадкові антени (кабельні лінії та провідники).

Такими елементами можуть бути:

- кінцеві технічні засоби і прилади;
- кабельні мережі, які з`єднують пристрої та обладнання;
- комутаційні пристрої (комутатори, кроси тощо);
- елементи заземлення та електроживлення.

Роботи із захисту ІзОД від витоку каналами ПЕМВН складаються з організаційних, підготовчих технічних, основних технічних заходів і контролю за виконанням заходів з ТЗІ та за ефективністю цього захисту.

5.1.1. Організаційні заходи

Організаційні і підготовчі заходи щодо ТЗІ проводяться одночасно і є першим етапом робіт, технічні заходи – наступним етапом робіт. Заходи щодо ТЗІ і контролю за його ефективністю можуть виконуватись організаціями, які мають ліцензію ДСТСЗІ СБУ на право надання послуг у галузі ТЗІ.

На етапі проведення організаційних заходів потрібно:

- визначити перелік відомостей з обмеженим доступом, які підлягають технічному захисту (визначає власник інформації згідно з чинним законодавством України);
- обґрунтувати необхідність розроблення і реалізування захисних заходів з урахуванням матеріальної або іншої шкоди, яка може бути завдана внаслідок можливого порушення цілісності ІзОД або її витоку технічними каналами;
- встановити перелік виділених приміщень, у яких не допускається реалізування загроз та витік ІзОД;
- визначити перелік технічних засобів, які повинні використовуватися як ОТЗ;
- визначити технічні засоби, застосування яких не обґрунтовано службовою та виробничою необхідністю та які підлягають демонтажу;
- визначити наявність задіяних і незадіяних повітряних, наземних, настінних та закладених у приховану каналізацію кабелів, кіл і провідників, які виходять за межі виділених приміщень;
- визначити системи, що підлягають демонтажу, потребують переобладнання кабельних мереж, кіл живлення, заземлення або встановлення в них захисних пристроїв.

За результатами обстеження складаються акт довільної форми з переліком виконаних заходів і додатками (за необхідністю):

- переліку ОТЗ, розміщених у виділених приміщеннях;
- плану виділених приміщень із зазначенням місць встановлення ОТЗ, а також схем прокладання кабелів, провідників;
- переліку технічних засобів, кабелів, кіл, провідників, які підлягають демонтажу.

Акт підписується виконавцем робіт і затверджується керівником організації (підприємства).

5.1.2. Підготовчі технічні заходи

Підготовчі технічні заходи включають у себе первинні заходи блокування електроакустичних перетворювачів і ліній зв`язку, які виходять за межі виділених приміщень.

Блокування ліній зв`язку може виконуватися такими способами:

- від’єднанням ліній зв`язку ОТЗ та ДТЗ або встановленням найпростіших схем захисту;
- демонтажем технічних засобів, кабелів, провідників, які виходять за межі виділених приміщень;
- винесенням за межі виділених приміщень окремих елементів технічних засобів, які можуть бути джерелом виникнення каналу витоку інформації.

Блокування каналів можливого витоку ІзОД у системах міського та відомчого телефонного зв`язку може здійснюватися:

- від’єднанням дзвінкових (викличних) ліній телефонного апарата;
- установленням у колі телефонного апарата без розривної розетки для тимчасового від’єднання;

- установленням найпростіших пристроїв ЗІ.

Запобігання витоку ІзОД через діючі системи гучномовного диспетчерського та директорського зв`язку здійснюється із застосуванням таких захисних заходів:

- встановленням у викличних колах вимикачів для розриву кіл;
- встановленням на вході гучномовців вимикачів (реле), які дають можливість розривати кола у двох провідниках;
- забезпеченням можливості від'єднання живлення мікрофонних підсилювачів;
- встановленням найпростіших пристроїв ЗІ.

Захист ІзОД від витоку через радіотрансляційну мережу, яка виходить за межі виділеного приміщення, може бути забезпечений:

- від'єднанням гучномовців від двох провідників;
- вмиканням найпростіших пристроїв захисту.

Для служби сповіщення доцільно надати доступ до чергових абонентських пристроїв поза виділеними приміщеннями: живлення до цих пристроїв необхідно прокладати окремим кабелем.

Блокування каналів витоку ІзОД через кола вторинних електрогодинників системи електрогодинофікації здійснюється від'єднанням їх на період проведення закритих заходів.

Запобігання витоку ІзОД через системи пожежної та охоронної сигналізацій здійснюється від'єднанням давачів пожежної та охоронної сигналізації на період проведення важливих заходів, що містять ІзОД, або застосуванням давачів, які не потребують спеціальних заходів ЗІ.

З метою виключення можливості витоку ІзОД незахищеними технічними засобами під час роботи телевізорів, радіоприймачів, звукопідсилювальної та звуковідтворювальної апаратури необхідно на період проведення важливих заходів зазначені пристрої від'єднувати від мережі електроживлення одночасно від двох провідників. Блокування витоку ІзОД через системи електронної оргтехніки та кондиціонування може бути забезпечене такими заходами:

- розташуванням зазначених систем усередині контрольованої території без винесення окремих компонентів за її межі;
- електроживленням систем від трансформаторної підстанції, яка знаходиться всередині контрольованої території.

При невиконанні зазначених вище умов системи повинні від'єднуватися від мережі електроживлення (одночасне відмикання усіх провідників).

Захист ІзОД від витоку через кола електроосвітлення та електроживлення побутової техніки повинен здійснюватися під'єднанням зазначених кіл до окремого фідера трансформаторної підстанції, до якого не допускається під'єднання сторонніх користувачів.

5.1.3. Технічні заходи

Технічні заходи є основним етапом робіт з технічного захисту ІзОД і полягають у забезпеченні ОТЗ та ДТЗ пристроями ТЗІ.

Під час вибору, встановлення, заміни технічних засобів слід керуватися паспортами, технічними описами, настановами з експлуатації, рекомендаціями з встановлення, монтування та експлуатації, які додаються до цих засобів.

ОТЗ повинні розміщуватися якомога ближче до центру будинку або в напрямку найбільшої частини контрольованої території. Складові елементи ОТЗ доцільно встановлювати в одному приміщенні або у суміжних.

Якщо відзначені вимоги неможливо виконати, необхідно вжити додаткових заходів ЗІ:

- встановити високочастотні ОТЗ в екрановане приміщення (камеру);
- встановити в незахищені канали зв`язку, лінії, провідники і кабелі спеціальні фільтри та пристрої;
- прокласти провідники і кабелі в екранувальних конструкціях;
- зменшити довжину ділянок паралельного прокладення кабелів і провідників різних систем з провідниками та кабелями, якими передається ІзОД;
- виконати технічні заходи щодо захисту ІзОД від витоку колами заземлення та електроживлення.

До засобів технічного захисту відносяться:

- фільтри-обмежувачі та спеціальні абонентські пристрої захисту для блокування витоку мовної ІзОД через двопровідні лінії телефонного зв`язку, системи директорського та диспетчерського зв`язку;
- пристрої захисту абонентських однопрограмних гучномовців для блокування витоку мовної ІзОД через радіотрансляційні лінії;
- мережеві фільтри для блокування витоку мовної ІзОД колами електроживлення змінного (постійного) струму;
- фільтри захисту лінійні (високочастотні) для встановлення в лініях апаратів телеграфного (телекодового) зв`язку;
- генератори лінійного зашумлення;
- генератори просторового зашумлення;
- екрановані камери спеціальної розробки.

Для телефонного зв`язку, не призначеного для пересилання ІзОД, рекомендується застосовувати апарати вітчизняного виробництва, сумісні з пристроями ЗІ. Телефонні апарати іноземного виробництва можуть застосовуватися за умови проходження спецдосліджень і позитивного висновку компетентних організацій системи ТЗІ про їх сумісність з пристроями захисту.

Вибір методів і способів захисту елементів ОТЗ та ДТЗ, які мають мікрофонний ефект, залежить від величини їх вхідного опору на частоті 1 кГц.

Елементи з вхідним опором меншим від 600 Ом (головки гучномовців, електродвигуни вентиляторів, трансформатори тощо) рекомендується від'єднувати від електроживлення усіх провідників або встановлювати у розрив кіл пристрої захисту з високим вихідним опором для зниження до мінімальної величини інформативної складової струму.

Елементи з високим вхідним опором (електричні дзвінки, телефонні капсулі, електромагнітні реле) рекомендується не тільки від'єднувати від кіл живлення, а й замикати на низький опір або закорочувати, щоб зменшити

електричне поле від цих елементів, зумовлене напругою, наведеною під час впливу акустичного поля. При цьому слід враховувати, що обраний спосіб захисту не повинен порушувати працездатність технічного засобу і погіршувати його технічні параметри.

Високочастотні автогенератори, підсилювачі (мікрофонні, приймання, пересилання, гучномовного зв`язку) та інші пристрої, які містять активні елементи, рекомендується від'єднувати від ліній електроживлення у "черговому режимі" або "режимі очікування виклику".

Під'єднання пристроїв захисту слід виконувати без порушення або зміни електричної схеми, ОТЗ і ДТЗ.

Захист ІзОД від витоку кабелями та провідниками рекомендується здійснювати шляхом:

- застосування екранувальних конструкцій;
- роздільного прокладання кабелів ОТЗ та ДТЗ.

За неможливості виконання вимог щодо рознесення кабелів електроживлення ОТЗ та ДТЗ електроживлення останніх слід здійснювати екранованими кабелями від розподілених систем або через мережеві фільтри.

Не допускається утворення петель та контурів кабельними лініями. Перехрещення кабельних трас різного призначення рекомендується здійснювати під прямим кутом одна до одної. Електроживлення ОТЗ повинно бути стабілізованим за напругою та струмом для нормальних умов функціонування ОТЗ і забезпечення норм захищеності.

Необхідно передбачити від'єднання електромережі від джерела живлення ОТЗ під час зникнення напруги в мережі, під час відхилення параметрів електроживлення від норм, заданих в ТУ, та під час виникнення несправностей у колах електроживлення.

Усі металеві конструкції ОТЗ (шафи, пульти, корпуси розподільних пристроїв та металеві оболонки кабелів) повинні бути заземлені.

Заземлення ОТЗ слід здійснювати від загального контуру заземлення, розміщеного в межах контрольованої території, з опором заземлення за постійним струмом відповідно до вимог стандартів.

Система заземлення повинна бути єдиною для всіх елементів ОТЗ і формуватися за радіальною схемою.

Утворення петель і контурів у системі заземлення не допускається. Екрани кабельних ліній ОТЗ, які виходять за межі контрольованої території, повинні заземлятися в кросах від загального контуру заземлення в одній точці для виключення можливості утворення петель в екранах та корпусах.

У кожному пристрої повинна виконуватися умова безперервності екрану від входу до виходу. Екрани слід заземляти тільки з одного боку. Екрани кабелів не повинні використовуватися як другий провід сигнального кола або кола живлення.

Екрани кабелів не повинні мати електричного контакту з металоконструкціями. Для монтажу слід застосовувати екрановані кабелі з ізоляцією або одягати на екрани ізоляційну трубку.

У довгих екранованих лініях (мікрофонних, лінійних, звукопідсилювальних) рекомендується ділити екран на ділянки для одержання малих опорів для високочастотних струмів і кожну ділянку заземляти тільки з одного боку.

Результати виконання технічних заходів оформляються актом приймання робіт, складеним у довільній формі, підписуються виконавцем робіт і затверджуються керівником підприємства.

5.2. Захист інформації під час використання засобів копіювально-розмножувальної техніки

5.2.1. Основні положення

Під час оброблення документів засобами копіювально-розмножувальної техніки (КРТ) електричні струми інформативних сигналів спричиняють виникнення ПЕМВН, які можуть бути носіями ІзОД і реєструватися технічними засобами розвідки за межами контрольованої зони (КЗ) об’єкта.

Крім того, ПЕМВН може наводити електрорушійну силу (ЕРС) в розташованих поряд з джерелом випромінювання колах електроживлення, заземлення, лініях зв’язку тощо. У разі виходу таких кіл і ліній за межі КЗ наведення інформативних сигналів можуть реєструватися технічними засобами розвідки.

Згідно з ″Класифікатором засобів копіювально-розмножувальної техніки″ засоби КРТ поділяються на два класи:

- клас А – засоби КРТ, що у процесі роботи не створюють інформативні ПЕМВН (світлокопіювальні, фотокопіювальні, термокопіювальні, мікрографічні, електрофотографічні аналогові апарати з оптичним перенесенням зображення з оригіналу на копію);
- клас Б – електрофотографічні цифрові апарати з оптично-дискретним перенесенням зображення з оригіналу на копію.

Клас Б поділяється на два підкласи:

- підклас І – засоби КРТ з циклічним інформативним сигналом (цифрові електрофотографічні апарати);
- підклас ІІ – засоби КРТ з одноразовим інформативним сигналом (різографи).

Інформативна складова в електромагнітному випромінюванні присутня лише в цифровій КРТ (клас Б), яка реалізовує оптичне сканування зображення оригіналу з його наступним цифровим розкладанням, подальшою передачею цифрового електричного сигналу та лазерною розгорткою інформативного сигналу при створенні копії. У цифровій КРТ існує реальна загроза витоку ІзОД. Під час роботи таких апаратів можливий витік інформації каналами ПЕМВН.

5.2.2. Вимоги до захисту інформації та організація технічного захисту інформації

Захист інформації забезпечується, якщо задовільняється одна з таких вимог:

- використовуються КРТ класу А;
- у разі використання КРТ класу Б здійснено заходи ТЗІ, які забезпечують виконання відповідних норм захисту згідно з НД ТЗІ.

ЗІ здійснюється в порядку, встановленому нормативними документами системи ТЗІ (НД ТЗІ) з розроблення та впровадження заходів ТЗІ на об’єктах ІД з уточненнями, які визначаються особливостями використання технічних засобів:

- у приміщенні не циркулює інша інформація, крім тієї, яка обробляється засобами КРТ;
- у приміщенні, разом з ІзОД, яка обробляється КРТ, циркулює також інша інформація.

Якщо у приміщенні не циркулює інша інформація, крім тієї, яка обробляється засобами КРТ, тоді у разі використання КРТ класу А під час розроблення та впровадження ТЗІ слід виходити з того, що технічні канали витоку інформації (ТКВІ) можуть створювати закладні пристрої з оптичними перетворювачами.

У разі використання КРТ класу Б, слід виходити з можливості існування ТКВІ шляхом ПЕМВН та закладних пристроїв з оптичними та електромагнітними перетворювачами.

Якщо у приміщенні, разом з ІзОД, яка обробляється КРТ, циркулює також інша інформація, тоді необхідно виконати повний обсяг робіт, передбачених загальним порядком розроблення заходів з ТЗІ, що враховує загрози витоку ТКВІ, що обробляється засобами КРТ, а також іншої інформації, яка є наявною у цьому ж приміщенні.

У разі використання КРТ класу Б в процесі розроблення заходів з ТЗІ необхідно враховувати вимоги НД ТЗІ. При цьому слід передбачати:

- встановлення КЗ, за межами якої виконуються норми захисту;
- вилучення незадіяних (задіяних) допоміжних технічних засобів, застосування яких не обґрунтоване виробничою необхідністю, а також вилучення з КЗ незадіяних (задіяних) кабелів та провідників, що виходять за межі КЗ, у яких можливе наведення ЕРС інформативними ПЕМВН;
- застосування захищених засобів КРТ;
- блокування ТКВІ за допомогою засобів ТЗІ (пасивних, активних тощо).

Технічні засоби, що використовуються з метою забезпечення ТЗІ, охорона якої забезпечується державою, повинні мати дозвіл уповноваженого органу і міститися у відповідних переліках.

Контроль ефективності ЗІ здійснюється згідно з чинними НД ТЗІ.

Заходи з ТЗІ доцільно виконувати одночасно з захистом іншої інформації, яка циркулює на об’єкті, де використовуються засоби КРТ.

Оброблення ІзОД можливе лише після атестування комплексу ТЗІ на відповідність вимогам НД ТЗІ.

5.2.3. Рекомендації з захисту інформації, яка обробляється засобами КРТ класу Б

З метою ТЗІ від витоку мережами електроживлення трансформаторну підстанцію низької напруги, кабелі електроживлення, усі елементи заземлення та засоби ТЗІ, які під’єднуються до мережі живлення, рекомендується розміщувати у межах КЗ. Забороняється під’єднання до низької сторони трансформаторної

підстанції споживачів електроенергії, які розміщуються за межами КЗ. Якщо ця вимога не виконується, тоді необхідно вживати додаткові заходи із захисту (пасивні та активні), які визначаються за результатами обстеження та спецдосліджень.

Кола електроживлення КРТ на ділянці від технічних засобів до розділяючої системи або захисних мережевих фільтрів рекомендується прокладати в жорстких екранованих конструкціях, кабелі прокладати окремими пакетами без утворення петель, перетинання здійснювати під прямим кутом без електричного контакту екрануючих оболонок кабелів. У разі неможливості виконання вимог щодо рознесення кабелів, електроживлення засобів КРТ повинно забезпечуватися екранованими кабелями від розділювальних систем або через мережеві фільтри.

Опір контуру заземлення не повинен перевищувати 4 Ом, заземлюючі провідники повинні мати перехідний опір з`єднання не більший, ніж 600 мкОм та розміщуватися у межах КЗ (можливе використання глибинного заземлювача). Забороняється використовувати для заземлення металеві конструкції водопостачання, опалення, газофікації тощо. Якщо заземлення виконати неможливо, тоді допускається виконати занулення КРТ.

Екрануючі конструкції засобів КРТ та кабелів повинні створювати екранований замкнутий об’єм. У разі недостатності пасивних заходів ТЗІ вживаються заходи активного захисту – просторове або лінійне зашумлення.

ЛЕКЦІЯ 6.

ЗАХИСТ WEB-РЕСУРСІВ У ІС ПІДПРИЄМСТВ

План

Вступ.

6.1. Характеристика типових умов функціонування та вимоги до захисту інформації Web-порталу підприємства

6.2. Вимоги до захисту Web-порталу підприємства

6.3. Інформаційна система підприємства

6.4. Середовище користувачів інформаційної системи підприємства

6.5. Фізичне середовище інформаційної системи підприємства

6.6. Поняття політики інформаційної безпеки у інформаційній системі підприємства

6.7. Політика інформаційної безпеки Web-порталу підприємства

ВСТУП

Підприємство під час створення Web-порталу та визначення операторів, вузли яких будуть використовуватися для під'єднання до мережі Internet, повинно керуватися законами України, іншими нормативно-правовими актами, що встановлюють вимоги з ТЗІ.

Web-портал підприємства може бути розміщена на власному сервері або на сервері, який є власністю оператора. Власник сервера зобов'язаний гарантувати власнику інформації встановлений рівень захисту. Функціонування Web-порталу забезпечується ІС підприємства, за допомогою якої здійснюється актуалізування розміщених на Web-порталі інформаційних активів та керування доступом до них.

