ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

**М.І. Копитко**

# МЕНЕДЖМЕНТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВ

**Навчально-методичний посібник**

**Львів-2016**

УДК 330.3:338.4:658
ББК У9(4Ук)305.851-98
К55

*Рекомендовано Вченою радою Львівського державного університету внутрішніх справ, протокол № 7 від 24.02.2016 року*

**Рецензенти:**

**Штангрет А.М.** – д.е.н., професор, завідувач кафедри фінансово-економічної безпеки, обліку і аудиту Української академії друкарства

**Лихолат С.М.** – к.е.н., доцент, доцент кафедри менеджменту Львівського державного університету внутрішніх справ

**Копитко М.І. Менеджмент інформаційних ресурсів та інформаційна безпека підприємств. Навчально-методичний посібник. – Львів: Ліга-Прес, 2016. – 172 с.**

У навчально-методичному посібнику представлено навчальні матеріали, які містять тексти лекцій, тестові завдання та контрольні запитання. Для студентів, курсантів, аспірантів економічних спеціальностей вищих навчальних закладів, фахівців у галузі менеджменту, для власників та керівників комерційних структур, керівників та менеджерів а також інших осіб, які цікавляться питаннями менеджменту та інформаційної безпеки.

**ISBN _____**

# ЗМІСТ

# ВСТУП

Останнім часом повідомлення про атаки на інформацію, про хакерів і комп'ютерні зломи заполонили всі засоби масової інформації. З масовим упровадженням комп'ютерів у всі сфери діяльності людини обсяг інформації, що зберігається в електронному вигляді, збільшився в тисячі разів. І тепер скопіювати за півхвилини і понести дискету, флеш-пам'ять із файлом (лами), що містить план випуску продукції, набагато простіше, ніж копіювати або переписувати купу паперів. А з появою комп'ютерних мереж навіть відсутність фізичного доступу до комп'ютера перестала бути гарантією збереження інформації.

При вирішенні багатьох завдань із прикладної сфери діяльності людини майбутній спеціаліст-менеджер стикається із проблемою захисту інформації, програмних продуктів, технічного забезпечення АРМ фахівців, комп'ютерних мереж, інформаційних систем. Для спеціалістів істотного значення набуло вміння не тільки застосовувати сучасні комп'ютерні програми, інформаційні технології, а й захищати інформацію, програмні пристрої, комп'ютерні мережі та їх складові.

Сучасні програмні продукти, інформаційні системи й технології базуються на апаратних і програмних засобах. Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, інших фінансових установ призводить до порушення нормального функціонування підприємств, значних фінансових збитків, а інколи до повного їх банкрутства.

Метою навчальної дисципліни є підготовка професіоналів, здатних з позиції сучасного менеджменту вибудувати систему інформаційної безпеки підприємства, забезпечити безпечне функціонування його підрозділів у різних видах діяльності, організувати надійний захист власності, об'єктів інфраструктури, інформаційних ресурсів, персоналу і керівництва.

Менеджери безпеки повинні знати особливості ринкової економіки і ділових відносин, уміти оцінювати наявні та потенційні погрози, планувати, організовувати і контролювати роботу з протидії зовнішнім і внутрішнім загрозам безпеки фірми, зокрема і у інформаційній сфері.

## ТЕМА 1:

## «Поняття та основи управління інформаційною безпекою організації»

## ПЛАН

1.1.Інформаційна безпека (поняття і визначення)

1.2. Визначення та загальні властивості інформації

1.3. Цінність та класифікація інформації

1.4. Інформація як об’єкт власності

1.5. Передумови розвитку менеджменту в сфері інформаційної безпеки на рівні підприємств

1.6. Загальна структура управлінської роботи щодо забезпечення інформаційної безпеки на рівні підприємства

## Література:


1. Закон України "Про інформацію";
2. Закон України "Про захист інформації в автоматизованих системах";
3. НД ТЗІ Загальні положення щодо захисту інформації в КС від несанкціонованого доступу
4. НД ТЗІ Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
5. НД ТЗІ Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
6. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
7. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – 188 с.
8. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х т. – М.: Энергоатомиздат, 1994. – 400 с.
9. Хоффман Л. Дж. Современные методы защиты информации. Пер. с англ. – М.: Советское радио, 1980. – 238 с.
10. «Інформаційна безпека. Організаційні заходи по забезпеченню безпеки. Розподіл відповідальності». [Електронний ресурс]. – Джерело доступу: usufit.org.ua/teaching/MSZBP/DownloadHandler.ashx?pg
11. Домарєв В.Основні поняття та визначення політики інформаційної безпеки. [Електронний ресурс]. – Джерело доступу: http://domarev.com.ua/obuch/lek_14_n6.htm
12. Менеджмент в сфере информационной безопасности [Електронний ресурс]. – Джерело доступу: http://www.intuit.ru/department/itmngt/manofis/1/

## 1.1. Інформаційна безпека (поняття і визначення)

Забезпечення безпечної діяльності необхідне для будь-яких підприємств і установ, починаючи від державних організацій і закінчуючи маленькою ланкою, що займається роздрібною торгівлею. Різниця полягатиме лише в тому, які засоби і методи й у якому обсязі будуть потрібні для забезпечення їх безпеки.

Перш ніж приступити до аналізу сучасного стану проблеми інформаційної безпеки, розглянемо проблеми безпеки взагалі. Спочатку необхідно визначити, що підлягає захисту і якими основними принципами слід керуватися при організації захисту. За сформованою історичною та міжнародною практикою безпеки об’єктами захисту з урахуванням їх пріоритетів є:

1) особа;

2) інформація;

3) матеріальні цінності.

Якщо пріоритет збереження безпеки особи є природним, то пріоритет інформації над матеріальними цінностями вимагає більш докладного розгляду. Це стосується не тільки інформації, що становить державну чи комерційну таємницю, а й відкритої інформації.

Ринкові відносини з їх невід’ємною частиною – конкуренцією обов’язково вимагають протидії зовнішнім і внутрішнім впливам. Об’єкти захисту більшою чи меншою мірою, залежно від цілей зловмисника (ЗЛ) і від конкретних умов, можуть зазнавати різних нападів чи загроз опинитися в ситуації, в якій вони з об’єктивних причин наражаються на небезпеку.

Поняття «безпечна діяльність» будь-якого підприємства чи організації включає:

1) фізичну безпеку, під якою розуміється забезпечення захисту від загрози життю людей;

2) економічну безпеку;

3) інформаційну безпеку (ІБ);

4) матеріальну безпеку, тобто збереження матеріальних цінностей від усякого роду загроз – починаючи від їх крадіжок і закінчуючи загрозами пожежі та інших стихійних лих.

Не зупиняючись детально на загрозах фізичної і матеріальної безпеки, відзначимо тісний зв’язок між економічною та інформаційною безпекою.

Як вважають західні фахівці, витік 20% комерційної інформації в 60 випадках зі 100 призводить до банкрутства фірми. Жодна, навіть процвітаюча фірма не проіснує більш як три доби, якщо її інформація, що становить комерційну таємницю, стане відомою. Таким чином, економічна та інформаційна безпека виявляються тісно взаємозалежними.