Для забезпечення ЗІ Web-порталу у цій ІС створюється КСЗІ, яка є сукупністю організаційних і інженерно-технічних заходів, а також програмно-апаратних засобів, які забезпечують ЗІ. КСЗІ підлягає державній експертизі у порядку, передбаченому Положенням про державну експертизу в сфері ТЗІ.

Захист інформації на всіх етапах створення та експлуатування Web Web-порталу здійснюється відповідно до розробленого підприємством плану ЗІ. План захисту затверджується керівником підприємства, а у випадку використання сервера оператора – погоджується з власником сервера.

Перелік інформації, призначеної для публічного розміщення на Web-порталі, визначається з урахуванням вимог чинного законодавства та затверджується керівником підприємства, що є власником Web-порталу.

Організація робіт із ЗІ та забезпечення контролю за станом її захищеності на Web-порталі підприємства здійснюється відповідальним підрозділом або відповідальною особою. У випадку користування послугами оператора щодо розміщення, експлуатування та адміністрування Web-порталу власник інформації укладає з оператором угоду, яка визначає права і обов'язки сторін, умови під'єднання, розміщення інформації та забезпечення доступу до неї, інші питання, що вимагають урегулювання між власником інформації Web-порталу та оператором, виходячи з вимог чинного законодавства України у сфері ЗІ.

Окремі питання із ЗІ можуть оформлятися у вигляді додатків, які є невід'ємною частиною угоди.

6.1. Характеристика типових умов функціонування та вимоги до захисту інформації Web-порталу підприємства

Важливим напрямком підвищення ефективності функціонування інформаційних систем є інтегрування з глобальною мережею Internet. У багатьох випадках завдяки, власне ступеню інтегрування, вирішуються дві основні задачі. По-перше, об'єднуються територіально розподілені підсистеми ІС. По-друге, користувачам Internet забезпечується доступ до відкритої інформації ІС. Досить часто при вирішенні обох задач використовується Web-сайт (Web-портал), який, крім того, відіграє представницьку роль ІС у мережі Internet. Практичний досвід показує, що функціонування Web-порталу значною мірою впливає на ефективність функціонування всієї ІС. Основою Web-порталу є Web-сервер, що забезпечує доступ клієнтів із мережі Internet до Web-сторінок порталу.

Останнім часом зафіксовані непоодинокі випадки масованих атак порушників на ІС зі сторони Internet, причому досить часто об'єктом атак був Web-сервер. Наприклад, за даними Міністерства Оборони США, було зафіксовано багато атак, мета яких – отримання контролю над військовими серверами. Як правило, наслідками більшості успішних атак на Web-сервер ставало унеможливлення санкціонованого доступу, порушення цілісності або створення неконтрольованого поширення інформації ІС.

Таким чином у багатьох випадках успішна атака на Web-сервер може призвести не тільки до загрози функціонування Web-порталу, але й до значного зменшення ефективності функціонування всієї ІС. Цим визначається актуальність загальної проблеми захису Web-активів, а також її зв'язок з глобальною науково-практичною задачею забезпечення інформаційної безпеки ІС.

До складу ІС, яка забезпечує функціонування Web-порталу, підприємства входять:

- ОС, фізичне середовище, в якому вона знаходиться і функціонує, середовище користувачів,
- оброблювана інформація, у тому числі й технологія її оброблення.

Під час забезпечення ЗІ мають бути враховані всі характеристики відзначених складових частин, які впливають на реалізування політики безпеки Web-порталу. У випадку, якщо Web-портал підприємства містить посилання на інформаційні ресурси іншого Web-порталу, умови функціонування останнього не повинні порушувати встановлену для даного Web-порталу політику безпеки.

6.2. Вимоги до захисту Web-порталу підприємства

КСЗІ повинна забезпечувати реалізування вимог із захисту цілісності та доступності розміщеної на Web-порталі загальнодоступної інформації, а також конфіденційності та цілісності технологічної інформації Web-порталу.

Технологія оброблення інформації повинна відповідати вимогам політики безпеки інформації, визначеної для ІС, яка забезпечує функціонування Web-порталу.

Вимоги щодо забезпечення цілісності загальнодоступної інформації Web-порталу та конфіденційності й цілісності технологічної інформації вимагають застосування технологій, що забезпечують реалізування контрольованого і санкціонованого доступу до інформації та охорону неконтрольованого й несанкціонованого її модифікування.

Технологія оброблення інформації повинна бути здатною реалізовувати можливість виявлення спроб НСД до інформації Web-порталу та процесів, які з цією інформацією пов'язані, а також забезпечити реєстрацію в системному журналі визначених політикою відповідної послуги безпеки подій (як НСД, так і авторизованих звернень).

Для користувачів, які порушили встановлені правила розмежування доступу до Web-порталу, засоби КСЗІ на період сеансу роботи повинні забезпечити блокування доступу до Web-порталу.

Технологічними процесами повинна бути реалізована можливість створення резервних копій інформації Web-порталу та процедури їх відновлення з використанням резервних копій.

Технологія оброблення інформації повинна передбачати можливість аналізу використання користувачами і процесами обчислювальних ресурсів ІС і забезпечувати керування ресурсами.

6.3. Інформаційна система підприємства

Узагальнена функціонально-логічна структура інформаційної системи підприємства включає:

- підсистему оброблення інформації;
- підсистему взаємодії з користувачами ІС;
- підсистему обміну даними.

Підсистема оброблення інформації забезпечує створення, зберігання, актуалізування інформації Web-порталу і складається із засобів оброблення інформації, системного та функціонального програмного забезпечення.

До засобів оброблення інформації належать Web-сервер та необхідна кількість робочих станцій для забезпечення всіх функцій щодо супроводу Web-порталу та ЗІ.

Підсистема взаємодії з користувачами ІС забезпечує за запитами користувачів, надання доступу до загальнодоступної інформації Web-порталу, яка має вигляд HTLM-документа, з використанням мереж передавання даних та стандартних Internet-протоколів. Підсистема складається з програмно-апаратного комплексу, який дозволяє здійснювати маршрутизацію запитів користувачів, забезпечувати пошук необхідних користувачу інформаційних ресурсів і доступ до них.

Підсистема обміну даними забезпечує підготування та безпосередній імпорт/експорт інформації в/з ІС, а також внутрішньосистемний обмін інформацією між Web-сервером та робочими станціями з реалізуванням фаз встановлення, підтримання та завершення з'єднання.

Відповідно до політики безпеки інформації в ІС підсистеми комплектуються засобами ЗІ (можуть використовуватися штатні засоби захисту системного і

функціонального програмного забезпечення (ПЗ) та/або спеціалізовані засоби). Програмно-апаратні засоби захисту повинні мати належним чином оформлені документи (експертні висновки, сертифікати), які засвідчують відповідність цих засобів вимогам НД системи ТЗІ.

Встановлення на ОС нових (додаткових) компонентів, ПЗ (системного та/або функціонального), сервісів та розміщення довільних інших мережевих ресурсів, які не належать до категорії Web-порталу підприємства, не повинно порушувати політику безпеки інформації в ІС, яка забезпечує функціонування Web-порталу.

Вимоги до робочих станцій фізичних і юридичних осіб, які є користувачами загальнодоступної інформації Web-порталу, та їхнього ПЗ не висуваються.

6.4. Середовище користувачів інформаційної системи підприємства

За рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються у процесі функціонування ІС, користувачі поділяються на такі категорії:

- користувачі, яким надано право доступу тільки до загальнодоступної інформації Web-порталу;
- користувачі, яким надано повноваження супроводжувати КСЗІ та забезпечувати керування ІС (адміністратор безпеки, інші працівники системи ЗІ, користувачі з функціональними обов’язками Web-майстрів, адміністраторів сервісів, адміністраторів мережевого обладнання, адміністраторів ресурсів DNS (Domain Name System), PROXY, FTP (File Transfer Protocol), якщо передбачається їх взаємодія з Web-порталом тощо);
- технічний обслуговуючий персонал, який забезпечує належні умови функціонування ІС, повсякденну підтримку життєдіяльності фізичного середовища (електрики, технічний персонал з обслуговування приміщень будівель, ліній зв’язку тощо);
- розробники ПЗ, які здійснюють розроблення та впровадження нових функціональних процесів, а також супроводження вже діючого функціонального ПЗ сервера, розробники та проектанти фізичної структури ІС;
- постачальники обладнання і технічних засобів та фахівці, які здійснюють його монтаж, поточне гарантійне й післягарантійне обслуговування.

Користувачі, які належать до категорії "В", повинні мати належний рівень кваліфікації для виконання своїх службових та функціональних обов’язків у відповідності до визначених технологічних процесів та режимів експлуатування обладнання.

Доступ до інформаційних активів Web-порталу повинен надаватися користувачам у відповідності до положень політики ІБ, визначеної для ІС, що забезпечує функціонування Web-порталу.

Для встановлення правил і регламентування доступу цих користувачів до інформації Web-порталу розробляються та впроваджуються нормативні та розпорядчі документи, передбачені планом ЗІ.

Користувачі, які належать до категорій "В" – "Д", можуть мати доступ до програмних та апаратних засобів ІС лише під час робіт із тестування й інсталяції

ПЗ, встановлення і регламентного обслуговування обладнання тощо, за умови обмеження їхнього доступу до технологічної інформації КСЗІ.

Зазначені категорії осіб повинні мати дозвіл на доступ до відомостей, які містяться в програмній та технічній документації на ІС або окремі її компоненти, і необхідні їм для виконання функціональних обов'язків.

Користувачі загальнодоступної інформації одержують доступ до Web-порталу у відповідності до діючих у мережі Internet правил та регламенту.

6.5. Фізичне середовище інформаційної системи підприємства

Фізичне середовище, що призначене для розміщення, експлуатування, адміністрування Web-порталу підприємства, включає:

- приміщення, в яких розташовані сервер і робочі станції з усіма компонентами (ОС, сховища для носіїв інформації та документації, робочі місця обслуговуючого персоналу);
- засоби енергопостачання, заземлення, життєзабезпечення та сигналізації приміщення;
- допоміжні технічні засоби та засоби зв'язку.

Приміщення, де розміщуються компоненти ОС, повинні знаходитися у межах КЗ і мати охорону.

Доступ здійснюється у порядку визначеному системою ЗІ та затвердженому власником Web-порталу, або у відповідності до умов, передбачених угодою між власником Web-порталу та оператором (провайдером).

Вимоги до засобів енергопостачання, заземлення, життєзабезпечення, сигналізації приміщення та допоміжних технічних засобів і засобів зв'язку не висуваються.

6.6. Поняття політики інформаційної безпеки у інформаційній системі підприємства

Політика інформаційної безпеки – це пакет документів, який описує і регламентує систему управління інформаційною безпекою інформаційних систем, відповідає вимогам чинного законодавства України та міжнародних угод, базується на рекомендаціях міжнародних стандартів. Такими стандартами є:

- ISO/IEC 27002:2005 Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою;
- ISO/IEC 27003:2010 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації;
- ISO/IEC 27004:2009 Інформаційні технології. Методи захисту. Вимірювання;
- ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки;
- ISO/IEC 27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем управління інформаційною безпекою

Метою політики інформаційної безпеки є впровадження та ефективне управління системою забезпечення інформаційної безпеки, спрямованої на

захист інформаційних активів, забезпечення безперервної діяльності ІС підприємства, мінімізування ризиків інформаційної безпеки.

Основним завданням впровадження політики інформаційної безпеки є захист інформаційних активів від зовнішніх та внутрішніх навмисних та ненавмисних загроз. Політика розповсюджується на всі аспекти діяльності ІС та застосовується до всіх інформаційних активів, які можуть справляти матеріальний інтерес для кримінальних структур у разі несанкціонованого витоку.

Як основні об'єкти області діяльності інформаційної безпеки, розглядаються наступні види активів:

- **інформаційні активи:** інформація та дані у довільному вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, (до цього виду необхідно віднести знання працівників, бази даних та системи біометричного ідентифікування, документація, навчальні матеріали, описи процедур, інформація на фізичних носіях);
- **програмне забезпечення:** прикладне програмне забезпечення, системне програмне забезпечення, сервісне програмне забезпечення та довільне інше програмне забезпечення, незалежно від форми отримання (придбання, власного розроблення, таке, що вільно розповсюджується), яке використовується працівниками для роботи та у процесі взаємодії з іншими службами;
- **фізичні активи:** працівники, апаратні засоби ІТ (КМ і мережеві технології, сервери, робочі станції, міжмережеві екрани, телекомунікаційне обладнання, обладнання зв'язку, маршрутизатори, АТС), приміщення, виробниче обладнання, технічні засоби;
- **сервісні активи:** інформаційні та комунікаційні сервіси (корпоративні КМ спеціального призначення, Internet, E-mail, спеціальні канали зв'язку), інші технічні сервіси (опалення, освітлення, системи сигналізацій та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передавання та знищенням активів, усі юридичні та фізичні особи, організації, установи та підприємства (а також їх працівники), яким передані певні послуги на ІТ-утсорсинг.

Для кожного активу визначаються можливі ризики та шляхи їх мінімізування, тобто рекомендуємо використати ризик-орієнтований підхід. Оцінювання можливих ризиків активів провадиться за чотирма основними критеріями безпеки:

- **доступність** – забезпечення безперервного доступу до інформаційних та супутніх активів ІС, спеціальних КМ та сервісів згідно з наданими працівникам повноваженнями та правами у мінімально необхідному обсязі;
- **цілісність** – захист точності/коректності та повноти активів і методів оброблення інформації;
- **конфіденційність** – забезпечення доступності до ІС, спеціальних КМ, інформації, активів тільки для офіційно авторизованих працівників та користувачів у мінімально необхідному обсязі.

- **спостережливість** – забезпечення можливості визначення – хто, що і коли робив з тим або іншим інформаційним активом (забезпечення принципу невідмови від вчинених дій).

Політика регламентує управління доступами та паролями, чітке розподілення ролей та обов'язків, визначення вимог інформаційної безпеки для кожного активу. Впровадження ПІБ в ІС забезпечує підтримку рівня безпеки на належному рівні, що свою чергу передбачає:

- постійне навчання працівників у сфері ІБ;
- проведення контролю безпеки та доступу до ІС;
- управління інцидентами, класифікування та забезпечення конфіденційності інформації;
- антивірусний захист, резервне копіювання, ліцензійну чистоту програмного забезпечення, вхідний/вихідний контроль за обміном інформацією у ІС;
- забезпечення фізичної безпеки та інших аспектів інформаційної безпеки.

Документи ПІБ розробляються підрозділом безпеки ІТ. Постійний контроль впровадження, виконання, вдосконалення та підтримки ПІБ в актуальному стані також лежить на плечах працівників підрозділу безпеки інформаційних технологій. Документи ПІБ доступні працівникам у межах їх повноважень і призначені допомагати у її впровадженні та виконанні.

Для зменшення ризиків виникнення інцидентів інформаційної безпеки, пов'язаних з зовнішніми і внутрішніми навмисними та ненавмисними впливами, елементарною необізнаністю працівників необхідно розробити та запровадити систему управління інцидентами інформаційної безпеки, яка є базовою частиною загальної системи управління інформаційною безпекою (СМІБ). СМІБ дозволяє виявляти, враховувати, реагувати й аналізувати події та інциденти ІБ. Без реалізування цих процесів неможливо забезпечити рівень захищеності, який є адекватним вимогам сучасних стандартів і галузевих норм.

Управління інцидентами, це важливий процес, який забезпечує можливість спочатку виявити інцидент, а потім за допомогою коректно обраних засобів підтримки якомога швидше його вирішити.

Основна задача управління інцидентами – якомога швидше відновити нормальну роботу служб і звести до мінімуму негативний вплив інциденту на роботу ІС для підтримки якості і доступності служб на максимально можливому рівні. Нормальною вважається робота служб, що не виходить за рамки угоди про рівень обслуговування.

Цілі, які ставлять перед СУІБ є такими:

- відновлення нормальної роботи служб у найкоротші терміни;
- зведення до мінімуму впливу інцидентів на функціонування ІС;
- забезпечення злагодженого оброблення всіх інцидентів і запитів обслуговування;
- зосередження ресурсів підтримки на найбільш важливих напрямах;
- надання відомостей, які дозволять оптимізувати процеси підтримки, зменшити кількість інцидентів і запланувати управління.

Використовуючи найкращі, перевірені часом напрацювання і вирівнювання ІТ-процесів для оброблення збоїв довільних видів, рішення з управління інцидентами дозволяють використовувати ресурси залежно від пріоритетів оперативної діяльності, управляти рівнями обслуговування, а також краще контролювати роботу ІТ-служб.

Для реалізування системи управління інцидентами інформаційної безпеки СУІБ необхідно виконати такі роботи:

- надати ресурси для розроблення та впровадження системи СУІБ;
- здійснити фахову підготованість працівників;
- визначити область функціонування системи управління інцидентами;
- розробити комплекс процесів СУІБ;
- впровадити процеси СУІБ та інтегрувати їх з уже функціонуючими процесами, такими як інвентаризування активів, аналіз ризиків та оцінювання ефективності;
- розробити архітектуру і комплекс програмно-технічних засобів з автоматизації процесів СУІБ і моніторингу подій.

У результаті проведених робіт буде запроваджена СУІБ, яка буде розв’язувати наступні задачі:

- оперативний моніторинг стану інформаційної безпеки в рамках функціонування ІС;
- виявлення, облік, реагування, розслідування та аналіз інцидентів Б;
- інформування вищого керівництва про поточний стан ІБ.

Таким чином, необхідно реалізувати комплексний підхід щодо розв’язання наступних задач:

- виявлення, інформування та облік інцидентів ІБ;
- реакція на інциденти ІБ, включаючи застосування необхідних засобів для запобігання, зменшення і відновлення завданого збитку;
- аналіз реалізованих інцидентів, з метою планування превентивних заходів захисту і поліпшення процесу забезпечення ІБ в цілому.

Для оброблення подій та інцидентів інформаційної безпеки необхідно організувати процес реагування на інциденти. Основними задачами процесу реагування на інциденти ІБ є:

- забезпечення координації реагування на інцидент;
- підтвердження/спростування факту виникнення інциденту;
- забезпечення збереження і цілісності доказів виникнення інциденту, створення умов для накопичення і зберігання точної інформації про інциденти, що мали місце, про корисні настанови;
- мінімізування порушень порядку роботи і пошкодження даних, відновлення в найкоротші терміни працездатності ІС при її порушенні у результаті інциденту;
- мінімізування наслідків порушення конфіденційності, цілісності і доступності інформації у ІС;
- створення умов для порушення цивільної або кримінальної справи проти зловмисників;

- захист активів ІС;
- швидке виявлення та/або попередження подібних інцидентів в майбутньому.