Зменшення загрози для економічної діяльності будь-якої організації передбачає одержання інформації про конкурентів. Тому, цілком природно, зменшення даної загрози для одних організацій спричиняє збільшення загрози економічній діяльності інших організацій. Це стало можливим через наявність промислового, і зокрема економічного, шпигунства.

Збитки від діяльності конкурентів, які використовують методи шпигунства, становлять у світі до 30% усього збитку, а це мільярди доларів. Точну цифру збитків указати не можна в принципі внаслідок того, що ні ЗЛ, ні потерпілі не прагнуть оприлюднювати інформацію про скоєне. Перші, мабуть, через страх відповідальності за вчинене, а другі – через страх зіпсувати імідж. Цим пояснюється високий рівень латентності правопорушень і відсутність повідомлень про них у засобах масової інформації. Тому до публіки доходить інформація про менш як 1% від усіх випадків порушень, що мають кримінальний характер і які приховати неможливо.

Таким чином, завдання безпеки будь-яких видів доводиться вирішувати щоразу при розгляді різноманітних аспектів людської діяльності. Але, як бачимо, всі види безпеки тісно пов'язані з ІБ, і, більше того, їх неможливо забезпечити без забезпечення ІБ. Отже, предметом нашого подальшого розгляду буде саме ІБ.

Зробимо зауваження з приводу термінології. На сьогоднішній день термінологія щодо ІБ в основному розроблена, хоча цей процес триває досі. Найбільш поширені і необхідні терміни зафіксовані в Українському стандарті з технічного захисту інформації. Тому, звичайно, далі слідуємо саме йому.

Безпека інформації (БІ) (information security) – стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації. Автоматизована система (АС) – це організаційно-технічна система, що об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію. Захист інформації в АС (information protection, information security, computer system security) – діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС у цілому і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків унаслідок реалізації загроз. Комплексна система захисту інформації (КСЗІ) – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС. Інші терміни та поняття будуть вводитися та визначатися мірою потреби.

### 1.2. Визначення та загальні властивості інформації

Інформація – це результат відображення та обробки в людській свідомості різноманіття навколишнього світу, відомостей про предмети, що оточують людину, явища природи, діяльність інших людей і т. п.

З такого визначення випливає, що будь-яка інформація може бути важливою. Однак якщо обмежитися поняттям комп'ютерної системи (КС), що зараз дуже актуально, то можна дати більш просте визначення іформації – це все, що може бути представлене в КС. Відразу ж виникає питання про форми та види представлення інформації в КС.

Звичайно виділяють такі види представлення інформації, як букви, символи, цифри, слова, тексти, малюнки, схеми, формули, графіки, таблиці, плани, креслення, алгоритми і т. д. З цих видів можуть створюватися більш

складні види та структури представлення інформації: команди, повідомлення, довідки, рішення, інструкції, масиви, файли, томи і т. д.

Інформація, що втілена і зафіксована в певній матеріальній формі, називається повідомленням. Повідомлення можуть бути безперервними (аналоговими) і дискретними (цифровими).

Безперервне повідомлення представляється деякою фізичною величиною (електричною напругою, струмом і т. д.), зміни якої відображають перебіг певного процесу. Фізична величина, що передає безперервне повідомлення, може набувати будь-яких значень і змінюватися в довільні моменти часу. Таким чином, у безперервному повідомленні скінченної довжини може міститися велика кількість інформації.

Для дискретних повідомлень характерна наявність фіксованого набору окремих елементів, з яких у дискретні моменти часу формуються різні послідовності елементів. Важливою є не фізична природа елементів, а те, що набір елементів скінченний, і тому будь-яке дискретне повідомлення скінченної довжини передає скінченне число значень деякої величини, а отже, кількість інформації в такому повідомленні скінченна. При дискретній формі представлення інформації окремим елементам її можуть бути присвоєні числові (цифрові) значення. У таких випадках маємо цифрову інформацію.

Елементи, з яких складається дискретне повідомлення, називають буквами чи символами. Набір цих букв (символів) утворює алфавіт. Число символів в алфавіті називається об’ємом алфавіту. Дискретне повідомлення можна розбити на групи символів, що називаються словами. Зі слів можуть формуватися більш складні структури (записи, файли, томи і т. д.). Зауважимо лише, що найбільш простим є двійковий алфавіт.

Звичайно в КС інформація представляється двійковим алфавітом, що фізично реалізується сигналом, здатним приймати два добре помітних значення, наприклад електричну напругу високого і низького рівня, протилежні значення напруженості магнітного поля і т. д. Найважливішою вимогою до фізичних аналогів двійкового алфавіту є можливість надійного розпізнавання двох різних значень сигналу, що при описі функціонування схем позначають символами 0 (нуль) і 1 (одиниця).

Інформація в КС піддається різним процесам: введення, збереження, обробка, виведення.

Введення інформації у КС може здійснюватися з перфокарт, перфострічок, магнітних стрічок, барабанів, дисків, дискет, клавіатури, спеціальних пультів і т. д. Збереження інформації здійснюється на запам’ятовуючих пристроях – оперативних запам’ятовуючих пристроях, різних регістрах пам’яті, магнітних стрічках, барабанах, дисках, дискетах і т. д. Обробляється у КС інформація відповідно до прийнятого в даній системі порядку (ОС, ПЗ і т. д.). Для виведення інформації є багато каналів (візуальний, звуковий, друк та ін.).

Найбільш загальними інформаційними процесами, що відбуваються в АСОД, є такі:

• інформаційно-довідкове забезпечення;

• інформаційне забезпечення задач;

• обслуговування інформаційних баз.

Усі вони реалізуються персоналом за допомогою апаратних засобів, ПЗ та інформаційних баз АСОД.

### 1.3. Цінність та класифікація інформації

Крім представлення в КС, цікаво і важливо подивитися на інформацію з інших точок зору. Зокрема, виявляється, що інформація – це товар і, отже, є об'єктом товарних відносин. В Україні інформаційні відносини регулюються кількома законами, у тому числі і Законом «Про інформацію». Зокрема, у цьому законі в статті 18 подано класифікацію видів інформації:

• статистична інформація;

• масова інформація;

• інформація про діяльність державних органів влади й органів місцевого і регіонального самоврядування;

• правова інформація;

• інформація про особу;

• інформація довідково-енциклопедичного характеру;

• соціологічна інформація.

Оскільки інформацію можна продати, купити, імпортувати, фальсифікувати, украсти і т. д., то з цього випливає, що вона повинна якимось чином оцінюватися. Далі, інформація, якою обмінюється людина через машину з іншою людиною чи машиною, може бути важливою і, отже, є предметом захисту. Однак захисту підлягає не будь-яка інформація, а тільки та, котра має ціну, тобто цінна інформація. Цінною ж стає та інформація, володіння якою дасть змогу її дійсному чи потенційному власнику одержати який-небудь виграш: моральний, матеріальний, політичний і т. д. Оскільки в суспільстві завжди існують люди, які бажають мати якісь переваги над іншими, то у них може виникнути бажання незаконним шляхом одержати цінну інформацію, а в її власника виникає необхідність її захищати. Цінність інформації є критерієм при прийнятті будь-якого рішення про її захист. Хоча було багато різних спроб формалізувати процес оцінки інформації з використанням методів теорії інформації та аналізу рішень, цей процес залишається дуже суб'єктивним.

Для оцінки потрібен розподіл інформації на категорії не тільки відповідно до її цінності, а й за важливістю. За рівнем важливості можна розділити інформацію на категорії таким чином:

1) життєво важлива незамінна інформація, наявність якої необхідна для функціонування системи;

2) важлива інформація – інформація, що може бути замінена чи відновлена, але процес її відновлення важкий і пов'язаний з великими витратами;

3) корисна інформація – інформація, яку важко відновити, однак система може досить ефективно функціонувати і без неї;

4) несуттєва інформація – інформація, без якої система продовжує існувати.

Хоча здається, що такий розподіл легко застосовувати, на практиці віднесення інформації до однієї з цих категорій може являти собою дуже важке завдання, тому що та сама інформація може бути використана багатьма підрозділами систем, кожний з яких може віднести цю інформацію до різних категорій важливості. Категорія важливості, як і цінність інформації, звичайно змінюється з часом і залежить від рівня її значущості для різних груп споживачів і потенційних порушників.

Існують визначення груп осіб, пов'язаних з обробкою інформації: власник – організація чи особа, що володіє інформацією; джерело – організація чи особа, що постачає інформацію; ЗЛ – організація чи особа, що прагне незаконно одержати інформацію. Для цих груп значущість однієї і тієї ж інформації може бути різною. Наприклад:

• оперативна інформація деякого підприємства (список замовлень на даний тиждень і графік виробництва) важлива для власника, а для джерела (замовника) чи порушника не має цінності;

• інформація про перспективи розвитку ринку може бути важливою для порушника, а для джерела чи власника, що завершили її аналіз, уже неважлива.

Наведені категорії важливості цілком узгоджуються з існуючим принципом розподілу інформації за рівнями таємності (або секретності).

Рівень таємності – це адміністративні чи законодавчі заходи, що відповідають мірі відповідальності особи за витік конкретної інформації, регламентованої спеціальними документами, з урахуванням державних, воєнно-стратегічних, комерційних, службових чи особистих інтересів. Такою інформацією може бути державна, військова, комерційна, службова чи особиста таємниця. Рівень таємності визначається грифом, що присвоюється тій чи іншій інформації. В Україні в державних структурах встановлено такі рівні (грифи) таємності: несекретно, для службового користування, таємно, цілком таємно (Н, ДСК, Т, ЦТ). Аналогічна термінологія існує в більшості країн світу: unclassified, confidential, secret, top secret (U, C, S, TS). Така класифікація дає можливість визначити просту лінійну порядкову шкалу цінності інформації: Н < ДСК < Т < ЦТ (U < C < S < TS). За цією шкалою відразу видно, до якої категорії інформації необхідно висувати більш високі вимоги щодо її захисту.

Слід додати, що, як показала практика, у багатьох випадках захищати потрібно не тільки секретну інформацію. І несекретна інформація, що піддана несанкціонованим ознайомленням чи модифікації, може привести до витоку чи втрати пов'язаної з нею секретної інформації, а також до невиконання АС функцій обробки секретної інформації. Існує також можливість витоку секретної інформації шляхом аналізу сукупності несекретних відомостей. Усе це лише підтверджує тезу про складність класифікації інформації, яку необхідно захищати.

Як було раніше зазначено, останнім часом інформація стала найважливішим ресурсом, випереджаючи за важливістю навіть сировинні та енергетичні ресурси. Але для ефективного її використання необхідно вміти

оцінювати значимість її для виконання відповідної діяльності, тобто оцінювати інформацію як об'єкт праці. Для такої оцінки необхідні показники двох видів:

1) що характеризують інформацію як ресурс для забезпечення процесу отримання розв'язків різноманітних задач;

2) що характеризують інформацію як об'єкт звичайної праці.

Зміст показників першого виду визначається важливістю інформації в процесі розв'язання задач, а також кількістю і складом інформації, яка використовується. Під кількістю інформації тут розуміється об'єм відомостей, які використовуються в процесі розв'язання задач, причому не абсолютний їх об'єм, а їх достатність для інформаційного забезпечення конкретних задач, їх адекватність задачам. Отже, показники першого виду можуть бути такими:

• важливість – це узагальнений показник, який характеризує значимість інформації з точки зору задач, для яких вона використовується, а також із точки зору організації її обробки. Тут оцінка може здійснюватися за: важливістю самих задач для даної діяльності; ступенем важливості інформації для ефективного виконання відповідних завдань; рівнем витрат при небажаних змінах інформації; рівнем витрат на відновлення порушень інформації. Слід зазначити, що для деяких видів інформації важливість можна досить точно оцінювати за так званим коефіцієнтом важливості, обчислення якого здійснюється на основі математичних, лінгвістичних або неформально-евристичних моделей;

• повнота – це показник, що характеризує міру достатності інформації для розв'язання відповідної задачі. Для кількісного вираження цього показника також відомі формальні і неформальні моделі обчислення коефіцієнта повноти;

• адекватність – це ступінь відповідності інформації дійсному стану тих об'єктів, які вона відображає. Адекватність залежить від об'єктивності генерування інформації про об'єкт, а також від тривалості часу між моментом генерування та моментом оцінки адекватності. Зазначимо, що для оцінки адекватності також відомі формальні і неформальні підходи, які дозволяють отримати її кількісні оцінки;

• релевантність – це показник, що характеризує відповідність її потребам задачі, яка розв'язується. Відомий коефіцієнт релевантності – це відношення обсягу релевантної інформації до загального її обсягу. Існують моделі його обчислення;

• толерантність – показник, що характеризує зручність сприйняття та використання інформації в процесі розв'язання відповідної задачі. Це поняття є дуже широким, невизначеним і суб'єктивним, а отже, формальних методів його оцінки поки що немає.

Якщо повернутися до показників другого виду, то слід зазначити, що для них інформація виступає як:

• сировина, яку добувають та обробляють;

• напівфабрикат, що виникає в процесі обробки сировини;

• продукт для використання.

Тобто тут маємо звичайний виробничий ланцюжок: добування сировини – переробка для отримання напівфабрикатів – їх переробка для отримання

кінцевого продукту. Нагадаємо, що при цьому всі стадії переробки інформації мають задовольняти показники першого виду. Зрозуміло, що тут найбільш важливими є форма або спосіб представлення інформації, а також її об'єм. Отже, як показники другого виду можуть виступати:

1) спосіб або система кодування інформації, тобто ефективність кодування;

2) обсяг кодів, що відображають дану інформацію.

Таким чином, необхідний рівень захисту інформації слід визначати з урахуванням значень усіх розглянутих вище показників, а також грифів таємності.

Насамкінець звернемо увагу на розбіжність між визначеною вище таємністю і безпекою інформації. Безпека інформації – це захист інформації від негативних впливів на неї, і вона має відношення до технологічних процедур забезпечення захисту. Таємність інформації – це статус інформації, який фіксується залежно від її важливості і вимагає певного рівня її захищеності. Отже, це поняття має відношення до людей, окремих осіб, які відповідають за інформацію і вирішують, яку інформацію можна розкрити, а яку приховати від інших людей.

### 1.4. Інформація як об'єкт власності

Фактично сфера безпеки інформації – не захист інформації, а захист прав власності на неї. Щоб переконатися в цьому, розглянемо особливості інформаційної власності.