Також слід відзначити, що при експлуатуванні СМІБ процес управління інцидентами є одним з найважливіших у постачанні даних для аналізу функціонування таких систем, оцінювання ефективності використовуваних заходів, зниження ризиків і планування удосконалення роботи ІС.

6.7. Політика безпеки інформації Web-порталу підприємства

Політика безпеки інформації в ІС повинна поширюватися на ОІД, які безпосередньо або опосередковано впливають на БІ.

До таких об’єктів належать:

- адміністратор безпеки та працівники служби ЗІ;
- користувачі, яким надано повноваження забезпечувати управління ІС;
- користувачі, яким надано право доступу до загальнодоступної інформації;
- інформаційні об’єкти, які містять загальнодоступну інформацію;
- системне та функціональне ПЗ, яке використовується в ІС для оброблення інформації;
- технологічна інформація КСЗІ (дані про мережеві адреси, імена, персональні ідентифікатори та паролі користувачів, їхні повноваження та права доступу до об’єктів, встановлені робочі параметри окремих механізмів або засобів захисту, інша інформація баз даних захисту, інформація журналів реєстрації дій користувачів тощо);
- засоби адміністрування і управління ІС та технологічна інформація, яка при цьому використовується;
- обчислювальні ресурси ІС (наприклад, дисковий простір, тривалість сеансу роботи користувача із засобами ІС, час використання центрального процесора тощо), безконтрольне використання або захоплення яких окремим користувачем може призвести до блокування роботи інших користувачів, компонентів ІС або ІС в цілому.

З урахуванням особливостей надання доступу до інформаційних активів Web-порталу, типових характеристик середовищ функціонування та особливостей технологічних процесів оброблення інформації визначаються наступні мінімально необхідні рівні послуг безпеки для забезпечення захисту інформації від загроз:

- за умови, коли Web-сервер і робочі станції розміщуються на території власника Web-порталу або на території оператора (технологія Т1);
- за умови, коли Web-сервер розміщується у оператора, а робочі станції – на території власника Web-порталу, взаємодія яких з Web-сервером здійснюється з використанням мереж передавання даних (технологія Т2).

Технологія Т1 відрізняється від технології Т2 способом передавання інформації від робочої станції до Web-сервера, а саме: наявністю у другому випадку незахищеного середовища, яке не контролюється, і додатковими вимогами щодо ідентифікування та автентифікування між засобами захисту

робочої станції і Web-сервера під час спроби розпочати обмін інформацією та забезпечення цілісності інформації при обміні.

6.8. Захист Web-сторінки регулярними засобами операційної системи Windows

При роботі у мережі Internet користувачеві необхідно потурбуватися про те, аби трансмісія даних, особливо інформація конфіденційного та службового характеру, були захищеними від НСД. З іншого боку, проблема безпеки даних постає при трансмісії файлів і програм між Web-вузлами і Вашою WS. Без вживання системи ЗІ Ви можете отримати програму, яка при активуванні пошкодить дані, що зберігаються на WS.У процесі написання цього розділу використано опис ПЗ (OpenSource).

Ступінь надійності Web-вузлів у Internet різна. Програма Internet Explorer дозволяє розподіляти отримувані Вами дані мережею за зонами безпеки і встановлювати різні рівні захисту залежно від того, хто є їх надсилачем. Перед завантаженням Web-сторінки Internet Explorer перевіряє відповідність вузла заданій зоні безпеки. Для того, щоб дізнатися, до якої зони безпеки відноситься завантажена Web-сторінка, погляньте на рядок стану. У його правій частині розміщується назва зони.

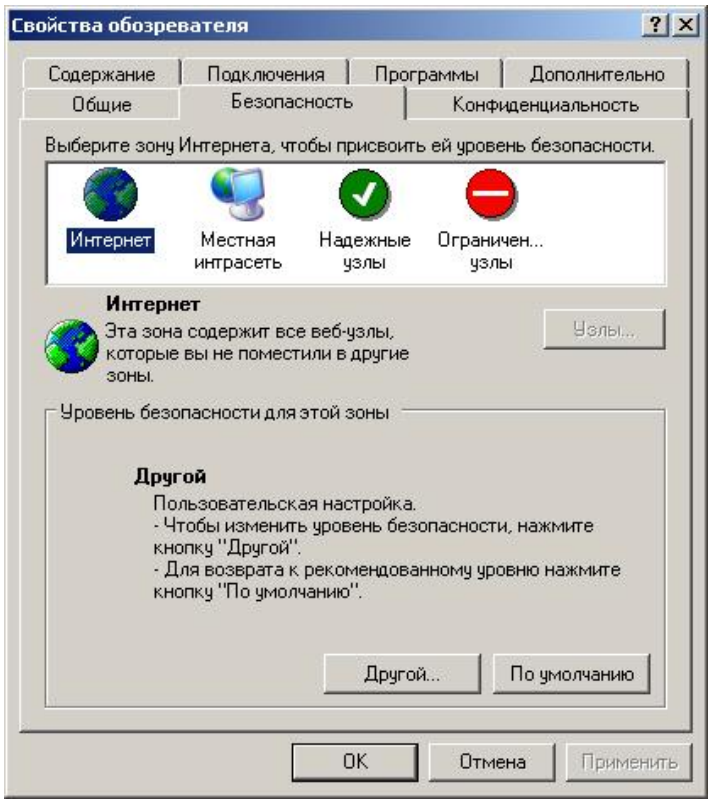


Рис. 6.1. Вкладка Властивості оглядача, яка призначена для налаштування параметрів безпеки

Використовуючи вкладку Безпека (рис. 6.1) діалогового вікна Властивості оглядача можна встановити для зон Internet різні параметри безпеки. У верхній частині вкладки розташований поданий у вигляді значків перелік основних категорій зон, на які є доступ з комп'ютера користувача (табл. 6.1).

Таблиця 6.1.

Основні категорії зон безпеки

Зона	Призначення
Internet	До цієї зони входить все те, що не має відношення до вашого комп'ютера, внутрішньої мережі або іншої зони. За замовчуванням зона володіє середнім рівнем захисту.
Місцева Intranet	Дана зона містить адреси, для яких використання проксі-сервера не обов'язкове. Ці адреси призначаються системним адміністратором за допомогою адміністративного комплекту Internet Explorer (IEAK). За замовчуванням зона має рівень захисту нижчий від середнього.
Надійні вузли	Зона містить вузли, яким ви довіряєте і з яких можна завантажувати інформацію і програми, не турбуючись про можливе пошкодження ваших власних даних або комп'ютера. За замовчуванням ця зона має низький рівень захисту.
Обмежені вузли	Зона містить вузли, яким Ви не довіряєте. За замовчуванням ця зона має високий ступінь ризику.

На вкладці міститься повзунок, використовуваний для завдання рівня безпеки зони, вибраної з верхнього списку (таблиця. 6.2).

Таблиця. 6.2.

Рівні безпеки

Рівень безпеки	Виконувана програмою дія
Високий	При загрозі безпеці з Web-вузла видається повідомлення. Інформація, яка може нести загрозу безпеці, не завантажується. Небезпечні функції відмикаються.
Середній	Перед завантаженням небезпечного вмісту з Web-вузла видається повідомлення. Після попередження подається запит на підтвердження або скасування завантаження активного вмісту.
Нижчий від середнього	Велика частина вмісту запускається без попередження. При загрозі безпеці з Web-вузла видається повідомлення.
Низький	Мінімальний рівень безпеки. За потенційної загрози безпеці з Web-вузла видається повідомлення, після чого активний вміст завантажується на комп'ютер.

Вкладка Безпека діалогового вікна Властивості оглядача містить клавіші, перераховані у табл. 6.3.

Таблиця 6.3.

Призначення кнопок вкладки Безпека

Клавіша	Призначення
Вузли	Дозволяє додати або видалити вузол із заданої зони.

За замовчуванням	Дозволяє для обраної зони встановити рівень захисту, прийнятий за замовчуванням.
Інший	Відкриває діалогове вікно Правила безпеки для визначення додаткових налаштувань захисту.

Параметри вкладки Вміст

Вкладка Вміст (рис. 6.2) діалогового вікна Властивості оглядача містить три області, які мають таке призначення:

- Обмеження доступу – дозволяє ввести обмеження на переглядання інформації у Internet;
- Сертифікати – призначена для переглядання особистих сертифікатів безпеки, встановлених на даній WS, сертифікатів вузлів і видавців;
- Особисті дані – зберігає персональні дані, які надаються вузлам при запитах.

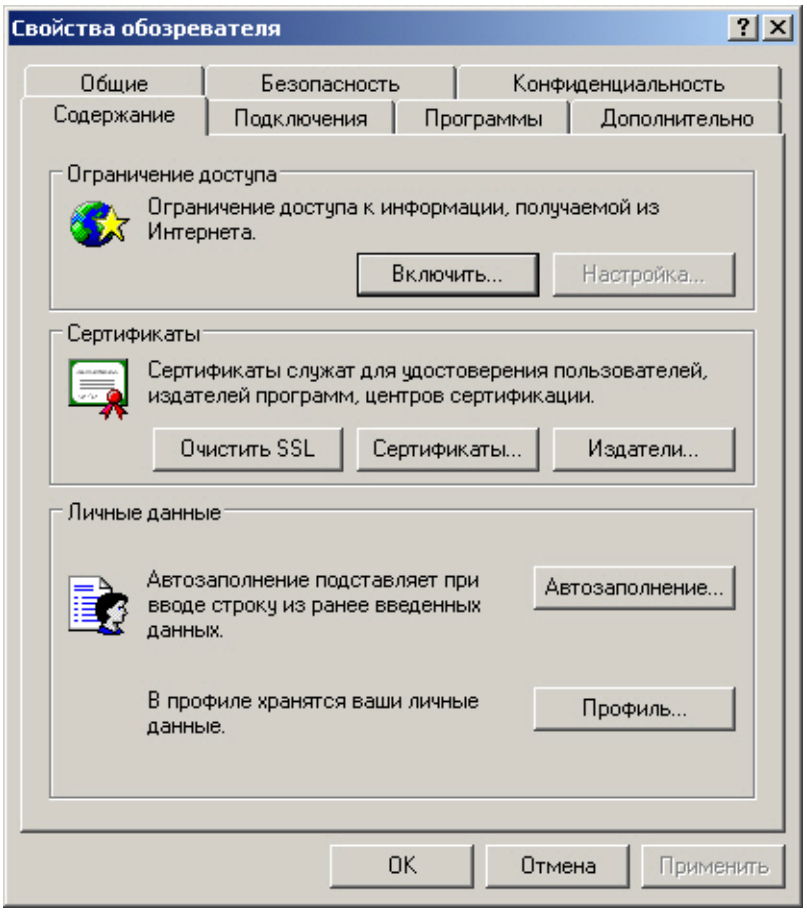


Рис. 6.2. Вкладка Вміст

Налаштування Internet Explorer

Ви можете змінити налаштування та параметри у програмі Internet Explorer, щоб захистити конфіденційність користувача, покращити безпеку WS або полегшити роботу у броузері. Нижче подані корисні посилання щодо змінення налаштувань у програмі Internet Explorer, зокрема,. Встановлення спеціальних або прийнятих за замовчуванням рівнів безпеки для Internet, Intranet та окремих Web-сайтів.

Область містить клавішу Увімкнути при натисненні на яку відкривається діалогове вікно Обмеження доступу (рис. 6.3), яке містить чотири вкладки:

- Оцінки;
- Дозволені вузли;
- Загальні;
- Додатково.

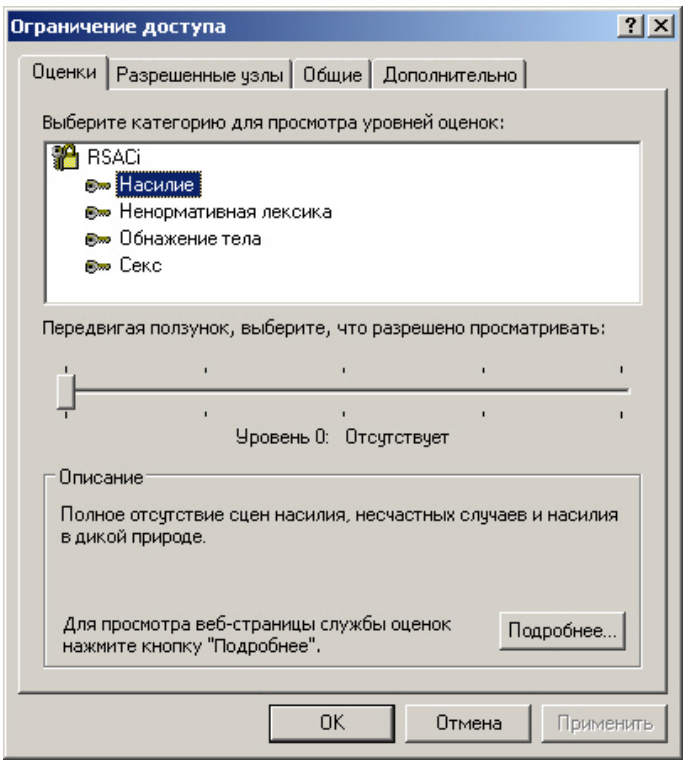


Рис. 6.3. Діалогове вікно Обмеження доступу, використовуване для обмеження доступу до інформації

У верхній частині вкладки Оцінки розташований список розділів, на які можна задати обмеження, а нижче за нього – повзунок, який вказує на рівень обмеження. Для зміни рівня заборони на перегляд інформації виберіть із списку категорію, що налаштовується. При цьому в розділі Опис вкладки відтворюється інформація про встановлений рівень заборони для даного розділу. Переміщаючи повзунок – змініте встановлений рівень доступності матеріалів даної категорії.

Вкладка Дозволені вузли дозволяє сформувати список вузлів, які можна переглядати або, навпаки, не переглядати, не дивлячись на параметри, встановлені на вкладці Оцінки.

Прапорець Користувачі можуть переглядати вузли, що не мають оцінок вкладки Загальні визначає дозвіл на перегляд вузлів, які не мають оцінки, для користувачів даної WS. При встановленні цього прапорця користувач дістає доступ до небажаного матеріалу, якщо рейтинг Web-сторінки не визначений. Якщо цей прапорець не встановлений, користувач не матиме доступу до Web-сторінок, які не мають оцінки, навіть якщо вони не містять небажаного матеріалу.

Встановлений прапорець Дозволити введення пароля для перегляду заборонених вузлів вкладки Загальні дозволяє переглядати заборонену для перегляду інформацію Web-сторінок після введення пароля.

Налаштування під'єднання до Internet. Вкладка Під'єднання (рис. 6.4) діалогового вікна Властивості оглядача дозволяє налаштувати параметри віддаленого доступу.

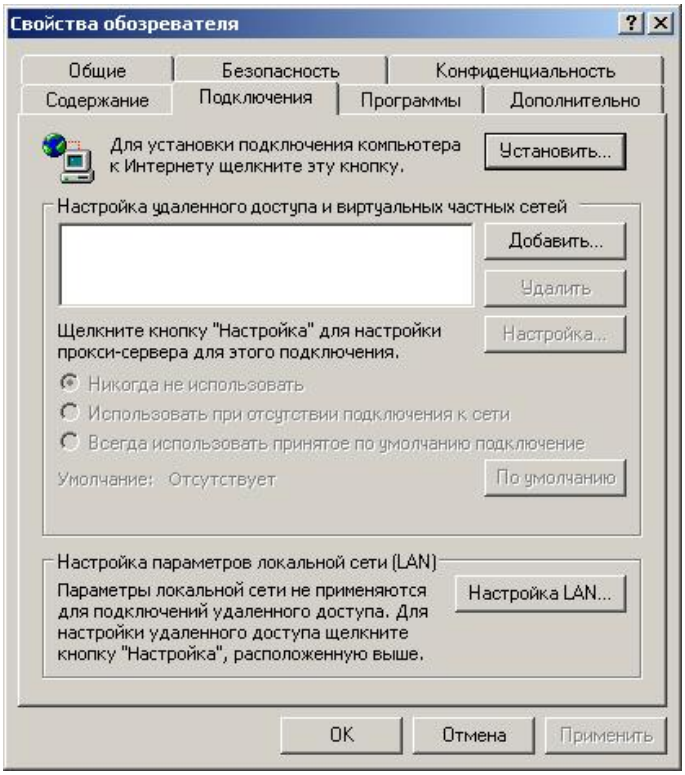


Рис. 6.4. Вкладка, призначена для налаштування з'єднання з Internet

У верхній частині вкладки знаходиться клавіша Встановити при натисненні на неї активується Майстер під'єднання до Internet, який допоможе встановити з'єднання. Розташовані нижче перемикач і клавіша Налаштування дозволяють здійснити самостійне налаштування параметрів з'єднання.

У області Налаштування віддаленого доступу знаходиться список з'єднань для віддаленого доступу до мережі, встановлених на WS, і три клавіші:

- Додати – додає до списку за допомогою майстра нове з'єднання для віддаленого доступу до мережі;
- Видалити – видаляє із списку відзначене з'єднання з Internet;
- Налаштування – відкриває діалогове вікно Налаштування, яке дозволяє переглянути і змінити налаштування долученого вибраного з'єднання.

Встановлена під списком опція Не використовувати вказує на необхідність при з'єднанні з Internet вибирати використовуване з'єднання вручну.

Опція Використовувати за відсутності з'єднанні з мережею Internet вказує, що для входу в Internet за відсутності з'єднання програма Internet Explorer використовуватиме з'єднання для віддаленого доступу до мережі Internet, прийняте за замовчуванням.

Встановивши розташовану під списком опцію Завжди використовувати прийняті за замовчуванням з використанням клавіші За замовчуванням можна вказати, нові з'єднання використовувані за замовчуванням при з'єднанні з Internet.

Область Налаштування локальної мережі дозволяє здійснити з'єднання з Internet через Proxy-сервер локальної мережі, який служить захисним бар'єром між внутрішньою мережею і Internet, не дозволяючи іншим користувачам Internet дістати доступ до конфіденційної інформації внутрішньої мережі.

Налаштування з'єднання. Для створення з'єднання для віддаленого доступу до мережі Internet, виберіть його зі списку з'єднань на вкладці З'єднання і натискуйте клавішу Налаштування. Відкриється однойменне діалогове вікно (рис. 6.5), призначене для перегляду і зміни параметрів. У його верхній частині розташовано два прапорці:

Автоматичне визначення налаштувань – при встановленні прапорця здійснюється автоматичне визначення налаштувань Proxy-сервера або параметрів автоматичного налаштування, використовуваних для з'єднання з Internet і налаштування оглядача Internet Explorer.