Історично традиційним об'єктом права власності є матеріальний об'єкт, а це означає, що фактично право власності було речовим правом.

Інформація ж не є матеріальним об'єктом, інформація – це знання, тобто відображення дійсності у свідомості людини (причому правильне чи помилкове відображення – неістотно, важливо, що у свідомості). І тільки згодом інформація може втілюватися в матеріальні об'єкти навколишнього світу. Однак не будучи матеріальним об'єктом, інформація нерозривно пов'язана з матеріальним носієм: це – мозок людини чи відчужені від людини матеріальні носії, такі як книга, дискета та інші види «пам'яті» (запам'ятовуючі пристрої).

Можливо, з філософської точки зору можна говорити про інформацію як про деяку абстрактну субстанцію, що існує сама по собі. Але з конкретної, матеріальної точки зору ні збереження, ні передача інформації поки що без матеріального носія неможливі. Унаслідок цього можна сформулювати такі особливості інформації як об'єкта власності.

1. Інформація як об'єкт права власності може копіюватися (тиражуватися) за допомогою матеріального носія. Матеріальний об'єкт права власності, як відомо, копіювати неможливо (принаймні поки що). Справді, якщо розглянути дві однакові речі (одяг, автомобіль тощо), то вони складаються з однакових структур, але все-таки вони різні (чим детальніше їх розглядати, тим більше вони будуть розрізнятися). Тим часом інформація при копіюванні залишається тою ж, це те саме знання.

2. Інформація як об’єкт права власності легко переміщується до іншого суб’єкта права власності без очевидного (принаймні помітного) порушення права власності на інформацію. Переміщення ж матеріального об’єкта від одного суб’єкта (без його згоди) до іншого неминуче спричиняє втрату первісним суб’єктом права власності на цей об’єкт, тобто відбувається очевидне порушення його права власності.

3. Небезпека копіювання і переміщення інформації збільшується тим, що вона, як правило, відчужувана від власника, тобто зберігається та обробляється в сфері доступності великого числа суб’єктів, що не є суб’єктами права власності на цю інформацію (автоматизовані системи, мережі ЕОМ і т. д.). Крім відзначених особливостей інформації як об’єкта власності в іншому, мабуть, вона нічим не відрізняється від традиційних об’єктів права власності.

Справді, право власності, як відомо, включає три правомочності власника, що становлять у цілому зміст права власності: право розпоряджання, право володіння, право користування. Стосовно інформації можна сказати, що суб’єкт права власності на інформацію може передати частину своїх прав (право розпоряджання), не втрачаючи їх сам, іншим суб’єктам, наприклад власнику матеріального носія інформації (це – володіння чи користування) чи користувачу (це – користування і, можливо, володіння).

Для інформації право розпоряджання передбачає виключне право (ніхто інший, крім власника) визначати, кому ця інформація може бути надана (у володіння чи користування). Право володіння передбачає володіння цією інформацією в незмінному вигляді. Право користування передбачає право використовувати цю інформацію у своїх інтересах. Таким чином, до інформації, крім суб’єкта права власності на неї, можуть мати доступ і інші суб’єкти права власності як законно, санкціоновано, так і (внаслідок відзначених вище особливостей) незаконно, не санкціоновано. Тому виникає дуже складна система взаємин між різними суб’єктами права власності. Ці взаємини повинні регулюватися та охоронятися, тому що відхилення від них тягнуть порушення прав власності на цю інформацію. Реалізацією права власності на інформацію звичайно займається певна інфраструктура (державна чи приватна).

Як і для будь-якого іншого об’єкта власності, для інформації така інфраструктура складається з ланцюжка: законодавча влада – судова влада – виконавча влада (закон – суд – покарання). Тому, незважаючи на ряд особливостей, інформація поряд з матеріальними об’єктами може і повинна розглядатися законом як об’єкт права власності.

Будь-який закон про власність з метою захисту прав власника, зафіксувавши суб’єкти та об’єкти права власності, повинен регулювати відносини між ними. Особливості регулювання цих відносин залежать від специфіки об’єктів права власності. У випадку інформаційної власності закон повинен регулювати відносини суб’єктів, а також суб’єктів і об’єктів права власності на інформацію з метою захисту прав як власника, так і законних власників і користувачів інформації для захисту інформаційної власності від розголошення, витоку, обробки (копіювання, модифікації чи знищення) інформації.

В Україні прийнято закони «Про інформацію» і «Про захист інформації в автоматизованих системах». У першому законі в статті 39 встановлено, що інформаційна продукція та інформаційні послуги громадян і юридичних осіб, що займаються інформаційною діяльністю, можуть бути об’єктами товарних відносин, регульованих цивільним і іншим законодавством. Інакше кажучи, інформація – це товар. Інформаційна продукція (стаття 40) – це матеріалізований результат інформаційної діяльності, призначений для задоволення інформаційних потреб громадян, державних органів, підприємств, закладів і організацій. Інформаційна послуга (стаття 41) – це здійснення у визначеній законом формі інформаційної діяльності.

## 1.5. Передумови розвитку менеджменту в сфері інформаційної безпеки на рівні підприємств

Забезпечення власної інформаційної безпеки на підприємствах, як правило, є невід'ємною частиною загальної системи управління, необхідної для досягнення статутних цілей і завдань. Значимість систематичної цілеспрямованої діяльності щодо забезпечення інформаційної безпеки стає тим більш високою, чим вищий ступінь автоматизації бізнес-процесів підприємства і чим більша " інтелектуальна складова" в його кінцевому продукті, тобто чим більшою мірою успішність діяльності залежить від наявності та збереження певної інформації (технологій, ноу-хау, комерційних баз даних, маркетингової інформації, результатів наукових досліджень), забезпечення її конфіденційності та доступності для власників і користувачів. Роль інформації у діяльності підприємств зростає в міру лібералізації світових ринків, коли матеріальні активи, меншою мірою є джерелами конкурентних переваг в силу значного зменшення торгових бар'єрів. Нематеріальні активи, існують зазвичай у вигляді інформації, в цих умовах починають грати роль однієї з провідних засад для підвищення конкурентоспроможності та розвитку бізнесу.

Забезпечення інформаційної безпеки також, як правило, має велике значення не тільки для стратегічного розвитку підприємства і створення основного продукту, але і для окремих (іноді допоміжних) напрямків діяльності та бізнес-процесів, таких як комерційні переговори і умови контрактів, цінова політика.

Крім того, значущість забезпечення інформаційної безпеки в деяких випадках може визначатися наявністю в загальній системі інформаційних потоків підприємства відомостей, що становлять не тільки комерційну, а й державну таємницю, і також інші види конфіденційної інформації (відомості, що становлять банківську таємницю, лікарську таємницю, інтелектуальну власність компаній-партнерів). Забезпечення інформаційної безпеки в цій сфері і, зокрема, основні вимоги, організаційні правила і процедури безпосередньо регламентуються законодавством, і нагляд за виконанням вимог здійснюється органами влади.