Використовувати сценарій автоматичного налаштування – при встановленні прапорця для автоматичного налаштування використовується файл, який містить параметри налаштування, надані системним адміністратором.

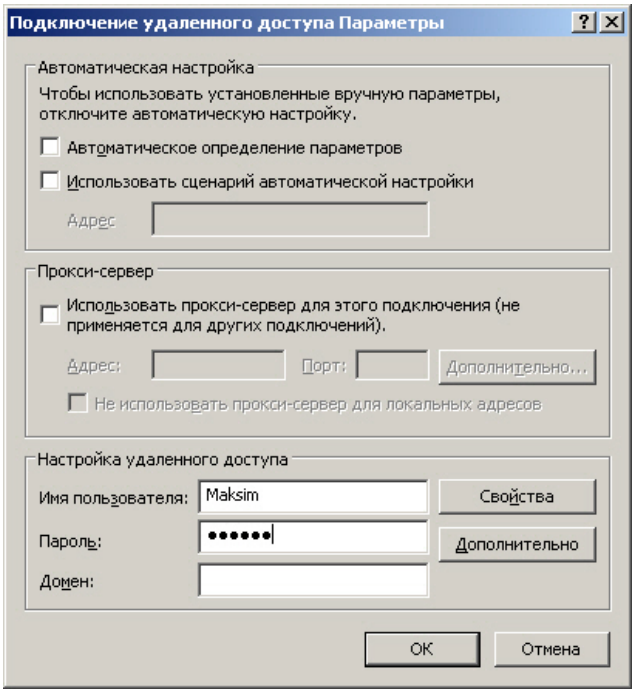


Рис. 6.5. Діалогове вікно, призначене для налаштування з'єднання

При встановленні прапорця Використовувати сценарій автоматичного налаштування стає доступним для введення інформації поле Адреси, призначене для задання адреси або імені файлу, використовуваного для налаштування Internet Explorer

Розділ Proxy-сервер дозволяє здійснити під'єднання до Internet через Proxy-сервер локальної мережі. При встановленні прапорця Використовувати Proxy-сервер для цього під'єднання стають доступними для введення наступні поля:

- Адреса – адреси Proxy-сервера, що надаються системним адміністратором мережі;
- Порт – порт Proxy-сервера, використовуваний для доступу до Internet.

При під'єднанні до Internet через Proxy-сервер локальної мережі необхідно здійснити додаткові налаштування Proxy-сервера. Для цього натискуйте клавішу Додатково. Відкриється діалогове вікно Параметри Proxy-сервера біля якого необхідно ввести адреси і порт Proxy-сервера, використовуваного для доступу до Internet після протоколів HTTP, Secure, FTP, Gopher і Socks.

Для налаштування віддаленого доступу призначений розділ Налаштування віддаленого доступу діалогового вікна Під'єднання віддаленого доступу Параметри. Він містить поля, у які потрібно ввести дані, надані провайдером:

- Ім'я користувача – ім'я користувача;
- Пароль – пароль;
- Домен – ім'я домена.

Натиснення клавіші Властивості цього розділу відкриває вікно, призначене для зміни номера телефону, модему і інших додаткових параметрів поточного з'єднання віддаленого доступу до мережі.

Формування списку використовуваних програм. Використовуючи вкладку Програми (рис. 6.6) діалогового вікна Властивості оглядача можна задати вживані разом з Internet Explorer програми:

- редактора HTML – для редагування HTML-файлів;
- електронної пошти – для роботи з електронною поштою;
- груп новин – для читання груп новин Internet;
- викликів через Internet – для набору номера;
- календаря – для переглядання календаря;
- адресної книги – для роботи з адресною книгою.

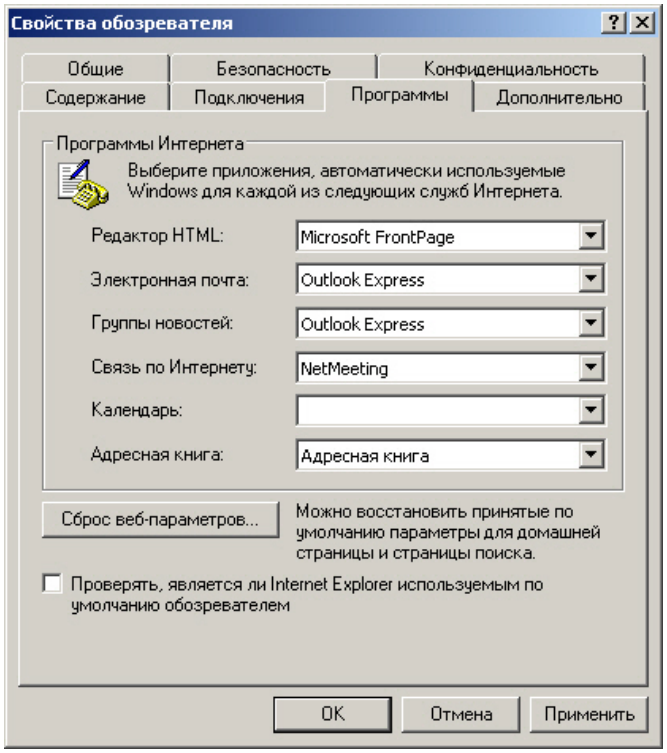


Рис. 6.6. Вкладка Програми, яка дозволяє задати перелік використовуваних програм

При встановленні прапорця Перевіряти, чи є Internet Explorer оглядачем, який використовується за замовчуванням при кожному запуску Internet Explorer виконує перевірку, чи зареєстрований Internet Explorer, як засіб перегляду Internet, використовуваного за замовчуванням. Якщо зареєстрована інша програма, буде запропоновано відновити вживання Internet Explorer як стандартного засобу перегляду інформації в Internet.

Додаткові налаштування оглядача. Для додаткових налаштувань оглядача використовується вкладка Додатково (рис. 6.7) діалогового вікна Властивості оглядача, що містить великий список параметрів, згрупованих у розділи. Для їх активування досить встановити прапорець або одну з пропонованих опцій.

Аби відновити значення, встановлені у системі за замовчуванням, натискуйте клавішу Відновити значення за замовчуванням.

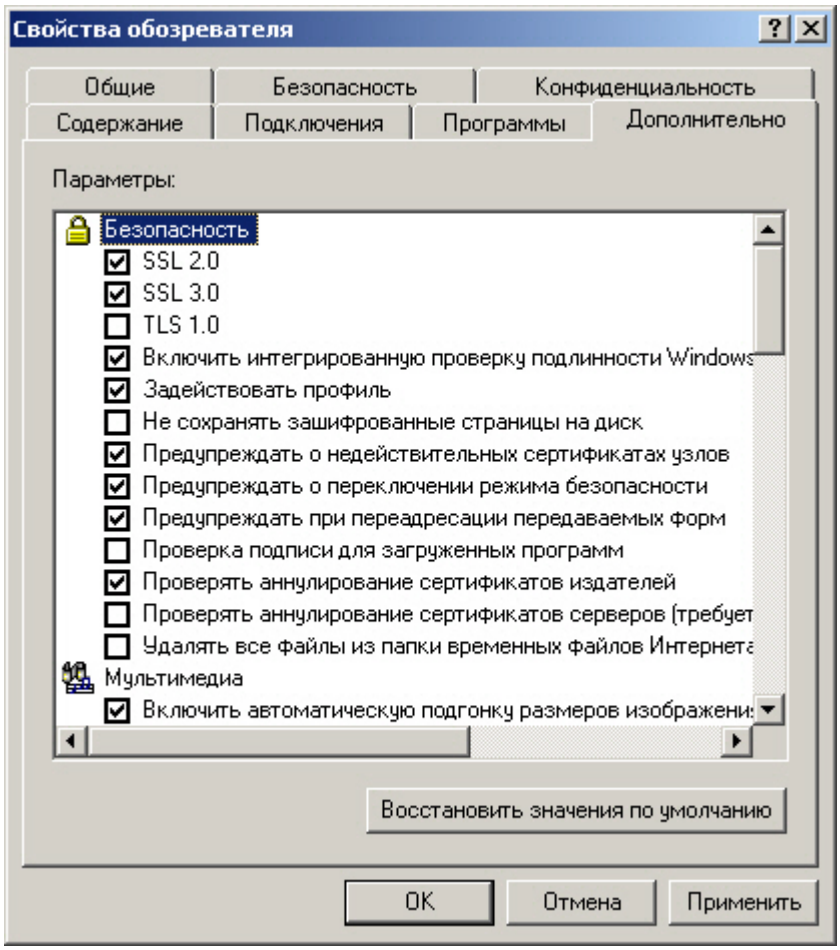


Рис. 6.7. Вкладка налаштування додаткових параметрів оглядача

ЛЕКЦІЯ 7.

ЗАХИСТ СЛУЖБОВИХ ДОКУМЕНТІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

План

ВСТУП

Інформація, яка використовується підприємцем у бізнесі та управлінні підприємством, банком, компанією або іншою комерційною структурою, є його власною або приватною інформацією, яка становить істотну цінність для підприємця. Ця інформація є його інтелектуальною власністю.

Власна інформація підприємця, з метою її захисту, може бути віднесена до комерційної таємниці та носить конфіденційний характер за дотримання таких умов: інформація не повинна відтворювати негативні сторони діяльності підприємства, порушення законодавства та інші подібні факти; інформація не повинна бути загальнодоступною або загальновідомою; виникнення або отримання інформації повинно нести законний характер; персонал підприємства зобов'язаний знати про цінність такої інформації та повинен бути навчений правилам роботи з нею; підприємцем повинні бути виконані дії з захисту цієї інформації.

Отже, власна цінна інформація підприємця не обов'язково є конфіденційною. Доволі часто звичайний правовий документ важливо зберегти в цілісності та безпеці від викрадача або стихійного лиха.

Цінну ділову інформацію, як правило, містять: плани розвитку виробництва, ділові плани, плани маркетингу, бізнес-плани, списки власників акцій та інші документи.

Найцінніші відомості про виробництво і продукцію, ринок, наукові розробки, матеріально-технічне забезпечення, умови контрактних перемовин, відомості про персонал, принципи управління підприємством, організацією, систему безпеки підприємства тощо. Комерційна цінність інформації, як правило, недовготривала і визначається часом, необхідним конкуренту для створення тієї ж ідеї або її викрадення та відтворення.

Ступінь цінності інформації та необхідна надійність її захисту знаходяться у прямій залежності. Закордонні підприємства з метою підвищення свого престижу та конкурентоспроможності товарів використовують різні рекламні прийоми і, зокрема, створюють неіснуючі секрети. Виявлення та регламентування реального складу інформації, яка є цінною для підприємця і підлягає захисту, становить основоположну частину системи захисту.

7.1. Гриф обмеження доступу до документа

Склад цінної інформації визначається її власником і фіксується у спеціальному переліку. Перелік цінних відомостей, які складають таємницю підприємства, є постійним робочим матеріалом керівництва підприємства, служб безпеки та службової документації (СД). Він регулярно оновлюється, коректується та становить інвентарний перелік відомостей про конкретні роботи, продукцію, дослідження, контракти тощо. До переліку включаються дійсно цінні відомості про роботу підприємства, хоча певна номенклатура типових відомостей у переліку може міститися.

У кожній позиції переліку рекомендується вказувати гриф конфіденційності інформації, прізвища працівників, які мають право доступу до них і які несуть відповідальність за їх зберігання, термін дії грифу або найменування події, яка знімає це обмеження, види документів та баз даних, в яких ці відомості фіксуються і зберігаються. Важливим завданням переліку є подрібнення комерційної таємниці на окремі інформаційні елементи, відомі різним особам.

На основі переліку відомостей складається і ведеться перелік документів підприємства, які підлягають захисту і мають відповідний гриф обмеження доступу. Під *службовим документом*, тобто документом, до якого обмежений доступ персоналу, треба розуміти необхідним чином оформлений носій цінної задокументованої інформації, яка складає інтелектуальну власність підприємця.

Особливість СД полягає у тому, що він є одночасно масовим носієм захищеної інформації, основним джерелом накопичення та розповсюдження цієї інформації, в тому числі її розголошення (витоку) і обов'язковим об'єктом захисту. Конфіденційний характер включеної у документ інформації позначається грифом обмеження доступу до документа, який ініціює виокремлення його з загального потоку і оброблення в спеціальному автономному режимі, а також поширює на документ захисні та інші заходи підвищеної уваги та контролю.

Гриф обмеження доступу до документа є службовою позначкою (реквізитом), яка проставляється на носії службової інформації або супровідному документі. Інформація і документи, віднесені до підприємницької таємниці, мають декілька рівнів грифів обмеження доступу, відповідно до різних ступенів конфіденційності інформації: перший, найнижчий і масовий рівень – грифи ″Комерційна таємниця″, ″Конфіденційно″, ″Службова інформація″; другий рівень – ″Комерційна таємниця. Суворо конфіденційно″, ″Суворо конфіденційно″, ″Суворо службова інформація″, ″Конфіденційно – Особливий контроль″.

У практичній діяльності може використовуватися однорівнева система грифування (грифів тільки першого рівня) або, інколи, трирівнева, за якої вводиться вищий за значенням гриф – ″Комерційна таємниця особливої важливості″. Під означенням грифу завжди вказується номер примірника документа, термін дії грифу або інші умови його зняття, а також позначки типу – ″Особисто″, ″Тільки адресатові″ тощо. Гриф конфіденційності присвоюється документу: виконавцем на стадії підготовки проекту документа; керівником структурного підрозділу або керівником підприємства на стадії узгодження або підписання документу; дресатом (отримувачем) документу на стадії його первинної оброблення у службі службової документації (ССД).

Зміна грифу конфіденційності документа проводиться при зміні ступеня конфіденційності відомостей, які містяться у ньому. *Підставою для зміни або зняття грифу конфіденційності є*: відповідне коректування переліку службових відомостей або СД підприємства; закінчення встановленого терміну дії грифу; наявність події, за якої гриф повинен бути змінений або знятий (наприклад, закінчення дії контракту, вимога замовника продукції, опублікування опису виробу в пресі, патентування винаходу).

Отже, довільна підприємницька діяльність завжди пов'язана зі створенням, використанням та зберіганням значних обсягів інформації та документів, які є цінними для підприємства та підлягають обов'язковому захисту від різного виду загроз. З цією метою на носії інформації позначається гриф обмеження доступу, який відносить цей носій до категорії захищених СД та ініціює застосування у відношенні до нього системи захисних заходів.

7.2. Джерела службової інформації та канали її витоку

Джерелом цінної, службової документованої інформації є накопичувачі (концентратори) цієї інформації. До числа основних видів джерел СІ відносять: персонал підприємства і дотичні до підприємства люди; документи; публікації про фірму та її розробки, рекламні видання, виставкові матеріали; фізичні поля, ПЕМВН, що супроводжує роботу офісної техніки, різних приладів і обладнання.

Документація, як джерело цінної підприємницької інформації включає: СД, яка містить підприємницьку таємницю; цінну правову, установчу, організаційну та розпорядчу документацію; службову, поточну ділову і науково-технічну документацію, яка містить загальновідомі відомості; робочі записи працівників, їх службові щоденники, особисті робочі плани, переписку з комерційних та наукових питань; особисті архіви працівників підприємства.

Інформація завжди розповсюджується від джерела у зовнішнє середовище. Канали розповсюдження інформації носять об'єктивний характер, відрізняються активністю і включають у себе: ділові, управлінські, торгові, наукові та інші комунікативні регламентовані зв'язки; інформаційні мережі; технічні канали.

Збільшення кількості каналів розповсюдження інформації породжує розширення складу джерел цінної інформації. Джерела і канали розповсюдження інформації за певних умов можуть стати об'єктом уваги конкурентів, що створює потенційну загрозу збереження і цілісності інформації. Загроза безпеці інформації передбачає НСД конкурента або найманого ним зловмисника до СІ і, як результат цього, – крадіжку, знищення, фальсифікування, модифікування, підміну документів. За відсутності інтересу конкурента загроза цілісності інформації не виникає навіть у тому випадку, якщо створились передумови для ознайомлення з нею сторонніх осіб.

Цінна інформація, до якої не проявляють цікавість конкуренти, може не включатися до складу такої інформації, яка захищається, а документи, що містять її, контролюються тільки з метою забезпечення збереження носія. Конкурент або інша зацікавлена особа (далі за текстом – зловмисник) створює загрозу інформації шляхом встановлення контакту з джерелом інформації або перетворення каналу розповсюдження інформації в канал її витоку.

Зловмисник може створювати уявну загрозу, на протидію якій будуть витрачені реальні сили та засоби. Загрози інформації реалізовуються зловмисником за допомогою прийомів і методів промислового або економічного шпіонажу. Загроза збереженню інформації та документів особливо велика при її виході за межі ССД, наприклад, при передаванні документів персоналу на розгляд та виконання, при пересиланні або передаванні документів адресатам. Однак, необхідно враховувати, що втрата СІ відбувається, як правило, не в результаті навмисних дій конкурента або зловмисника, а через неуважність, непрофесіоналізм і безвідповідальність персоналу.

Втрата (витік) інформації передбачає несанкціонований перехід цінних, службових відомостей до особи, яка не має права володіти нею і використовувати її в своїх цілях для отримання прибутку. У тому випадку, коли мова йде про втрату інформації з вини персоналу, зазвичай, використовується термін ″розголошення інформації″.

Розголошує інформацію завжди людина – усно, письмово, за допомогою жестів, міміки, умовних сигналів, особисто або через посередника. Термін ″витік інформації″ використовується найбільш широко, хоча, на наш погляд, більшою мірою відноситься до втрати інформації за рахунок її перехоплення технічними засобами розвідки. При розголошенні, витоку інформація може переходити до зловмисника, а потім, можливо, до конкурента або до третьої особи. Під третьою особою, в даному випадку, розуміють осіб, які отримали інформацію у володіння в силу обставин (тобто які стали її джерелом), але які не мають права володіння нею і, що дуже важливо, не зацікавлені в цій інформації.

Однак, необхідно враховувати, що від третіх осіб інформація може перейти до зацікавленої особи – конкурента підприємства. Перехід інформації до третьої особи можна назвати ненавмисним, стихійним. *Перехід інформації виникає в результаті*: втрати або випадкового знищення документа, пакета (конверта); невиконання, незнання або ігнорування працівником вимог з ЗІ; надмірної балакучості працівників у присутності зловмисника; роботи з КД при сторонніх особах, несанкціонованому передаванні СД іншому працівнику; використання СІ у пресі, особистих записах, приватних листах; самовільного копіювання документів працівником.