Так само як і на державному рівні, управління інформаційною безпекою на рівні підприємств спрямоване на нейтралізацію різних видів загроз:

• зовнішніх, таких як неправомірні дії державних органів (у тому числі і закордонних), протиправна діяльність злочинців і злочинних угруповань, незаконні дії компаній-конкурентів та інших господарюючих суб'єктів, недобросовісні дії компаній-партнерів, невідповідність чинної нормативно-правової бази фактичному розвитку технологій та суспільних відносин, збої і порушення в роботі глобальних інформаційних і телекомунікаційних систем та інформаційних систем компаній-партнерів ( контрагентів ) та ін;

• внутрішніх, таких як помилки і халатність персоналу підприємства, а також навмисно допускаються порушення , збої і порушення в роботі власних інформаційних систем та ін.

Таким чином, управління інформаційною безпекою на кожному окремому підприємстві має здійснюватися в контексті його загальної господарської діяльності: з урахуванням характеру діяльності компанії (технології виробництва, специфіки ринків збуту), а також фактично складається ситуації в ринковій конкурентній боротьбі, державній політиці, розвитку правової та правоохоронної системи, рівня розвитку окремих використовуваних інформаційних і телекомунікаційних технологій та інших факторів, що формують загальні умови поточної діяльності (рис. 1).


Рис. 1. Передумови розробки політики безпеки підприємства

Формальною підставою (передумовою) для здійснення цілеспрямованої діяльності у сфері захисту інформації, крім загальнодержавних вимог до захисту інформації, що становить державну, військову, лікарську та банківську таємницю, також є перелік відомостей, що становлять комерційну таємницю підприємства, який визначається підприємством самостійно з урахуванням вимог чинного законодавства.

Крім того, необхідність розробки і впровадження політики інформаційної безпеки може бути обумовлена такими обставинами, як:

• необхідність зменшення вартості страхування інформаційних ризиків або певних бізнес-ризиків ;

• необхідність впровадження міжнародних стандартів.

## 1.6. Загальна структура управлінської роботи щодо забезпечення інформаційної безпеки на рівні підприємства

Для нейтралізації існуючих загроз і забезпечення інформаційної безпеки підприємства організовують систему менеджменту у сфері інформаційної безпеки, в рамках якої (системи) проводять роботу за кількома напрямками (рис. 2):

• формування і практична реалізація комплексної багаторівневої політики інформаційної безпеки підприємства та системи внутрішніх вимог, норм і правил;

• організація департаменту (служби, відділу) інформаційної безпеки;

• розробка системи заходів і дій на випадок непередбачених ситуацій ("Управління інцидентами");

• проведення аудитів (комплексних перевірок) стану інформаційної безпеки на підприємстві.


Рис. 2. Структура організаційної діяльності у сфері інформаційної безпеки на підприємстві

Кожен з цих напрямків організаційної роботи має свої особливості і повинен реалізовуватися з використанням специфічних методів менеджменту та у відповідності зі своїми правилами. Політики і правила інформаційної безпеки є організаційними документами, що регулюють діяльність всієї організації або окремих підрозділів (категорій співробітників) в частині поводження з інформаційними системами та інформаційними потоками. Департамент інформаційної безпеки є вузькоспеціалізованим підрозділом, що вирішує специфічні питання захисту інформації. Система заходів з реагування на інциденти забезпечує готовність всієї організації (включаючи Департамент інформаційної безпеки) до осмислених цілеспрямованих дій у разі будь-яких подій, пов'язаних з інформаційною безпекою. Проведення внутрішніх аудитів інформаційної безпеки (періодичних або пов'язаних з певними подіями) має забезпечити контроль за поточним станом системи заходів щодо захисту інформації і, зокрема, незалежну перевірку відповідності реального стану справ встановленим правилам і вимогам.

При цьому кожен з напрямків діяльності має постійно вдосконалюватися в міру розвитку організації, а конкретні завдання повинні постійно уточнюватися відповідно до зміни в організаційній структурі, виробничих процесах або зовнішньому середовищі. Так, наприклад, якщо підприємство починає випуск продукції військового призначення паралельно з випуском цивільної продукції, то це може зажадати змін всіх основних напрямків організаційної роботи у сфері забезпечення інформаційної безпеки:

• корегування стратегії та основних положень політики інформаційної безпеки (на всіх її рівнях);

• зміни організаційної структури та функціональних завдань департаменту інформаційної безпеки;

• вдосконалення системи реагування на інциденти;

• використання досконаліших методик проведення аудитів інформаційної безпеки.

## ТЕМА 2:

## «Інформаційні потоки в організації»

### ПЛАН

2.1. Поняття та види інформаційних потоків в організації
2.2. Інформація та інформаційне середовище
2.3. Життєвий цикл інформаційного ресурсу

### Література:

1. Гриценко В.И., Паньшин Б.Н. Інформаційна технологія: стан і питання розвитку. – К.: Наукова думка, 1989. – 272 с.

2. Карминский А.М., Нестеров П.В. Інформація бізнесу. – М.: Фінанси і статистика 1997. – 416 с.

3. Матвієнко О.В. Основи інформаційного менеджменту: Навчальний посібник. – К.: Центр навчальної літератури, 2004. – 128 с.

### 2.1. Поняття та види інформаційних потоків в організації

***Організація*** – це динамічна структура, стан якої визначається як зовнішньою взаємодією з оточуючим середовищем, так і внутрішньою взаємодією між її елементами.

Здійснення інформаційної діяльності у системі організаційного управління в умовах функціонування автоматизованих систем ґрунтується на моделях “електронних офісів”, сформульованих ще наприкінці 80-х років:

− *інформаційна модель* - орієнтована на інформацію як ресурс, який виробляється і використовується у процесі функціонування системи управління, спрямована на розв’язування інформаційних проблем, раціоналізацію та інтеграцію інформаційних процесів, покращання організаційної структури, підвищення ефективності роботи у цілому;

− *комунікаційна модель* – обґрунтовує інформатизацію управління як комплексну систему, яка включає організацію апарата управління разом з персоналом, організаційними зв’язками, методами роботи, тобто є моделлю організаційної системи управління як складної системи соціальних комунікацій;

− *соціотехнічна модель* – описує процес і результат проектування автоматизованих систем, при якому вважається недостатнім обмеження параметрами інформаційних потоків, загальним характером вирішуваних завдань або типами комунікацій – повинні враховуватись також соціально-психологічні особливості організації, у якій буде функціонувати проектована система. У контексті соціотехнічного підходу кінцеві результати роботи організації залежать не в останню чергу від взаємовідносин людей, їх ціннісних орієнтацій.

У «електронному офісі» працівника оточують різноманітні засоби інформатизації з новими можливостями, які забезпечують одержання і видачу основних видів повідомлень і даних.

***Інформаційний потік*** – це сукупність повідомлень, які циркулюють у системі, і необхідні для здійснення процесів управління. Інформаційний потік характеризується: джерелом виникнення, напрямом, періодичністю, ступенем сталості, структурою, обсягом і щільністю, видом носія інформації, інформаційною ємністю окремих повідомлень, ступенем використання.

*Горизонтальний інформаційний потік* пов'язує органи управління, які знаходяться на одному рівні.

*Вертикальний інформаційний потік* пов'язує органи управління різних рівнів. Вертикальний інформаційний потік може бути висхідним і низхідним, тобто спрямованим від вище стоячих органів управління до нижче стоячих і навпаки.