На відміну від третьої особи зловмисник навмисно й таємно організовує, створює канал витоку інформації та експлуатує його тривалий час. *Знати можливий канал витоку інформації означає*: для зловмисника – мати стабільну можливість отримувати цінну інформацію; для власника інформації – протидіяти зловмиснику та зберігати таємницю, а, інколи, і дезінформувати конкурентів. Інформація повинна поступати до конкурента тільки каналом, який контролюється, у якому відсутні конфіденційні відомості, а інформація є загальнодоступною. Прикладом такого каналу є видання та розповсюдження рекламно-інформаційних матеріалів.

Канали витоку, якими користуються зловмисники, вирізняються різноманітністю. *Основними видами каналів витоку інформації можуть бути*: встановлення зловмисником взаємовідносин з працівниками підприємства або відвідувачами, працівниками фірм-партнерів, службовцями державних або муніципаль-

них органів управління та іншими особами; аналіз опублікованих матеріалів про фірму, рекламних видань, виставкових проспектів та іншої загальнодоступної інформації; влаштування зловмисника на роботу в фірму; робота у КМ; кримінальний, силовий доступ до інформації, тобто викрадення СД, шантаж персоналу та інші способи; робота зловмисника з технічними каналами витоку інформації.

Виявлення каналу розголошення (витоку) інформації – складна, довготривала і трудомістка задача. В основі її розв'язання лежить класифікація та постійне вивчення джерел і каналів розповсюдження інформації та можливих каналів її витоку, пошук і виявлення реальних каналів витоку, оцінювання ступеня небезпеки кожного реального каналу, придушення небезпечних каналів і аналіз ефективності захисних заходів. Канали розголошення (витоку) інформації завжди індивідуальні і залежать від конкретних задач, поставлених перед зловмисником.

Отже, контроль джерел і каналів розповсюдження СІ дозволяє визначити наявність і характеристику загроз інформації, виробити структуру системи ЗІ, яка надійно перекриє доступ зловмиснику до СІ підприємства.

7.3. Система захисту службових документів

Система ЗІ є комплексом організаційних, технічних і технологічних засобів, методів і заходів, які перешкоджають НСД до інформації. Власник інформації особисто визначає не тільки склад СІ, яка підлягає захисту, але й відповідні способи та засоби захисту.

Одночасно ним розробляються заходи матеріального і морального стимулювання працівників, які дотримуються порядку захисту СІ, і заходи відповідальності персоналу за розголошення таємниці підприємства.

Система ЗІ повинна бути багаторівневою з ієрархічним доступом до інформації, гранично конкретизованою і прив'язаною до специфіки підприємства за структурою методів та засобів захисту, які використовуються, відкритою для регулярного оновлення, надійної як у звичайних, так і в екстремальних ситуаціях. Вона не повинна створювати працівникам підприємства поважні незручності в роботі. Комплексність системи ЗІ досягається її формуванням з різних елементів – правових, організаційних, технічних та криптографічних (програмно-математичних).

Співвідношення елементів та їх зміст забезпечують індивідуальність системи ЗІ підприємства і гарантують її неповторність та складність подолання. Співвідношення елементів системи, їх склад та взаємозв'язок визначають не тільки її індивідуальність, але й конкретний заданий рівень захисту з врахуванням цінності інформації та вартості подібної системи.

Правовий захист інформації передбачає: наявність в засновницьких та організаційних документах підприємства, контрактах, які укладаються із працівниками і у посадових настановах положень та зобов'язань із ЗІ, яка складає таємницю підприємства і його партнерів, формулювання і доведення до відома всіх працівників підприємства механізму правової відповідальності за

розголошення СІ. До правового елементу системи захисту також може включатись страхування СІ від різних ризиків.

Організаційний захист інформації містить заходи управлінського та обмежувального характеру, які спонукають персонал дотримуватися правил захисту СІ і включає у себе: формування і регламентування діяльності служби безпеки підприємства; забезпечення цієї служби нормативно-методичними документами з організації і технології ЗІ; регламентування та регулярне оновлення переліку СІ, яка підлягає захисту; складання і ведення переліку СД підприємства; регламентування системи (ієрархічної схеми) обмеження доступу персоналу до СІ; регламентування технології захисту і оброблення СД; побудова захищеного традиційного або електронного документообігу; побудову технології документування СІ, складання, оформлення, виготовлення і видавання СД; побудову технологічної системи оброблення і збереження СД; організацію архівного зберігання СД; регламентування захисту СІ підприємства від несанкціонованих дій персоналу; порядок і правила роботи персоналу з СД і СІ, контроль за виконанням всіма працівниками цього порядку і правил; відбір персоналу для роботи з СІ, навчання та інструктування працівників; порядок ЗІ під час ведення перемовин, проведенні нарад з конфіденційними питаннями, прийомі відвідувачів, здійснення рекламної, виставкової та іншої діяльності; регламентування аналітичної роботи з виявлення загроз СІ підприємства і каналів витоку СІ; обладнання і атестування приміщень, робочих зон, виділених для здійснення службової діяльності, ліцензування технічних систем і засобів ЗІ та охорони; регламентування пропускного режиму на території, у спорудах і приміщеннях підприємства, ідентифікування персоналу та вантажу; регламентування системи охорони території, споруд, приміщень, обладнання, місць зберігання готівкових коштів, транспорту і персоналу підприємства; регламентування організаційних питань експлуатації технічних засобів ЗІ і охорони; регламентування дій служби безпеки та персоналу в екстремальних ситуаціях; регламентування роботи з управління системою ЗІ.

Організаційний захист є стрижнем, який позв'язує в одну систему всі інші елементи ЗІ. Центральною проблемою при розробці методів організаційного ЗІ є формування дозвільної (розмежувальної) системи і доступу персоналу до СІ, документів і баз даних. Важливо чітко і однозначно встановити: хто, кого, та до яких відомостей, коли, на який термін і як допускає. Дозвільна система доступу розв’язує наступні задачі: забезпечення працівників всіма необхідними для роботи документами і інформацією; обмеження кола осіб, які допускаються до СД; виключення несанкціонованого ознайомлення з СД. У відповідності з цією послідовністю визначається необхідний ступінь посилення захисних заходів, структура рубежів (ешелонів) ЗІ. Доступ працівника до СІ, який здійснюється у відповідності з дозвільною системою, називається *санкціонованим*.

Дозвіл (санкція) на доступ до СІ завжди є суворо персоніфікованим і видається керівником у письмовому вигляді: наказом, який затверджує схему посадового або поіменного доступу до СІ; резолюцією на СД, списком-дозволом у карточці видавання справи або на обкладинці справи ознайомлення з СД. Організаційні заходи захисту відображаються в нормативно-методичних документах

служби безпеки підприємства. З огляду на це, часто використовується єдина назва двох розглянутих вище елементів системи захисту – організаційно-правовий ЗІ.

Технічний захист інформації включає: засоби захисту технічних каналів витоку інформації, які виникають під час роботи ЕОМ, засобів зв'язку, копіювальних апаратів, принтерів, факсів та інших приладів і обладнання; засоби захисту приміщень від візуальних та акустичних способів технічної розвідки; засоби охорони споруд і приміщень від проникнення сторонніх осіб (засоби спостереження, сповіщення, сигналізації, інформування та ідентифікування, інженерні споруди); засоби протипожежної охорони; засоби виявлення приладів і пристроїв технічної розвідки.

Програмно-математичний захист інформації включає: регламентування доступу до електронних документів персональними паролями, які ідентифікуються командами та іншими найпростішими методами захисту; регламентування спеціальних засобів і продуктів програмного захисту; використання криптографічних методів ЗІ в ІС, криптографування (шифрування) інформації у процесі передавання каналами звичайного та факсимільного зв'язку, пересилання поштою.

Конкретна система ЗІ підприємства завжди є суворо конфіденційною. Спеціалісти, які розробляли систему, ніколи не повинні бути її користувачами. Отже, система захисту СІ є індивідуалізованою сукупністю необхідних елементів захисту, кожний з яких окремо розв’язує свої специфічні для даної підприємства задачі і володіє конкретизованим відносно до цих задач змістом. У комплексі ці елементи формують багаторівневий захист секретів підприємства і дають відносну гарантію безпеки підприємницької діяльності підприємства.

7.4. Технологія захисту документованої інформації

Документообіг, як об'єкт захисту, є сукупністю (мережею) каналів розповсюдження документованої СІ споживачами у процесі управлінської та виробничої діяльності. Рух документованої інформації не можна розглядати тільки як механічне переміщення документів інстанціями, як поштову функцію.

Головним напрямом захисту СІ (документів) від усіх видів загроз є формування захищеного документообігу і використання у обробленні та зберіганні документів технологічної системи, яка забезпечує ІБ на довільних носіях.

Окрім загальних для документообігу принципів захищений документообіг базується на ряді додаткових принципів: персональної відповідальності працівників за збереження носія і таємницю інформації; обмеженні ділової необхідності доступу персоналу до документів, справ і баз даних; операційному обліку документів і контролю за їх збереженням у процесі руху, розгляду, виконання і використання; жорсткому регламентуванні порядку роботи з документами, справами і базами даних для всіх категорій персоналу.

У великих підприємницьких структурах зі значним обсягом документів *захищеність документообігу досягається за рахунок*: формування самостійних, ізольованих потоків СД і, частково, додаткового подріблення їх на ізольовані потоки у відповідності з рівнем конфіденційності (грифу) документів, які перемі-

щаються; використання централізованої автономної технологічної системи оброблення і зберігання СД, ізольованої від системи оброблення інших документів; організації ССД, яка входить у склад служби безпеки, аналітичної служби підприємства.

Однією з найважливіших вимог до захищеного документообігу є вибірковість у доставлянні і використанні персоналом інформації. Вибірковість призначена не тільки для забезпечення оперативності в отриманні користувачем інформації, але й для обмеження у доставлянні йому тієї інформації, робота з якою йому не дозволена у відповідності до його функціональних обов'язків.

В основі вибірковості в доставлянні і використанні СД лежить діюча у фірмі дозвільна (розмежувальна) система доступу персоналу до СІ, документів, справ і баз даних. Система, у даному випадку, передбачає цілеспрямоване подріблення СІ між працівниками на складові елементи, кожний з яких окремо не має значної цінності.

Захист документованої інформації у потоках досягається одночасним використанням як дозвільних (розмежувальних) заходів, так і комплексом технологічних процедур і операцій, що входять у систему оброблення і зберігання документів. У захищеному документообігу використовується традиційна (ручна, діловодна) технологічна, система оброблення і зберігання СД. В окремих випадках автоматизуються довідкові та пошукові завдання, контроль виконання. Технологічна система набуває змішаного характеру. Необхідно зауважити, що технологічні системи оброблення і зберігання службових і відкритих документів базуються на єдиній науковій і методичній основі.

Однак між ними спостерігаються деяка різниця. Так, технологічна система оброблення і зберігання відкритих документів (діловодна, автоматизована або змішана) призначена для розв’язання завдань в одній сфері – документаційного забезпечення управління. У свою чергу, технологічна система оброблення і зберігання СД розв’язує завдання не тільки у вказаній сфері, але й у сфері ЗІ під час роботи персоналу з СД. До цих завдань можна віднести наступні: попередження НСД довільної особи до документа, його частин, варіантів, копій; забезпечення фізичного збереження документів і носіїв СІ; забезпечення збереження таємниці підприємства, СІ, яка міститься в документах.

Крім того, технологічна система оброблення і зберігання СД розповсюджується не тільки на управлінську (ділову) документацію, але й на конфіденційні конструкторські, технологічні, науково-технічні документи, документовану інформацію, записану на різних технічних носіях. Захист технічних та електронних носіїв СІ має важливе значення (особливо на стадіях їх оброблення і зберігання). Саме на цих стадіях велика ймовірність втрати носія, його копіювання або знищення, підміни і модифікування.

Оброблення і зберігання СД на різних стадіях їх руху має свої особливості. Оброблення документів, які надходять і відправляються у процесі оброблення СД, які надійшли, розв’язуються наступні задачі ЗІ і її носіїв: не допустити попадання в дану фірму СД інших фірм і організацій; переконатися, що конверти, пакети з СД не відкривались на шляху проходження від відправника до адресата; попередити втрату документів після відкриття пакета; виключити

можливість ознайомлення технічних працівників підприємства з СД; виключити можливість ознайомлення не уповноважених працівників підприємства з СД, які мають позначку ″Особисто″; не допустити втрату документів і їх частин за рахунок неповного вилучення їх з конвертів; переконатися у комплектності документу, наявності всіх аркушів, примірників, відсутності факту підміни документа.

Складність виокремлення СД з загального потоку кореспонденції полягає в тому, що на пакетах, конвертах і часто на самих документах не ставиться гриф конфіденційності. Пояснюється це не тільки суто індивідуальним підходом до присвоєння інформації статусу службової, але й небажанням відправника звертати увагу сторонніх осіб на гриф обмеження доступу.

Враховуючи цю особливість відкриття документів, попередній розгляд і розподіл всієї кореспонденції, що надходить, виконується кваліфікованим працівником ССД підприємства, який добре знає структуру підприємства, функції структурних підрозділів і працівників, склад СІ.

Працівник відкриває всі пакети, конверти, бандеролі (крім тих, які мають позначку ″Особисто″), перевіряє правильність адресування та комплектність документів. Документи, які надійшли, він розподіляє на дві групи: ті, що мають гриф або довільну позначку обмеження доступу і ті, що не мають такої позначки. Документи другої групи порівнюється з переліком документів підприємства, віднесених до категорії службових. Подібний перелік регулярно коректується у відповідності із змінами в діяльності підприємства, виникненням нових видів роботи, складеними прогнозами і планами. Якщо співпадає найменування або тема документа, який надійшов, з однією з позицій переліку на документі проставляється гриф обмеження доступу необхідного рівня конфіденційності. Одночасно проставляється термін дії грифу і умови його зняття, вказані у переліку. Якщо документ надійшов з грифом обмеження доступу, тоді цей гриф не може бути знятий навіть у випадку, коли даний документ не входить у вказаний вище перелік. Гриф може бути змінений тільки в сторону підвищення рівня конфіденційності, тому що фірма зобов'язана захищати не тільки свої секрети, але й секрети всіх юридичних і фізичних осіб, які встановили контакт з даною підприємницькою структурою.

Всі СД, які надійшли, підлягають негайному обліку. Документи, які не віднесені до розряду СД повторно уважно розглядаються і передаються працівнику, який займається обробленням і зберіганням відкритих документів. У процесі оброблення СД, що відсилаються, розв’язуються наступні задачі ЗІ та її носіїв: виключення можливості таємного відкриття пакету і несанкціонованого ознайомлення з документами у процесі їх пересилання адресату, підміни документів і листів; обмеження можливості втрати, викрадення або підміни пакету з СД; підтвердити факт відправлення документу і правильність оформлення цього факту в облікових формах; виключення помилкового відправлення документа іншому адресату, безпідставне розсилання документів. Конвертування і відправлення СД здійснюється працівником ССД підприємства.

Відправлення СД особисто виконавцями не допускається. Дозволом на відправлення вихідного СД є підписаний керівником підприємства супровідний

лист до документу або дозвільний запис, зроблений особисто керівником в обліковій картці, якщо документ відсилається без супровідного листа. Під час пересилання СД поштою, каналами факсимільного або іншого оперативного зв'язку текст документу шифрується. СД запаковуються у два пакети, тобто здійснюється їх подвійне пакетування. На внутрішньому пакеті вказуються: гриф конфіденційності, прізвище особи, якій документ адресується, номери вкладених документів, за необхідністю ставиться позначка ″Особисто″. Внутрішній пакет опечатується паперовими наклейками, на яких ставиться печатка ″Для пакетів″ або печатка ССД підприємства. Зовнішній пакет оформляється у відповідності з поштовими правилами, вказані вище відомості на ньому не вказуються. Пакети з СД пересилаються цінними відправленнями. Передавання їх у поштове відділення фіксується в поштовому реєстрі, копія якого з поштовим штемпелем підшивається у відповідній справі. Частіше за все пакети з СД передаються адресатам кур'єрами підприємства. У цьому випадку подвійне конвертування, як правило, не застосовується. Всі необхідні позначки робляться на одному світлонепроникному пакеті, який опечатується.

Передавання документів кур'єром фіксується у реєстрі, розписці. Отже, оброблення СД, які надійшли і відправляються, пов'язане з виконанням ряду додаткових процедур та відрізняється ускладненою технологією, що дозволяє розв’язати не тільки чисто експедиційні завдання, але й завдання ЗІ та носія від можливого НСД.

7.5. Облік службових документів і формування довідково-інформаційного банку даних

Облік СД передбачає не тільки реєстрацію факту створення (видання) або отримання документа, але й обов'язкове фіксування усіх переміщень документа інстанціями, керівниками і виконавцями у процесі розгляду, виконання і використання документів. Облік цих документів та їх зберігання завжди централізовані в ССД підприємства або у референта керівника.

Головною метою обліку СД є забезпечення їх фізичного збереження. Облік СД вирішує наступні завдання: фіксування факту надходження або видавання документа; фіксування місця знаходження документа; забезпечення пошуку документів під час перевірки наявності або необхідності звернення до документа; забезпечення довідково-інформаційної і контрольної роботи з документами; попередження втрати копій та примірників документів, чернеток і редакцій, додатків та окремих аркушів. Для вирішення цих завдань доцільно вести наступні види обліку СД підприємства: облік вхідних документів; облік підготованих, виданих вихідних (ті, які відправляються) і внутрішніх документів; інвентарний (виділений) облік документів, справ та носіїв СІ. При довільному виді обліку індексування СД базується на порядковій нумерації документів всього потоку протягом календарного року.

Перевага порядкової нумерації полягає в гарантованому збереженні номеру, виділеного для даного СД, записі вихідних відомостей про документ і картку, заведену на документ. Жоден номер не може щезнути, а карточка випасти із систематизованого за номерами масиву. Поважним недоліком порядкової

нумерації документів є відсутність її прив'язки до місця зберігання документа. Однак до валового номера СД може додаватися смисловий індекс, який відзначатиме справу за номенклатурою. Номер СД, що надійшов, проставляється не тільки у вхідному штампі на першому аркуші СД, але й на першому аркуші кожного додатку в штампі ″До вх. № __″ з вказанням року реєстрації. У вхідному штампі СД додатково проставляється кількість аркушів основного документа і додатків з вказанням грифу їх конфіденційності.

У журналах і картках обліку вносяться не тільки вихідні дані про документ, але й відомості про його рух з моменту поступлення або видання до закінчення виконання і підшивання до справи, відправлення адресату або знищення. Кожний запис завіряється підписами працівника ССД і виконавця або іншого працівника цієї служби. При заповненні на СД одного примірника облікової картки виникає необхідність ведення контрольного журналу. Журнал призначений для забезпечення послідовності присвоєння СД порядкових облікових номерів, контролю за наявністю СД і карток, прискорення пошуку. Навпроти облікового номеру СД у журналі відзначається прізвище особи, яка розписалася у картці за отримання СД, тобто фіксується місцезнаходження документа.