Розвиток апаратно-програмного забезпечення інформаційних технологій створює умови інформаційного насичення робочих місць у офісі з інтеграцією різних видів інформаційних повідомлень (рис.1).

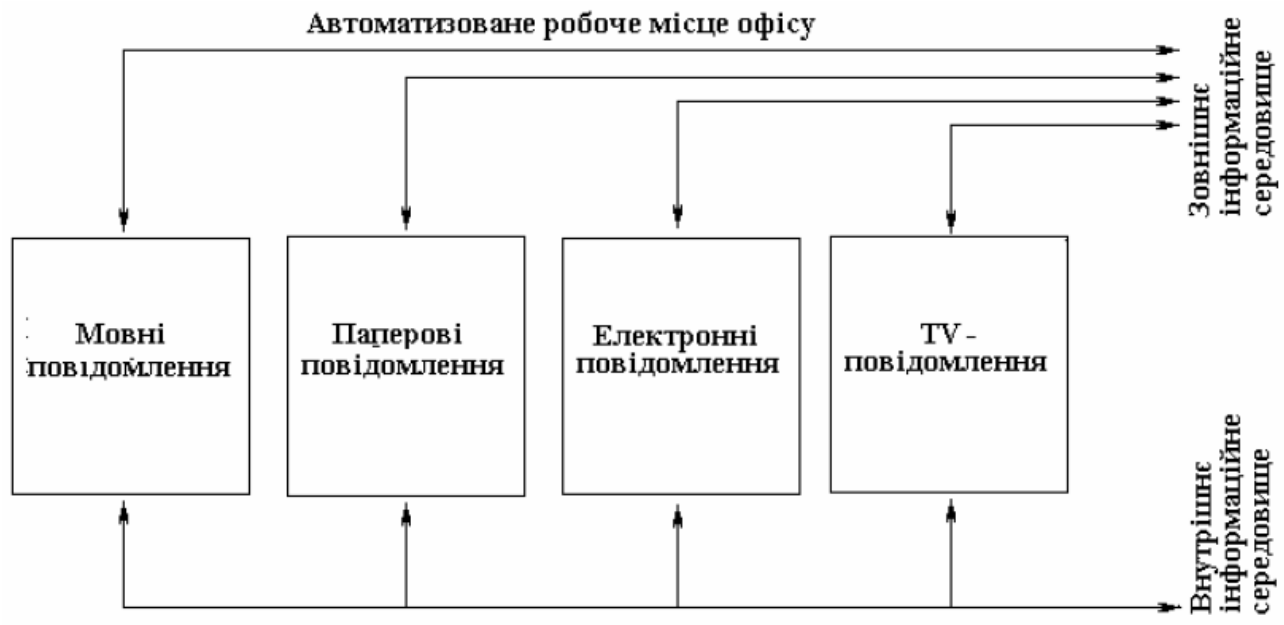


Рис. 1. Види інформаційних повідомлень у офісі

Сучасні інформаційні технології забезпечують доступ до інформаційних масивів (бази даних, електронні довідники та енциклопедії, оперативні дані, аналітичні дослідження, законодавчі та нормативні дані та ін.), які надходять з міжнародних, регіональних і національних інформаційних мереж. Це дозволяє використовувати електронні документи та інформаційні масиви для пошуку варіантів і визначення раціональних рішень у будь-якій діловій сфері.

## 2.2. Інформація та інформаційне середовище

Інформаційне забезпечення є базою, на якій ґрунтується управлінська діяльність. Інформацію тут слід розглядати як деяку сукупність різних повідомлень, відомостей, даних про відповідні предмети, явища, процеси, відношення та ін. Ці відомості, систематизовані і перетворені у придатну для використання форму, відіграють в управлінні надзвичайно важливу роль.

Інформація може бути класифікована за рядом ознак:

− функціональним призначенням і характером діяльності структурних підрозділів;

− за відношенням повідомлення до суб'єкта, який керує структурним підрозділом;

− за типом зв'язку структурного підрозділу і зовнішнього середовища (прямий і зворотній обмін інформацією шляхом здійснення постійних контактів, проведення прес-конференцій, брифінгів, інформаційних зустрічей);

− за відношенням до цільової функції структурного підрозділу;

− за логічним змістом (поділ на інформацію про суб'єктів органа управління, об'єкти його управлінського впливу (регіони, підприємства і організації, громадяни) та притаманних їм властивостях і відношеннях;

− за фізичною формою подання (усна доповідь; повідомлення на папері у вигляді текстів, анкет, таблиць графіків; електронний варіант – надходження електронною поштою, факсом, з інформаційних систем, на дискетах; у вигляді аудіо та відеокасет; книги, журнали, газети);

− за процедурою перетворення (ймовірнісні, соціологічні, моделюючі, аналітичні, обчислювальні);

− за ступенем перетворення (основна або така, що надходить; опрацьована у аналітичні або прогнозні записки, теле-, фото-, радіоматеріали; згрупована у інформаційні бюлетені та ін.).

З позицій *соціального управління* слід виділити такі ознаки класифікації інформації:

− межі фіксації (така, що підлягає або не підлягає реєстрації);

− ступінь додаткового опрацювання перед використанням;

− сфера використання (універсальна, що використовується у всіх управлінських структурах – довідки, положення, накази керівництва; спеціалізована, яка використовується тільки в тих або інших структурах);

− ступінь комплектності (комплектна документальна, тобто придатна для використання у початковому вигляді; некомплектна, тобто використовувана лише у зв'язку з іншими видами даних та відомостей);

− ємність і стабільність (вичерпна, яка не потребує доповнень; така, що потребує доповнень; постійна; змінна; така, що характеризує ймовірність настання події);

− форма і спосіб одержання (надходить з органа управління, шляхом вивчення статей та інших публікацій, проведення моніторингів, дослідження суспільної думки, обміну досвідом, роботи різних інформаційних підрозділів);

− впорядкованість (систематизована; відомості про нормативно-правові акти, що приймаються державними структурами; регламентована у часі, просторі, за особами, джерелами опублікування і змістом).

Інформаційні потоки можуть також відрізнятись залежно від:

– напряму руху (від структурних підрозділів до органу управління і, навпаки, від суб'єкта до об'єкта керуючого впливу);

− якісного змісту (виокремлення цінної за змістом інформації, від якої залежать певні керуючі дії, що спрямовані від структурних підрозділів);

− якісних характеристик (доцільно виділяти ймовірнісні, семантичні та інші міри інформації, використовувані в управлінському регулюванні та забезпеченні управлінських потреб). Важливою основою для класифікації є джерело інформації. Джерелом може виступати як об'єкт, відображенням якого є інформація, так і суб'єкт, який створює і розповсюджує її.

Залежно від суб'єкта (органа управління або його працівника, який одержує, поширює і опрацьовує інформацію) розрізняють аналітичну, прогнозну, довідкову, ознайомчу, рекомендаційну та ін. інформацію.

Корисність інформації визначається внутрішніми та зовнішніми користувачами, які висувають до її якості такі вимоги:

1. Відповідність і своєчасність інформації – здатність впливати на прийняття рішення користувачем і задовольнити його інтереси у потрібний момент або у певний термін.