При заповненні на СД двох або більше примірників картки функцію контрольного журналу виконує поточна картотека. Традиційний обліковий та довідково-інформаційний банк даних з СД звичайно включає в себе: довідкову картотеку на невиконані документи, в якій перші примірники карток розташовуються за виконавцями; валову картотеку з розділами невиконаних (для других примірників карток) і виконаних (для перших примірників карток) СД, в якій картки розташовуються у послідовності облікових номерів СД; контрольну картотеку, в якій додаткові примірники карток розташовуються за термінами виконання; довідкову картотеку на виконані документи.

Якщо на СД ведеться довідкова картотека, аналогічна до картотеки на відкриті документи, тоді частина картотеки на невиконані документи формується за виконавцями, а у частині на виконані документи картки розташовуються за рубриками номенклатури справ (якщо нумерація СД ведеться за кожною справою окремо) або у валовій послідовності номерів документів.

В обох варіантах примірники картки розміщуються одночасно в обидві частини картотеки. По закінченні робочого дня інший працівник ССД перевіряє правильність реєстрації СД та їх наявність. У облікових формах не дозволяється робити довільні виправлення за допомогою корегуючої речовини тощо. Виправлення ретельно вписуються працівником ССД біля/або вище помилкового запису і завіряються його підписом.

Помилковий запис закреслюється однією рискою. Облікові форми не повинні містити СІ. Разом з тим журнали і картотеки містять, в сукупності, дані обмеженого розповсюдження, у зв'язку з чим їх належить зберігати в умовах, які виключають доступ до них сторонніх осіб.

Переміщення КД між працівниками ССД фіксується у передавальному журналі. Автоматизований облік СД включає в себе наступні процедури: ввід у систему початкових відомостей про документи і формування машинного (електронного) журналу (картотеки); контроль правильності внесених записів та їх

відповідність документам; роздрук на паперовому носії введених записів для формування традиційного журналу (картотеки); роздрук облікової форми видавання документа.

У електронний журнал СД вносяться в хронологічній послідовності їх надходження до ССД. Паперові роздруки записів вихідних відомостей про документ, внесений в електронний журнал, забезпечують облікову функцію засвідчення факту надходження або видання документа, його місцезнаходження і зберігання.

Роздруки в комплексі формують традиційній обліковий журнал (картотеку), в якому записи про документи розташовуються у валовому порядку. Журнал одночасно є: описом СД; страховим масивом облікових даних про документи на випадок пошкодження або знищення електронного журналу.

Автоматизований банк даних реалізовує функцію довідкового та пошукового обслуговування користувачів, контролю виконання документів та, інколи, – роботи персоналу з електронними аналогами паперових документів.

Облік виданих СД додатково вирішує наступні завдання: попередження втрати чернеток і варіантів документа; підтвердження фактів знищення всіх чернеток матеріалів, які виникли у процесі виконання документа; підтвердження факту передавання документа на відправлення або виконання, передавання його іншим працівникам ССД. Для обліку виданих СД виконавець здає працівнику ССД: всі примірники підписаного керівником документа; додатки до документа; чернетки основного документа і додатків, редакції і варіанти документа, робочі записи; документ, який став основою для складання даного документа.

Про здачу та знищення вказаних матеріалів працівник ССД робить позначку в облікових картках документів і у внутрішніх описах СД, які знаходяться у виконавця. Позначка в обліковій картці завіряється підписами працівника і виконавця. Факт знищення чернетки і інших матеріалів підтверджується позначкою на копії документа, яка залишається у справі ССД.

Додатки до виданих СД є самостійними документами і мають свої облікові номери за відповідними видами обліку. Виданим конфіденційним розпорядчим документам і протоколам присвоюється не тільки загальний валовий обліковий номер, але й порядковий номер у даній групі документів.

На інвентарний облік після заповнення довідкових карток можуть братися всі СД підприємства, якщо обсяг таких документів невеликий. Картотека (журнал) інвентарного обліку СД ведеться безперервно. Номери кожного року продовжують номери попередніх років. Інвентарний номер вказується на документі в верхньому лівому кутку першого аркуша, наприклад: ″Інв. №__ і дата″. Одночасно може формуватися електронний довідковий масив з СД. Поставлені на інвентарний облік технічні носії інформації маркуються. Маркування передбачає нанесення на них таких даних: інвентарного номера, номера або назви структурного підрозділу, прізвища виконавця. Написи роблять речовиною, яка має високу механічну стійкість.

Облік СД дозволяє не тільки забезпечити збереження документів та організувати довідково-інформаційну і контрольну роботу, але й проводити періодичні і неперіодичні перевірки наявності документів.

Метою перевірки наявності СД є встановлення фактичної відповідності наявних документів записам в облікових формах, їх збереженню, цілісності та комплектності. Такі перевірки спонукають виконавців до ретельного дотримання правил роботи з СД і піклування про їх фізичне збереження. Перевірка проводиться від облікових даних до документів, примірників документів і складових частин кожного примірника. Регламентовані, обов'язкові перевірки наявності СД проводяться щоквартально і по завершенні календарного року.

Нерегламентовані перевірки здійснюються під час зміни керівництва підрозділів, звільненні виконавця, після закінчення екстремальної ситуації, виявлення фактів загрози інформації та в інших випадках. Перевірки наявності документів проводяться спеціально призначеною комісією, в яку звичайно входять: заступник керівника підприємства, керівник служби безеки та інші особи. За результатами перевірки складається акт.

Щоденні перевірки наявності документів (самоперевірки) проводяться по закінченні робочого дня всіма працівниками, які працюють з СД.

7.6. Порядок роботи персоналу з службовими документами

При виході документів за межі служби СД їх безпека різко знижується за рахунок санкціонованого ознайомлення з ними значної кількості працівників підприємства. У зв'язку з цим правильна організація роботи персоналу з цими документами є дуже важливою.

Особливо велика загроза електронним документам в результаті потенційної доступності інформації великій кількості працівників і важкості визначення самого факту крадіжки інформації. *Керівники і виконавці підприємства під час роботи з СД зобов'язані*: знайомитися тільки з тими СД, до яких вони отримали дозвіл на доступ в силу посадових обов'язків; подавати працівнику служби СД документи, що за ними числяться, для перевірки їх наявності і комплектності; вести облік документів, які у них знаходяться; щодня перевіряти наявність документів, здавати їх на зберігання в ССД; негайно повідомляти безпосередньому керівнику і у ССД про втрату або недостачу документів, виявлення зайвих або необлікованих документів, окремих аркушів; здавати за описом у ССД усі СД, які за ними рахуються, при звільненні, перед виходом у відпустку, від'їзді у відрядження.

Усі передавання СД керівникам і виконавцям повинні реєструватися в картках обліку СД. Приймання та видавання документів здійснюються під особистий підпис, що необхідно для встановлення факту покладення персональної відповідальності за документ на конкретних працівників.

Працівник служби СД, видаючи документи виконавцям для роботи, зобов'язаний: не допустити видання СД особі, яка не має права доступу до нього; зафіксувати факт передавання документа виконавцеві; забезпечити фізичне зберігання документа, додатків, аркушів і інших частин СД; ознайомити виконавця тільки з тією частиною СД, яка йому адресована; попередити можливість ознайомлення з документом сторонньої особи при видаванні СД виконавцеві і поверненні документа; забезпечити облік СД, які знаходяться у виконавців.

Відповідальність за збереження СД і попередження витоку інформації в підрозділах підприємства несуть їх керівники. Друкування СД на паперовому носії проводиться працівником ССД.

Виписки з СД робляться також з дозволу керівника підрозділу і враховуються за новими номерами на картках обліку підготованих (виданих) СД. Цільове використання працівниками підприємства копіювальної техніки необхідно суворо контролювати.

Розгляд та виконання електронних СД і електронних аналогів паперових документів супроводжується додатковими вимогами до системи їх безпеки. Для персоналу централізовано розробляється ієрархічна система ідентифікуючих паролів, кодів і ключів для забезпечення розмежування доступу до інформації.

Система затверджується наказом керівника і доводиться вибірково, в індивідуальному порядку до кожного працівника підприємства під особистий підпис. Оновлення системи повинно бути постійним, що особливо важливо при частій зміні персоналу. Довільне санкціоноване або несанкціоноване звернення до інформації повинно реєструватися. Рекомендується систематично перевіряти програмне забезпечення, яке використовується користувачами, з метою виявлення підозрілих програм.

Застосування персоналом власних (не зареєстрованих) захисних заходів під час роботи з комп'ютером не допускається. При несанкціонованому вході в конфіденційний файл інформація повинна негайно автоматично знищуватися.

Під час роботи з СД керівники і виконавці повинні бути забезпечені постійним робочим місцем; особистим сейфом (металічною шафою) і кейсом для зберігання документів; особистою номерною металічною печаткою. Ключі від сейфа та кейса, металічна печатка постійно зберігаються у керівника або виконавця. Дублікати ключів повинні знаходитись у ССД. Робоче місце працівника підприємства необхідно розмістити таким чином, щоб виключити можливість перегляду СД, які знаходяться на столі, особами, що не мають до них відношення. Робочий стіл не повинен проглядатися через вікно з сусідніх будинків.

Приміщення, в яких СІ обробляється на носіях, повинні мати захист від технічних засобів промислового шпіонажу. На робочому столі завжди повинен знаходитися тільки той СД і матеріали до нього, з якими в даний момент працює працівник.

Керівники і виконавці не повинні вести довільні картотеки для організації роботи з СД і контролю за їх виконанням. Черговість виконання визначається розкладкою СД робочими папками: ″Ознайомлення″, ″Для погодження″, ″Терміново″, ″Завдання на конкретну дату″ тощо. Не дозволяється зберігання СД в шухлядах робочого столу, в шафах та інших доступних місцях, навіть якщо вони мають засуви.

ЛЕКЦІЯ 8.

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ІС ПІДПРИЄМСТВА

План

Вступ.

8.1. Організаційні принципи управління інформаційною безпекою

8.2. Основні принципи розроблення системи управління інформаційною безпекою

ВСТУП

Широке впровадження у діяльність підприємств різної форми власності інформаційних систем вимагає забезпечення доступності, цілісності, а також конфіденційності оброблюваної інформації. Порушення безпеки ІС підприємства може істотно ускладнити виконання виробничих завдань. езважаючи на величезну залежність від електронної інформації та ІС, окремі працівники і навіть цілі підрозділи продовжують стикатися з поважними проблемами у забезпеченні інформаційної безпеки.

Мета даної лекції полягає в тому, щоб визначити методи успішного управління ІБ в ІС підприємств. У результаті розглянемо набір принципів, які дозволяють створити ефективну систему управління інформаційною безпекою. Разом з тим, варто відзначити, що ці принципи є всього лише одним з аспектів стратегії управління інформаційними технологіями. Неможливо успішно керувати ІБ в ІС, при незадовільному управлінні ІТ.

8.1. Організаційні принципи управління інформаційною безпекою

Незважаючи на різні операції, продукти та послуги, вищий менеджмент підприємств використовує п'ять принципів управління ризиками ІБ:

1. Оцінювання ризиків і визначення потреб.
2. Встановлення централізованого адміністрування.
3. Впровадження політик безпеки і відповідних засобів контролю.
4. Досягнення необхідного рівня підготовленості працівників.
5. Контроль і оцінювання ефективності політик безпеки і механізмів контролю.

Істотним чинником ефективного здійснення цих принципів є сполучний цикл діяльності, який гарантує, що управління ІБ постійно націлене на поточні ризики. Важливо, щоб керівництво підприємства своєчасно оцінило наявність ризиків, пов'язаних з безпекою ІС. Підставою для розроблення і впровадження політик безпеки та вибору необхідних засобів контролю є оцінювання ризиків у окремих підрозділах. Прийняті кроки дозволять збільшити обізнаність користувачів про ризики і відповідні політики безпеки. Ефективність засобів контролю полягає в оцінюванні шляхом різних досліджень та аудиторських перевірок. Отримані результати забезпечують підхід до подальшого оцінювання ризиків і визначають необхідні зміни в політиках і засобах контролю. Всі ці дії централізовано адмініструються і координуються службою безпеки або штатом

фахівців, що складається з консультантів, представників окремих служб та відділів, керівників підрозділів підприємств. Цикл управління ризиками подано на рис. 8.1.

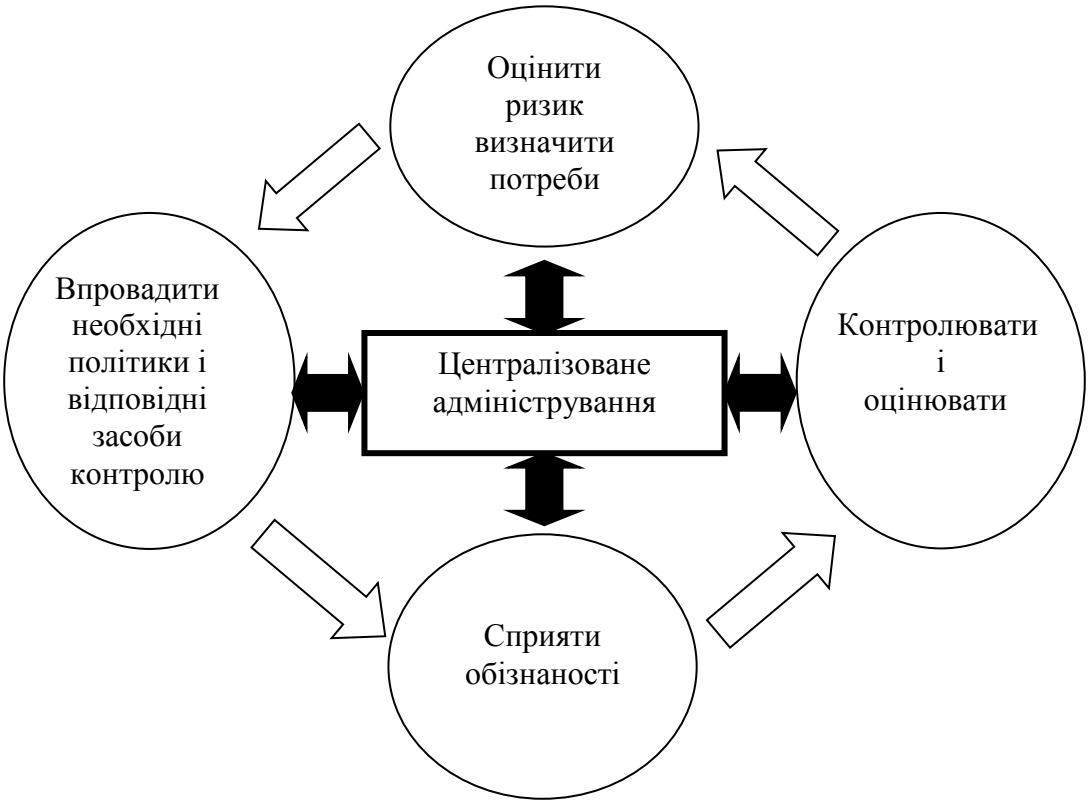


Рис. 8.1. Цикл управління ризиками інформаційної безпеки

Наступні шістнадцять методів, які використовуються для реалізування п'яти принципів управління ризиками, подані на рис. 8.2. Ці методи є ключовими для ефективного реалізування програми ІБ.

8.2. Основні принципи розроблення системи управління інформаційною безпекою

Оцінити ризик і визначити потреби. Оцінювання ризику є першим кроком реалізування програми забезпечення ІБ. Безпеку розглядатимемо як набір політик безпеки і відповідних засобів контролю, призначених для безпечного функціонування ІС та зменшення відповідних ризиків. Таким чином, визначення ризиків, пов'язаних з ІБ – відправна точка циклу управління ІБ.

Визнати інформаційні ресурси в якості істотних (невід'ємних) активів підрозділів підприємств. Визнання ризиків ІБ вищим менеджментом підприємств, а також набору заходів, спрямованих на визначення та управління цими ризиками є важливим чинником розвитку програми забезпечення ІБ. Такий підхід до менеджменту дозволить гарантувати, що ІБ серйозно розглядається і на більш низьких організаційних рівнях, а фахівці з ІБ забезпечені ресурсами, необхідними для ефективного здійснення програми. *Розробити практичні процедури оцінювання ризиків*. Існують різні методології оцінювання ризику, починаючи від неформального обговорення ризику і закінчуючи досить складними методами, які передбачають використання спеціалізованого ПЗ.

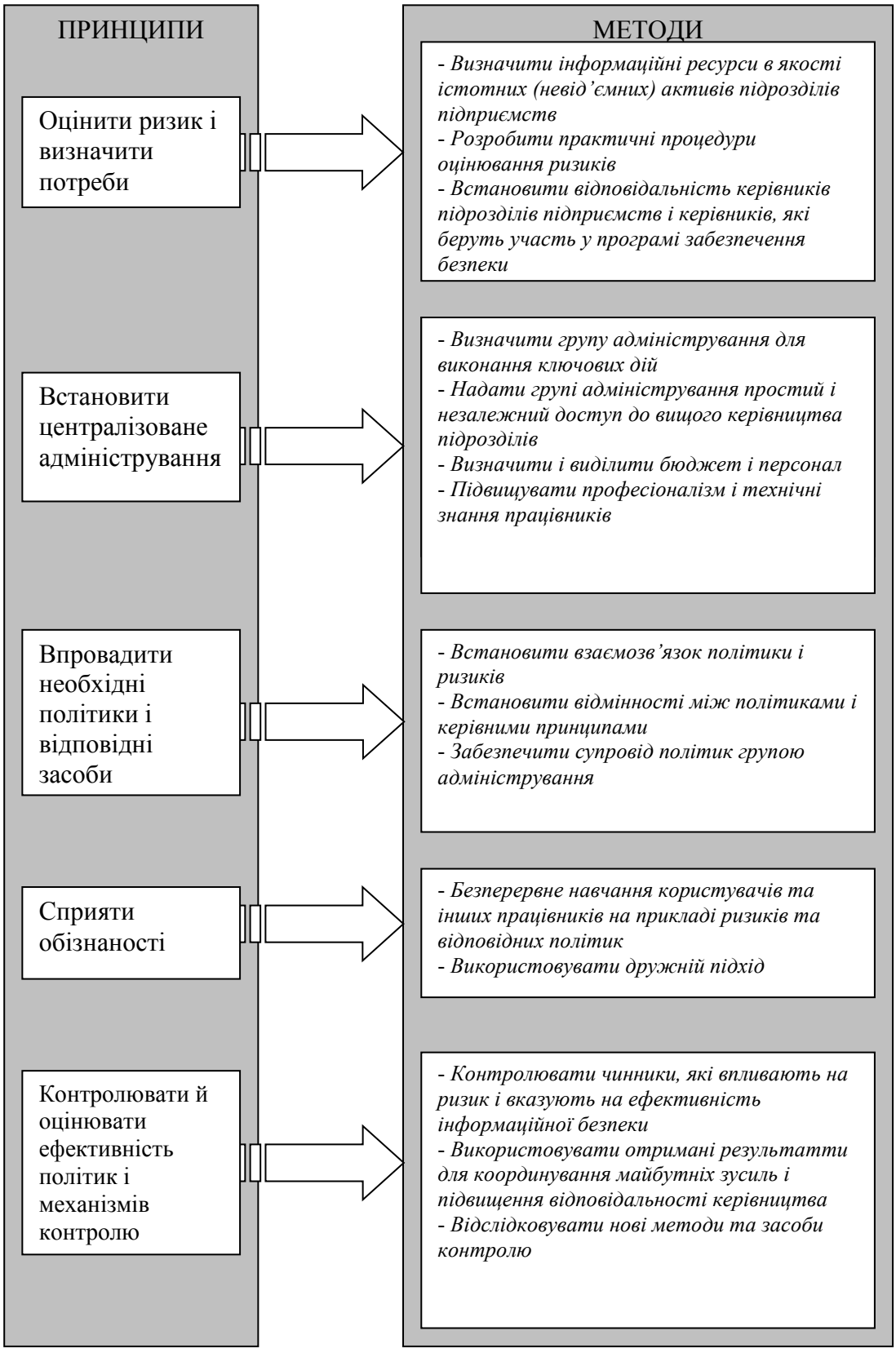


Рис. 8.2. Методи реалізування основних принципів

Світовий досвід успішних процедур управління ризиками описує відносно простий процес, який передбачає участь різних служб із залученням фахівців зі знаннями відповідних процесів, технічних фахівців і фахівців в галузі ЗІ.