2. Достовірність інформації – гарантія об'єктивності і правдивості наданих даних; передбачає необхідність зазначення методів, процедур одержання, щоб користувачі могли правильно розуміти її призначення і, за необхідності, перевірити її.

3. Порівнюваність інформації – можливість порівняння показників (наприклад, звітності), що потребує застосування набору визначень, одиниць вимірювання, методики опрацювання даних.

4. Доступність і зрозумілість інформації – подання інформації у зрозумілій для сприйняття формі. Форми надання звітності (поняття, які аналізуються, бази даних та ін.) повинні відображати сутність питання, бути чіткими, без зайвої деталізації, правильно перекладеними з іноземної мови тощо.

5. Конфіденційність інформації – надання користувачам лише тієї інформації, яка не завдасть шкоди організації з боку конкурентів.

Серед найбільш важливих видів джерел інформації для підприємства можна виділити:

− джерела всередині самої організації: спеціалізовані групи співробітників, періодичні звіти, різноманітні інформаційні зв'язки;

− інші організації: постачальники, рекламні агенції та засоби масової інформації, замовники, конкуренти;

− опубліковані джерела (звіти урядових організацій, звіти торгових організацій, наукові публікації, довідники);

− інформаційна індустрія: організації, які займаються дослідженнями в галузі маркетингу; спеціалізовані агенції та ін. Загальні вимоги до структури і функціональних властивостей елементів системи збирання, опрацювання,

зберігання і розповсюдження інформації з використанням сучасних електронних технологій дозволяють окреслити певний *організаційний інформаційно-технологічний простір*, систему, у якій відбувається опрацювання інформаційного ресурсу, який надходить із зовнішнього середовища. Одержані та опрацьовані інформаційні ресурси використовуються для прийняття управлінських рішень щодо діяльності об'єкта управління – організації, при чому інформація (у вигляді відповідних повідомлень) про діяльність організації надходить у зовнішнє середовище (рис.2).

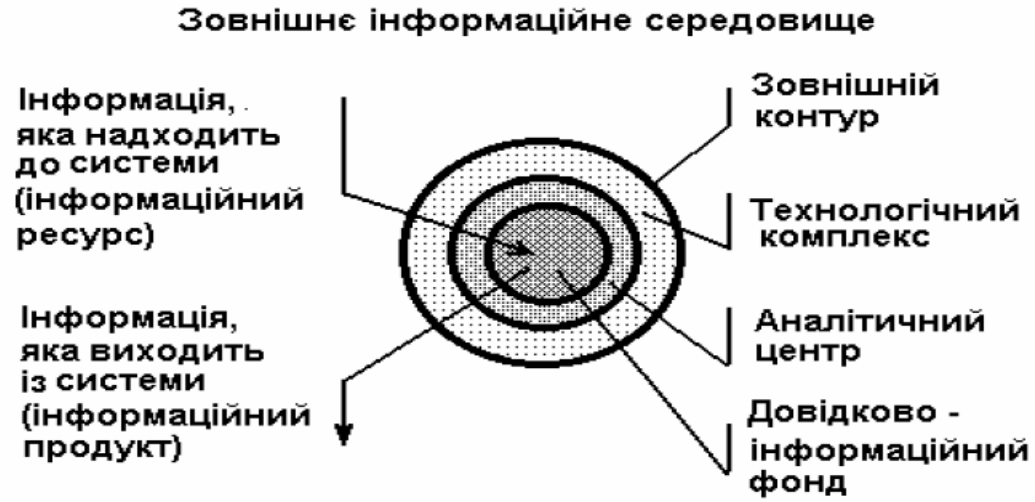


Рис. 2. Інформаційно-технологічний простір
системи інформаційного забезпечення організації

Зовнішній контур забезпечує структурування впливу зовнішнього середовища, забезпечує можливість надходження інформаційних ресурсів до системи і запобігає її руйнуванню від зовнішнього впливу.

***На вході*** забезпечується захист від несанкціонованого доступу до внутрішньої інформації системи, сумісність із зовнішнім середовищем (системним, апаратним, інформаційним, юридичним), селекція інформації, розподіл інформації внутрішніми каналами.

***На виході*** забезпечується блокування несанкціонованого виходу інформації з системи, забезпечується сумісність із зовнішнім середовищем, забезпечується можливість передавання інформації заданими каналами.

У загальному вигляді структура інформаційних процесів на підприємстві складається з таких підсистем:

1. *Первинне інформаційне середовище* (інформаційне поле).

2. *Вхідний інформаційний фільтр.* Система відбирає з первинного інформаційного середовища вихідний матеріал для опрацювання. Суттєву роль відіграє вибір принципу фільтрації цього середовища, який дозволить розумно обмежити обсяг вхідного потоку суттєво не втративши при цьому в обсягу інформації.

3. *Подання інформації всередині системи.* Це найбільш складний етап обробки, коли вхідна інформація перетворюється в інформаційну структуру, зручну для використання користувачем.

4. *Формування вторинного інформаційного середовища* є завершальним етапом внутрішньої інформаційної обробки.

5. *Аналіз реакції користувача.* Досліджується реакція користувача відповідно до критеріїв якості інформаційної діяльності.

Розрізняють чотири ***види інформаційних потоків*** у організації:

1. Обмін між організацією та зовнішнім середовищем (маркетинг, реклама, зв'язки з громадськістю).

2. Міжрівневий обмін інформацією в організації:

- низхідні потоки інформації, якими повідомляють підлеглим про поточні завдання, конкретні доручення, зміну пріоритетів та ін.;
- висхідні потоки інформації – звіти про виконання завдань, пропозиції з удосконалення технології та ін., за допомогою яких керівництво інформують про поточні та можливі проблеми, про можливі варіанти рішень.

3. Горизонтальний обмін інформацією:

- наради керівників суміжних підрозділів, задіяних у виконанні спільних завдань;
- наради керівників підрозділів, які мають схожі виробничі завдання;
- робота у межах робочих груп (управління проектом).

4. Неформальний обмін інформацією:

- обговорення виробничих питань під час неформальних зустрічей (під час обідньої перерви, святкових заходів та ін..);
- чутки, основною причиною яких є дефіцит офіційної інформації. Дослідження свідчать, що чутки бувають на 80-90% точними (за винятком випадків занадто емоційно забарвленої інформації). Чутки є надзвичайно впливовим чинником.

***Бар'єри на шляху інформаційних потоків у організації***

*1. Викривлення повідомлень:*

- ненавмисні викривлення, викликані проблемами у міжособистісному спілкуванні, а також можливими помилками персоналу при обліку та опрацюванні інформації
- навмисні викривлення, коли носій повідомлення не згоден з ним і змінює зміст повідомлення у власних інтересах. Проблеми при обміні інформацією можуть створювати конфлікти між різними групами та відділами організації. До викривлень інформації відноситься також її фільтрація. При передачі інформації зверху вниз основний мотив фільтрації висловлюється таким чином: "їх це не стосується". При передачі інформації знизу вверх існує тенденція повідомляти керівництву тільки хороші новини.

2. *Інформаційні перевантаження.* Керівник, зайнятий опрацюванням інформації, що надійшла, і необхідністю підтримувати інформаційний обмін, не в змозі ефективно реагувати на всю інформацію, яка надходить і змушений відсіювати менш важливу інформацію. Оцінка керівником важливості інформації може виявитись помилковою.