Розуміння ризиків не передбачає їх точного кількісного визначення, включаючи вірогідність інциденту або вартість збитків. Такі дані недоступні,

тому що втрати можуть бути не виявлені, а керівництво не поставлено до відома. Крім того, дані про повні витрати на усунення збитків, викликаних слабкими механізмами контролю безпеки, а також операційної вартості цих механізмів (механізмів контролю) обмежені. Через постійні зміни технологій, а також програмних засобів та інструментів, доступних зловмисникам, застосування статистичних даних, зібраних у попередні роки є сумнівним. У результаті важко, якщо це взагалі можливо, достеменно порівняти вартість коштів контролю з ризиком втрати щоб визначити який засіб контролю є найбільш рентабельним. У будь-якому випадку, фахівці в галузі ІБ повинні покладатися на найбільш повну інформацію, доступну їм при ухваленні рішення про вибір необхідних засобів (методів) контролю.

Встановити відповідальність керівників підрозділів і керівників, які беруть участь у програмі забезпечення безпеки. Керівники повинні нести первинну відповідальність за визначення рівня безпеки ІС. Саме вони найбільшою мірою здатні визначити, який з інформаційних ресурсів є найбільш критичним, а також можливий вплив на ефективну роботу, у разі порушення його цілісності, конфіденційності або доступності. Таким чином, залучаючи їх до вибору засобів контролю можна гарантувати, що засоби контролю задовільняють поставленим вимогам, і будуть успішно впроваджені.

Безперервно управляти ризиками. ІБ варто надавати постійну увагу, щоб гарантувати адекватність і ефективність засобів контролю. Як було зазначено раніше, сучасні ІТ і суміжні технології, також як і чинники, пов'язані з ІБ, постійно змінюються.

Встановити централізоване адміністрування. Служба безпеки виступає, перш за все, в ролі радника або консультанта керівника підприємства, і не може нав'язувати методи (засоби) ІБ.

Визначити групу адміністрування для виконання ключових дій. У цілому, група адміністрування повинна бути: каталізатором (прискорювачем) процесу, гарантувати, що ризики ІБ розглядаються безперервно; центральним консультаційним ресурсом; засобом доведення до керівництва підрозділів підприємств інформації про стан ІБ та прийнятих заходах. Крім того, група адміністрування повинна централізовано керувати поставленими завданнями, бо в іншому випадку ці завдання можуть дублю**ватися різними структурами.**

Надати групі адміністрування простий і незалежний доступ до вищого керівництва підприємств. Відзначимо необхідність обговорення проблем ІБ фахівцями групи адміністрування з керівництвом підприємств. Такий діалог дозволить діяти ефективно і уникнути розбіжностей. В іншому випадку можливі конфліктні ситуації з керівниками підрозділів та розробниками систем, охочими якнайшвидшого впровадження нових програмних продуктів, і, тому, заперечуватимуть застосуванню засобів контролю, які можуть перешкоджати ефективності та ″комфортності″ роботи з програмним забезпеченням. Таким чином, можливість обговорення проблем ІБ на вищому рівні зможе гарантувати повне розуміння ризиків та їх допустимість до прийняття остаточних рішень.

Обґрунтувати і виділити бюджет і персонал. Бюджет дозволить планувати і встановлювати цілі програми ІБ. Як мінімум, бюджет включає заробітну

платню працівників і витрати на навчання. Штатна чисельність групи адміністрування може змінюватись у залежності як від поставлених цілей, так і від проектів, які знаходяться на розгляді. До роботи в групі можуть залучатися як технічні фахівці, так і працівники підрозділу безпеки.

Підвищувати професіоналізм і технічні знання працівників. Працівники підрозділів підприємств повинні брати участь у різних аспектах програми ІБ та володіти відповідними навичками та знаннями. Необхідний фаховий рівень працівників може бути досягнутий за допомогою тренінгів, проводити які можуть як фахівці підрозділу безпеки, так і зовнішні консультанти.

Впровадити необхідні політики і відповідні засоби контролю. Політики в області ІБ є підставою прийняття певних процедур і вибору засобів контролю. Політика безпеки – первинний механізм, за допомогою якого керівництво підприємств доводить свою думку і вимоги до працівників. Для ІБ, як і для інших областей внутрішнього контролю, вимоги політик безпосередньо залежать від результатів оцінювання рівня ризику.

Встановити взаємозв'язок політик і ризиків. Всебічний набір адекватних політик, доступних і зрозумілих користувачам, є одним з перших кроків у встановленні програми забезпечення ІБ. Варто наголосити на важливості безперервного супроводу політик для своєчасного реагування на виявлення ризиків та можливі розбіжності.

Встановити відмінності між політиками і керівними принципами. Загальний підхід до створення політик ІБ повинен передбачати: короткі (лаконічні) політики високого рівня; більш детальну інформацію, подану в практичних настановах.

Політики передбачають основні і обов'язкові вимоги, прийняті вищим керівництвом, той час як практичне керівництво не є обов'язковими для всіх підрозділів. Такий підхід дозволяє вищому керівництву акцентувати увагу на найбільш важливих елементах ІБ, а також надати можливість маневрування, зробити політики легкими для розуміння працівниками.

Забезпечити супровід політик безпеки групою адміністрування. Служба безпеки повинна бути відповідальною за розроблення політик ІБ підрозділів підприємств у взаємодії з керівниками підрозділів, внутрішніми аудиторами та юристами. Крім того, група адміністрування повинна забезпечити необхідні тлумачення. Це допоможе владнати і запобігти непорозумінням, а також прийняти необхідні заходи, не передбачені політиками (керівними принципами).

Політики варто зробити доступними, щоб користувачі, за необхідності, могли отримати доступ до їх актуальних версій. Користувачі повинні розписуватися в тому, що вони ознайомлені з ПІБ до надання їм доступу до інформаційних ресурсів. Якщо користувач буде залучений у інцидент безпеки, ця угода послужить свідченням того, що працівник був поінформований як про ПІБ, так і про можливі санкції, у разі її порушення.

Забезпечити необхідний фаховий рівень. Компетентність користувачів є обов'язковою умовою для успішного забезпечення ІБ, а також дозволяє гарантувати, що засоби контролю працюють належним чином. Користувачі не можуть виконувати політику, яку вони не знають або не розуміють. Не знаючи

про ризики, пов'язані з інформаційними ресурсами, вони не можуть усвідомити необхідність виконання політики, розробленої з метою зменшення ризиків.

Безперервне навчання користувачів та інших працівників на прикладі ризиків та відповідних політик. Служба безпеки повинна забезпечити стратегію постійного навчання працівників, які так або інакше впливають на ІБ. Група адміністрування повинна зосередити зусилля на загальному розумінні ризиків, пов'язаних з інформацією, яка обробляється в підрозділах, а також політиках і методах (засобах) контролю, спрямованих на зменшення цих ризиків.

Використовувати дружній підхід. Служба безпеки повинна використовувати різноманітні методи навчання і заохочення (стимулювання) щоб зробити політику ІБ доступною і навчити користувачів. Варто уникати зустрічей, що проводяться раз на рік з усіма представниками підрозділів, а навпаки – навчання краще проводити в невеликих групах працівників.

Контролювати й оцінювати ефективність політик і механізмів контролю. Як і довільний вид діяльності, ІБ підлягає контролю і періодичному переоцінюванню, щоб гарантувати адекватність (відповідність) ПІБ і засобів (методів) контролю поставленим завданням.

Контролювати чинники, які впливають на ризики і вказують на ефективність інформаційної безпеки. Контроль повинен бути зосереджений, насамперед, на наявності засобів і методів контролю та їх використання, спрямованого на зменшення ризиків і оцінюванні ефективності програми і політик ІБ, що поліпшують розуміння користувачів і скорочують кількість інцидентів. Такі перевірки передбачають тестування засобів (методів) контролю, оцінювання їх відповідності політикам ІБ, аналіз інцидентів безпеки, а також інші індикатори ефективності програми ІБ. Ефективність роботи служби безпеки та групи адміністрування може бути оцінена, ґрунтуючись, наприклад, на наступних показниках (але, не обмежуючись ними): кількість проведених тренінгів та зустрічей; кількість виконаних оцінювань ризику (ризиків); кількість сертифікованих фахівців; відсутність інцидентів, які ускладнюють роботу користувачів; зниження кількості нових проектів, впроваджених з затримкою через проблеми у забезпеченні ІБ; повну відповідність або погоджені та зареєстровані відхилення від мінімальних вимог ІБ; зниження кількості інцидентів, які допускають НСД, втрату або спотворення інформації.

Використовувати отримані результати для координування майбутніх зусиль і підвищення відповідальності керівництва

Контроль, безумовно, дозволяє привести стан захищеності ІС у відповідність до прийнятих політик ІБ, однак повні вигоди від контролю не будуть досягнуті, якщо отримані результати не використовуються для поліпшення програми забезпечення ІБ. Аналіз результатів контролю надає фахівцям в області ІБ і керівникам підрозділів засоби: переоцінювання раніше ідентифікованих ризиків; визначення нових проблемних ділянок; переоцінювання достатності та доречності існуючих засобів і методів контролю (управління) та дій щодо забезпечення ІБ; визначення потреб у нових засобах і механізмах контролю; переадресування контрольних зусиль (контролюючих дій).

Крім того, результати можуть використовуватися для оцінювання діяльності керівників підрозділів, відповідальних за розуміння і зменшення ризиків.

Відслідковувати нові методи та засоби контролю. Важливо гарантувати, що фахівці в сфері ІБ не "відстають" від розроблювальних методів та інструментів (додатків) і мають у своєму розпорядженні найновішу інформацію про уразливість ІС та ПЗ, вище керівництво гарантує, що має у своєму розпорядженні для цього необхідні матеріальні ресурси.

ВИСНОВОК

Розвиток програми ІБ, яка відповідає основним принципам – перший і основний крок підрозділів підприємств на шляху побудови ефективної системи інформаційної безпеки. Таким чином, підрозділи підприємств повинні безперервно:

- досліджувати і оцінювати ризики ІБ, які впливають на процеси;
- встановити централізоване адміністрування ІБ;
- встановити ПІБ, стандарти і засоби (механізми) контролю (управління), спрямовані на зменшення цих ризиків;
- сприяти обізнаності та розумінню описаної проблеми серед працівників;
- оцінювати відповідність і підвищувати ефективність.

ЛЕКЦІЯ 9.

АУДИТ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ. АУТСОРСИНГ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

План

9.1. Аудит захищеності інформаційних систем

9.2. Аутсорсинг у сфері інформаційних технологій

ВСТУП

Впроваджуючи інформаційну стратегію при експлуатуванні ІС вважаємо за необхідне звернути увагу на теорію та практику інформаційного аудиту, який дає можливість отримати цілісну та об’єктивну картину стану всієї ІС та її окремих елементів, локалізувати притаманні проблеми з метою створення ефективної і оптимальної програми розвитку забезпечення ІБ.

В умовах впровадження технології систем з відкритою архітектурою, які вирізняється складною взаємодією ІС різного походження (інтероперабельність), наявністю проблем перенесення прикладних програм між різними платформами (мобільність) та іншими особливостями, питання ЗІ набуває все більшої ваги.

У даний час все більш актуальними на ринку інформаційних технологій стають послуги аудиту захищеності інформаційних систем та аутсорсингу у сфері інформаційних технологій. Однак, як показує практика, і замовники, і постачальники найчастіше розуміють суть цих послуг по-різному. Акцентуємо увагу на особливостях різних видів аудиту захищеності ІС та аутсорсингу. Крім того, детально розглянемо головні критерії раціонального вибору і застосування того або іншого виду аудиту.

9.1. Аудит захищеності інформаційних систем

На даний момент ще не сформовано усталеного визначення аудиту ІБ. У подальшому ми пропонуємо під поняттям аудиту ІБ розуміти системний процес вивчення об'єктивних якісних і кількісних оцінок заходів безпеки, процесів доступу, використання інформації, інформаційних ресурсів та потоків, їх зв’язку з персоналом відповідно до визначених критеріїв та показників ІБ, вимог міжнародних стандартів, чинного законодавства України, відомчих нормативно-правових актів.

Аудит інформаційної безпеки є обов'язковим механізмом контролю захищеності ресурсів ІС для будь-якої організації. Він повинен проводитися не рідше одного разу на рік незалежними експертами, які мають відповідну кваліфікацію та досвід. Аудит дозволяє керівництву організації, її акціонерам та третім сторонам отримати об'єктивну інформацію про стан її ІБ.

Аудит ІБ є комплексом робіт, який включає дослідження всіх аспектів забезпечення ІБ в організації, що проводиться за узгодженим із замовником планом, відповідно до обраної методики.

Тривалий час аудит безпеки ІС розглядався як окремий незалежний сервіс який супроводжувався створенням і впровадженням стандартів аудиторської діяльності у сфері інформаційних технологій. Як правило, це закриті стандарти.

Такий підхід не відповідає одному із головних завдань аудиту - результати аудиту повинні бути об’єктивними, неупередженими і такими, що можуть бути повторені та відтворені довільним аудитом, у кращому випадку - зовнішнім, який використовуватиме таку ж методику аудиту.

На відміну від закритих стандартів аудиту, існують відкриті стандарти аудиту безпеки ІС які окреслюють організаційно-правову структуру аудиту ІБ. Відкриті стандарти пов'язують ІТ і дії аудиторів, об'єднують і погоджують багато критеріїв у єдиний ресурс, що дозволяє на сучасному рівні впровадити систему менеджменту інформаційною безпекою у ІС, враховують практично всі особливості ІС (на програмно-апаратному рівні) довільного масштабу і складності.

Основними цілями проведення робіт з аудиту ІБ організації є:

- незалежне оцінювання поточного стану захищеності ІС;
- ідентифікування та ліквідування загроз;
- техніко-економічне обґрунтування механізмів безпеки;
- забезпечення відповідності вимогам чинного законодавства;
- мінімізування збитків від інцидентів безпеки.

Основним результатом аудиту ІБ є звіт, який містить опис поточного стану ІБ в організації, опис виявлених загроз і невідповідностей обраним критеріям аудиту, а також рекомендації щодо їх усунення.

Процедура аудиту ІБ включає у себе:

- ініціювання та планування;
- обстеження, документування та збір інформації;
- аналіз отриманих даних і загроз;
- вироблення рекомендацій;
- підготовка звітних документів і здача робіт.

У якості критеріїв аудиту ІБ використовуються:

- міжнародні, національні та галузеві стандарти;
- законодавча і нормативна база;
- внутрішні організаційно-розпорядчі документи організації;
- вимоги, сформульовані за результатами оцінювання ризиків;

Методика проведення аудиту ІБ включає в себе:

- методи аналізу захищеності, аналіз конфігурації засобів захисту інформації, аналіз сценаріїв здійснення атак;
- інтерв'ю зі співробітниками організації з використанням заздалегідь підготованих і стандартизованих опитувальних листів;
- документування та аналіз ризиків з використанням спеціалізованого програмного інструментарію і шаблонів звітів;
- аналіз організаційно-розпорядчої документації з забезпечення ІБ;
- оцінювання процесів забезпечення ІБ в організації, кваліфікації працівників, знання ними своїх посадових обов'язків та ступеня їх обізнаності у питаннях ІБ;
- оцінювання достатності фізичних механізмів безпеки.

Активний аудит. Одним з найпоширеніших видів аудиту є активний аудит. Це дослідження стану захищеності ІС з точки зору зловмисника, який володіє високою кваліфікацією в області ІТ.

Найчастіше компанії-постачальники послуг активного аудиту іменують його інструментальним аналізом захищеності, щоб виокремити цей вид аудиту від інших.

Суть активного аудиту полягає в тому, що за допомогою спеціального програмного забезпечення (у тому числі систем аналізу захищеності) і спеціальних методів здійснюється збір інформації про стан системи захисту. При здійсненні даного виду аудиту на захист ІС моделюється максимальна кількість атак, які може здійснити зловмисник. При цьому аудитор штучно ставиться саме в ті умови, в яких працює зловмисник, – йому надається мінімум інформації, тільки та, яку можна отримати з відкритих джерел.

Після закінчення активного аудиту подаються рекомендації з модернізування системи захисту, що надасть можливість підвищити рівень захищеності ІС від дій ″зовнішнього″ зловмисника за мінімальних витратах на ІБ.

Активний аудит – послуга, яка може, і повинна, замовлятися періодично. Виконання активного аудиту, наприклад, раз на рік, дозволяє впевнитися, що рівень системи безпеки залишається на колишньому рівні.

Активний аудит умовно можна поділити на два види – ″зовнішній″ і ″внутрішній″.

При ″зовнішньому″ активному аудиті фахівці моделюють дії ″зовнішнього″ зловмисника. У даному випадку проводяться такі процедури:

- визначення доступних з зовнішніх мереж IP-адрес замовника;
- сканування даних адрес з метою визначення працюючих сервісів і служб, а також призначення відсканованих хостів;
- збір інформації про ІБ замовника з відкритих джерел;
- аналіз отриманих даних з метою виявлення загроз.

″Внутрішній″ активний аудит за складом робіт аналогічний до ″зовнішнього″. Однак, при його проведенні за допомогою спеціальних програмних засобів моделюються дії ″внутрішнього″ зловмисника.

Іноді в ході активного аудиту замовнику пропонується ряд додаткових послуг, безпосередньо пов'язаних з оцінюванням стану системи ІБ, зокрема – проведення спеціалізованих досліджень.

Найчастіше організація у своїй ІС використовує спеціалізоване програмне забезпечення (ПЗ) власної розробки, призначене для вирішення нестандартних завдань (наприклад, корпоративний інформаційний портал, різні бухгалтерські системи або системи документообігу). Подібне ПЗ унікальне, тому будь-яких готових засобів і технологій для аналізу їх захищеності та відмовостійкості не існує. У даному випадку проводяться спеціалізовані дослідження, спрямовані на оцінку рівня захищеності конкретного ПЗ.

Ще один вид послуг, пропонованих в ході активного аудиту, – дослідження продуктивності та стабільності системи, або стрес-тестування. Воно спрямоване на визначення критичних точок навантаження, за якого ІС внаслідок атаки на відмову в обслуговуванні або підвищеної завантаженості перестає адекватно

реагувати на легітимні запити користувачів. Тестування включає в себе симулювання атак на відмову в обслуговуванні, запитів до системи і загальний аналіз продуктивності ІС.

Експертний аудит. Експертний аудит можна умовно подати як порівняння стану ІБ з ″ідеальним″ описом.

При виконанні експертного аудиту працівники компанії-аудитора спільно з представниками замовника проводять такі види робіт:

- збір початкових даних про ІС, її функції та особливості, використовувані технології автоматизованого оброблення та передавання даних;
- збір інформації про наявні організаційно-розпорядчі документи щодо забезпечення ІБ та їх аналіз;
- визначення точок відповідальності систем, пристроїв і серверів ІС;
- формування переліку підсистем кожного підрозділу організації з категоріювання критичної інформації і схемами інформаційних потоків.

Один з найбільш об'ємних видів робіт, які проводяться при експертному аудиті, – збір даних про ІС шляхом інтерв'ювання працівників замовника і заповнення ними спеціальних анкет.

Основна мета інтерв'ювання технічних фахівців – збір інформації про функціонування ІС, а керівного складу – з'ясування вимог до системи ІБ.

Ключовий етап експертного аудиту – аналіз проекту ІС та технології оброблення інформації. За результатами робіт даного етапу пропонуються зміни в існуючій ІС і технології оброблення інформації, спрямовані на усунення виявлених недоліків з метою досягнення необхідного рівня ІБ.

Наступний етап – аналіз інформаційних потоків організації. На даному етапі визначаються типи інформаційних потоків в ІС організації та складається їх діаграма, де для кожного інформаційного потоку вказуються його цінність. На підставі результатів даного етапу робіт пропонується захист або підвищення рівня захищеності тих компонент ІС, які беруть участь в найбільш важливих процесах передавання, зберігання та оброблення інформації. Для менш цінної інформації рівень захищеності залишається тим самим. Застосування аналізу інформаційних потоків організації дає можливість спроектувати систему забезпечення ІБ, яка відповідає принципу розумної достатності.

У рамках експертного аудиту проводиться аналіз організаційно-розпорядчих документів, таких як політика безпеки, план захисту і різних настанов. Організаційно-розпорядчі документи оцінюються на предмет достатності та несуперечності декларованим цілям і заходам ІБ.

Особлива увага на етапі аналізу інформаційних потоків надається визначенню повноважень і відповідальності конкретних осіб за забезпечення ІБ різних ділянок ІС. Повноваження і відповідальність повинні бути закріплені положеннями організаційно-розпорядчих документів.

Результати експертного аудиту можуть містити різнопланові пропозиції з побудови та модернізування системи забезпечення інформаційної безпеки, наприклад:

- зміни в інфраструктурі ІС і технології оброблення інформації;

- рекомендації з вибору і застосування систем захисту інформації та додаткових спеціальних технічних засобів;
- пропозиції щодо вдосконалення пакету організаційно-розпорядчих документів;
- рекомендації до кожного з етапів створення системи ІБ;
- орієнтовні витрати на створення і вдосконалення системи забезпечення ІБ.

Аудит на відповідність стандартам. Суть даного виду аудиту найбільш наближена до тих формулювань, які існують у фінансовій сфері. При проведенні даного виду аудиту стан ІБ порівнюється з абстрактним описом, який подається у стандартах.

Забезпечення ІБ у спеціалізованих ІС – це комплексний процес, що вимагає чіткої організації і дисципліни. Він повинен починатися з визначення ролей і розподілу відповідальності серед посадових осіб, які відповідальні за ІБ. Тому, перший пункт аудиторського обстеження починається, власне, з отримання інформації про організаційну структуру користувачів ІС і обслуговуючих підрозділів. У зв’язку з цим аудитору потрібна документація, що стосується схеми організаційної структури ІС.

Організаційно-правова структура аудиту системи ІБ у ІС формується відповідно до рекомендацій міжнародних стандартів та з дотриманням положень чинного законодавства України. Такими стандартами є: ISO/IEC 27001:2013 Інформаційні технології. Методи захисту. Системи менеджменту інформаційною безпекою; ISO/IEC 27002:2005 Інформаційні технології. Методи захисту. Кодекс практики для менеджменту інформаційною безпекою; ISO/IEC 27003:2010 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації; ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки; ISO/IEC 27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем менеджменту ІБ.

Офіційний звіт, підготований у результаті проведення даного виду аудиту, включає наступну інформацію:

- ступінь відповідності ІС обраним стандартам;
- ступінь відповідності власним внутрішнім вимогам в області ІБ;
- кількість і категорії отриманих невідповідностей і зауважень;
- рекомендації з побудови або модифікування системи забезпечення ІБ, що дозволяють привести її у відповідність з даним стандартом;
- докладне посилання на основні документи замовника, включаючи політику безпеки, опис процедур забезпечення ІБ, додаткові обов'язкові і необов'язкові стандарти і норми, які застосовуються до даної організації.

Причини проведення аудиту на відповідність стандарту (і сертифікування) можна умовно поділити за ступенем обов'язковості даної послуги у відношенні до організації:

- обов'язкове сертифікування;
- сертифікування, викликане ″зовнішніми″ об'єктивними причинами;

- сертифікування, яке дає змогу отримати переваги у довгостроковій перспективі;
- добровільне сертифікування.

Державні організації, які обробляють відомості, що становлять державну таємницю, відповідно до чинного законодавства зобов'язані проводити атестування ІС. Однак, найчастіше вони користуються не послугою аудиту на відповідність стандартам, а в обов'язковому порядку проводять атестування власних ІС.

Останнім часом вищий менеджмент організацій розглядає отримання сертифікату, який підтверджує високий рівень ІБ, як додатковий чинник довіри у боротьбі за поважного клієнта або ділового партнера. У цьому випадку доцільним є проведення аудиту з подальшим сертифікуванням на відповідність тим стандартам, які є значущими для клієнта або ділового партнера.

На закінчення відзначимо, що при плануванні перевірки стану системи ІБ важливо не тільки точно вибрати вид аудиту, виходячи з потреб і можливостей організації, але і не помилитися з вибором виконавця.

Якщо аудит проводить консалтингова компанія, яка крім консалтингової діяльності займається ще й розробленням власних систем захисту інформації, вона, зі зрозумілих причин, зацікавлена в тому, щоб результати аудиту рекомендували замовнику використовувати її продукти. Для того щоб настанови на основі аудиту були дійсно об'єктивними, необхідно, щоб компанія-аудитор була незалежною у виборі використовуваних систем захисту інформації і мала великий досвід роботи в галузі ІБ.

9.2. Аутсорсинг у сфері інформаційних технологій

Аутсорсинг у сфері інформаційних технологій – передавання сторонньому підряднику ряду внутрішніх послуг і (або) внутрішніх сервісів установи-замовника, у тому числі на основі використання програмних продуктів, додатків, технічних засобів і фрагментів інфраструктури.

Аутсорсинг може розглядатися як сервіс, організований певною компанією, де кілька послуг надаються комплексно для повного охоплення потреб клієнта. На практиці, зазвичай, акцент ставиться на одну з конкретних обраних послуг.

Обслуговування інформаційних систем. Обслуговування ІС – найбільш поширений на практиці вид аутсорсингу в сфері ІТ. За такого обслуговування замовнику пропонується комплексний набір послуг, що дозволяє йому обійтися без власного системного адміністратора або ж значно знизити його завантаженість. Обслуговування ІС, як правило, включає у себе наступні види послуг:

- налаштування і оновлення апаратної частини ІС;
- супровід програмного забезпечення;
- створення захисту проти несанкціонованого доступу до активів ІС.

На практиці аутсорсери надають супутні послуги – створення VPN-мереж, IP-телефонія, ІТ-аудит та ІТ-консалтинг.

Аутсорсинг розміщення інформаційних систем (SoD**).** Аутсорсинг розміщення ІТ-систем (модель ″програмне забезпечення на вимогу″, (Software

on-Demand, SoD) є різновидом аутсорсингу інформаційних процесів. На відміну від звичайного хостингу, SoD-аутсорсер не тільки надає фізичне устаткування для розміщення ІС, а й забезпечує їх супровід (встановлення, підтримку, оновлення і, за необхідності, навчання персоналу).

У рамках моделі SoD замовники платять не за володіння програмним забезпеченням як таким, а за його оренду. Таким чином, на відміну від класичної схеми ліцензування ПЗ, замовник несе порівняно невеликі періодичні витрати, і йому не потрібно інвестувати значні кошти в придбання ПЗ. Модель передбачає, що у випадку тимчасової відсутності потреби в ПЗ, замовник може призупинити виплати.

Аутсорсинг процесів управління інформаційною безпекою. Система управління інформаційною безпекою організації, є, перш за все, сукупністю взаємодії процесів, більшість з яких може здійснюватися із залученням сторонньої спеціалізованої організації, фахівці якої мають необхідний досвід і кваліфікацію, або бути повністю переданою на аутсорсинг цій спеціалізованій організації.

Спеціалізована установа, яка виконує частковий або повний аутсорсинг ключових процесів управління ІБ забезпечує:

- управління ризиками системи ІБ;
- внутрішній аудит системи ІБ.

Передаючи ці процеси на аутсорсинг, організація отримує такі основні переваги:

- *економія часу і коштів на впровадження процесів управління ІБ в організації* (процеси управління ІБ запроваджуються одразу ж після укладення відповідної угоди про рівень сервісу в повному обсязі, для їх реалізування використовується вже готова технологія);
- *досягнення більш високого рівня якості та ефективності процесів управління ІБ* (фахівці спеціалізованої організації володіють сучасними технологіями і засобами ІБ, мають накопичений достатній досвід у предметній області і вдосконалюють свою кваліфікацію);
- *істотне скорочення операційних витрат на забезпечення ІБ* (вартість аутсорсингу, як правило, не перевищує витрат на заробітну платню одного фахівця відповідної кваліфікації, який відряджається для реалізування управління ІБ, не враховуючи витрат на навчання та підтримку рівня кваліфікації фахівця, організацію робочого місця, соціальну програму, податки тощо);
- *значне заощадження коштів на відповідних технічних і програмних засобах* (спеціалізована організація володіє усіма необхідними засобами для проведення інвентарризації ресурсів, оцінювання ризиків, відповідності вимогам стандартів та сертифікування систем ІБ, розроблення політик безпеки і регламентів, планування процесів внутрішнього аудиту, звітності тощо, окрім того, позбавляє від неминучого вибору серед існуючих технологій, незнайомих програмних і апаратних засобів);
- *потенційно більш високий ступінь незалежності та об'єктивності зовнішніх фахівців* (фахівці спеціалізованої установи не пов’язані міркуваннями

кар'єрного зростання в установі замовника, внутрішніми політичними та економічними міркуваннями, тісними особистими взаєминам і іншими умовами, здатними істотно вплинути на об'єктивність аудиторських висновків або результати оцінювання ризиків).

Приймаючи процеси управління ІБ та внутрішнього аудиту на аутсорсинг спеціалізована установа бере на себе відповідальність за те, що система захисту інформації:

- повністю відповідає вимогам чинного законодавства та нормативної бази в галузі захисту інформації, існуючим міжнародним і національним стандартам, а також передового досвіду забезпечення ІБ;
- адекватно оцінює існуючі інформаційні ризики і своєчасно реагує на постійно змінювані тенденції, появу нових загроз і технологій забезпечення безпеки;
- забезпечує проходження обов'язкового зовнішнього аудиту, який подає свої висновки регулюючим органам;
- є у змозі забезпечити необхідний рівень захищеності ІТ-інфраструктури та інформаційних ресурсів, який би відповідав існуючим ризикам, вимогам безпеки, законодавства і контрактних зобов'язань;
- своєчасно виявляє і усуває технічні недоліки системи ІБ, а також будь-які невідповідності у складі та змісті документації, кваліфікації та розподілу функцій персоналу, організації внутрішніх процесів забезпечення ІБ.

Аутсорсинг процесів управління ІБ здійснюється відповідно до угоди про рівень сервісу, яка чітко визначає основні метрики і показники ефективності системи ІБ. У результаті установа-замовник отримує керовані, документовані і вимірювані процеси управління ІБ, на фундаменті яких, властиво, і буде формуватися цілісна система управління ІБ організації.

Стосовно передавання процесів управління ІБ є очевидними наявні переваги суттєвого зменшення витрат на утримання ІТ-підрозділів відмовившись від повного штату персоналу і передати частину їхньої роботи (а в багатьох випадках –повністю) на аутсорсинг.

Недоліком аутсорсингу є загроза невиконання умов конфіденційності. Аутсорсер гарантує, що витік інформації про замовника неможливий, але виконання цього пункту не може гарантуватися стовідсотково.

ЛІТЕРАТУРА

1. Андреєв В.І. Основи інформаційної безпеки: підручник. / В.І. Андреєв, В.О Хорошко, В.С. Чередниченко, М.Є. Шелест; за ред. В.О. Хорошко. - Вид. 2-ге, доп. і переробл. – К: ДУІКТ, 2009. – 293 с.

2. База знань Microsoft [Електронний ресурс]. – Режим доступу: http://support.microsoft.com/kb/309531/

3. Ворожко В.П. Правові основи захисту інформації в Україні / – [Електронний ресурс]. – Режим доступу: http://www.bezpeka.com.ru.

4. Захаров В.П. Проблеми інформаційного забезпечення правоохоронних структур. Навчальний-посібник: / Захаров В.П., Рудешко В.І.- Львів: ЛьвДУВС, 2007. – 372 с.

5. Захист інформації в автоматизованих системах. Попередження комп'ютерних злочинів, особливості методики їх розслідування. [Електронний ресурс]. Шлях доступу: http://www.naiau.kiev.ua/biblio/books/Kriminal_inform/tema_4.htm

6. Економічна безпека підприємств, організацій та установ [Електронний ресурс]. Шлях доступу: http://pidruchniki.ws/1065082451335/ekonomika/oglyad_mistsya_podiyi

7. Кулешник Я.Ф. Інформатика: посібник / Я.Ф. Кулешник, Т.В. Рудий, В.В. Сеник – Львів: Львівський державний університет внутрішніх справ, 2015. – 248 с.

8. Міжнародний стандарт ISO/IEC 27001 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org

9. Міжнародний стандарт ISO/IEC 27002 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org

10. Міжнародний стандарт ISO/IEC 27003-27004 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org

11. Міжнародний стандарт ISO/IEC 27005 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org

12. Міжнародний стандарт ISO/IEC 27006 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org

13. Міжнародний стандарт ISO/IEC 27035 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org

14. Настройки браузера Internet Explorer [Электронный ресурс]. – Режим доступа: http://windows.microsoft.com/uk-ua/windows-vista/internet-explorer-browser-settings

15. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в Україні / О. В. Олійник // Право і суспільство. – 2012. - № 3. – С. 132-137. – Режим доступу: http://nbuv.gov.ua/UJRN/Pis_2012_3_30.

16. Рудий Т.В. Інформаційні системи і технології: посібник / Т.В. Рудий, Я.Ф. Кулешник, І.В. Бичинюк, А.Т. Рудий – Львів: Львівський державний університет внутрішніх справ [Електронний ресурс], 2014. – 306 с.

17. Рудий Т.В. Інформаційні системи і технології: практикум / Т.В. Рудий, Я.Ф. Кулешник, В.В. Сеник, О.І. Руда – Львів: Львівський державний університет внутрішніх справ, 2015. – 248 с.

18. Тарасенко Р.Б. Інформаційне право: Навчально-методичний посібник / Р.Б. Тарасенко. МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2010. – 512 с.

19. Цимбалюк В. С. Інституціоналізація інформаційної безпеки в інформаційному праві України / В. С. Цимбалюк // Бюлетень Мін'юсту України. – 2007. – № 8. – С. 45–53.

20. Щур Б.В. Інформатика та інформаційні технології: посібник / Б.В. Щур, І.С. Керницький. В.В. Сеник, В.Б. Вишня, Т.В. Рудий. – Львів: Львівський державний університет внутрішніх справ, 2010. – 536 с.

21. Karpinski M. Information Security / M. Karpinski. Warsaw: –Measurements, Automation and Monitoring. – 2012. – 280 p.

22. O&O DISKRECOVERY [Електронний ресурс]. – Режим доступу: http://www.samsebeadmin.ucoz.ua/

23. Ontrack EasyRecovery Professional 6.21.03 Portable + RePack. [Електронний ресурс]. – Режим доступу:

24. http://rutracker.org/forum/viewtopic.php?t=2966803

НАВЧАЛЬНЕ ВИДАННЯ

Рудий Тарас Володимирович
кандидат технічних наук, доцент
професор кафедри інформатики ЛьвДУВС

Живко Зінаїда Богданівна
доктор економічних наук, професор,
завідувач кафедри менеджменту ЛьвДУВС

Кулешник Ярко Федорович
кандидат технічних наук, доцент
доцент кафедри інформатики ЛьвДУВС

Руда Ольга Іванівна
кандидат економічних наук, доцент
доцент кафедри економіки та економічної безпеки ЛьвДувс

ТЕХНОЛОГІЧНІ ЗАСОБИ БЕЗПЕКИ ЕКОНОМІЧНИХ СИСТЕМ

Курс лекцій

Комп’ютерний набір і верстка
Рудий Т.В.

Електронний ресурс

Львівський державний університет внутрішніх справ
79007, м. Львів, вул. Городоцька, 26

Рудий Т.В.

Т38 Технологічні засоби безпеки економічних систем: курс лекцій. Вид. 2. Доп. і перероб. / Т.В. Рудий, З.Б. Живко, Я.Ф. Кулешник, О.І. Руда – Львів: Львівський державний університет внутрішніх справ, 2017. – 122с.