3. *Незадовільна структура організації.* Оскільки при передачі інформації з одного рівня управління на інший в результаті корегування і фільтрації втрачається приблизно третина її обсягу, найбільш ефективно керованими вважаються організації з невеликою кількістю рівнів управління і каналами відносно прямого інформаційного обміну.

Серед **заходів з удосконалення процесів обміну інформацією** можна назвати:

1. Регулювання інформаційних потоків – інформація повинна бути структурована за певними категоріями, повинні бути виявлені споживачі кожної категорії інформації і канали її одержання.

Одним з можливих способів широкого інформування працівників про діяльність підприємства є інформаційні бюлетені, які можуть розповсюджуватись як у друкованому вигляді, так і за допомогою сучасних інформаційних технологій.

2. Організація системи зворотного зв'язку, за допомогою якої орган управління одержує інформацію про поточний стан об'єкта управління.

3. Сучасні інформаційні технології.

Сучасні концепції управління інформаційною діяльністю на підприємствах широко застосовують ідеї інформаційної логістики. Впровадження комп'ютерних технологій дозволяє застосовувати менеджмент ділових процесів (Workflow Management), який представляє собою управління інформаційною логістикою на базі комп'ютерної технології і має на меті забезпечення діяльності з виконання господарських завдань необхідною інформацією відповідного виду, обсягу, якості, у відповідні терміни і у відповідному місці.

Застосування цих концепцій дозволяє побудувати *інформаційну модель організації*, яка є схемою потоків інформаційних повідомлень, використовуваних у процесі управління, відображає різні процедури виконання функцій управління організацією і пов'язує кожне завдання з вхідними і вихідними документами.

Теорія і методика інформаційного забезпечення та документування управлінських процесів, управління документацією (в тому числі електронною) потребує вивчення самої схеми управління, змісту управлінських зв'язків, впливу управлінської дії суб'єкта, що керує, на керований об'єкт, а також проблем, пов'язаних із наступним користуванням документами у їхньому динамічному стані, тобто потребує застосування *методології інформаційного менеджменту*. Вирішення проблем, пов'язаних із технічним, технологічним, лінгвістичним забезпеченням потребує застосування *методології інноваційного менеджменту, стратегічного менеджменту і менеджменту проектів*.

## 2.3. Життєвий цикл інформаційного ресурсу

Планування і розробка систем управління інформаційними ресурсами і потоками ґрунтуються на етапах життєвого циклу інформаційного ресурсу, модель якого представлена на рис. 3.


Рис. 3. Життєвий цикл інформаційного ресурсу

Життєвий цикл інформаційного ресурсу визначає цикл взаємодії фахівця і системи:

- визначення цілей (особистих, корпоративних, суспільних) і змісту інформації, необхідної для їх досягнення;
- створення, збирання, зберігання і пошук інформації;
- передавання інформаційних ресурсів користувачам і їх використання;
- оновлення у процесі використання, пов‘язане з оновленням властивостей, якостей, підвищенням продуктивності, інших ознак;
- утилізація та ліквідація. Типовими завданнями є виконання основних функцій менеджменту, таких як планування, організація, координація, контроль.

Розглянемо, які функції менеджменту виконуються на кожному з етапів ***життєвого циклу інформаційного ресурсу*** (табл. 1).

Сферу діяльності інформаційного менеджера можна представити як систему, що складається з таких підсистем: *документно-інформаційні ресурси – управління інформаційною діяльністю – комунікації*. Завдання діяльності спеціалістів сформульовано відповідно циклу взаємодії фахівця і системи та наведено в табл. 2 – 4.

Таблиця 1

Функції менеджменту на етапах життєвого циклу інформаційного ресурсу

| Етапи життєвого циклу інформаційного ресурсу | Функції менеджменту | Зміст |
|---|---|---|
| Визначення цілей | Планування | - аналіз інформаційних потреб організації;<br>- аналіз інформаційних потоків і масивів даних;<br>- розробка планів інформаційної роботи;<br>- планування діяльності служби документаційного забезпечення управління; |
| | Організація | - створення умов для зберігання нормативної, довідкової та архівної інформації;<br>- організація інформаційного забезпечення діяльності фірми та її співробітників; |
| | Контроль | - контроль впровадження інформаційних систем організації згідно з визначеними цілями; |
| Збирання і створення, зберігання, пошук, передача повідомлень і даних | Планування | - вивчення потреб працівників підприємства в інформації;<br>- аналіз інформаційних потоків і масивів даних;<br>- аналіз перспектив розвитку галузі;<br>- планування діяльності служби документаційного забезпечення управління; |
| | Організація | - організація добору та прийому на роботу персоналу для роботи з інформаційними системами, організація умов його роботи, підвищення кваліфікації;<br>- пошук зовнішньої інформації, яка відповідає потребам організації;<br>- організація комп'ютерної переробки інформації;<br>- впровадження, ведення і розвиток системи документації;<br>- забезпечення підрозділів і окремих працівників необхідною інформацією; |
| | Контроль | - контроль за надходженням інформації; |

*Продовження Таблиці 1*

| Етапи життєвого циклу інформаційного ресурсу | Функції менеджменту | Зміст |
|---|---|---|
| | | - контроль за станом діловодства у структурних підрозділах; |
| Використання інформаційних ресурсів | Планування | - аналіз інформаційного забезпечення комп'ютерних систем організації;<br>- аналіз функціонування служби документаційного забезпечення управління;<br>- участь у постановці задач, проектуванні, удосконаленні (в частині інформаційного забезпечення) автоматизованих інформаційних систем;<br>- видання інформаційних матеріалів, каталогів, проспектів;<br>- планування архівування і збереження інформації; |
| | Організація | - забезпечення підрозділів і окремих працівників необхідною інформацією;<br>- створення умов для зберігання нормативної, довідкової та архівної інформації;<br>- організація управління інформаційними ресурсами;<br>- проведення нарад, семінарів, виставок;<br>- видання інформаційних матеріалів, каталогів, проспектів;<br>- знищення інформації, згідно розкладу зберігання; |
| | Контроль | - контроль і підтримка функціонування системи безпеки інформації у комп'ютерній системі;<br>- контроль ефективності використання інформаційних матеріалів; |

Таблиця 2

*Підсистема:* ***Документно-інформаційні ресурси***

*Планування*

| ***Типове завдання діяльності*** | ***Уміння*** |
|---|---|
| - планування комплексу інформаційних ресурсів для забезпечення цілей діяльності організації<br>- визначення оптимального обсягу і безперервності інформаційних потоків;<br>- структуризація і впорядкування управлінських інформаційних потоків;<br>проектування уніфікованих систем документації;<br>- регулювання систематизації даних у інформаційному масиві, диференціація його за видами, сферами управлінської діяльності, типам управлінських задач і проблем, доступом користувачів<br>- надійне зберігання і оперативний вибірковий доступ до великих масивів документальної і довідкової інформації;<br>- розробка проектних рішень щодо вдосконалення документального забезпечення управління;<br>- аналіз інформаційних потреб та інформаційне забезпечення користувачів<br>- аналіз інформаційних потоків і масивів даних;<br>- аналіз перспектив розвитку галузі | - визначення узагальненої тематики інформації, необхідної для вирішення завдань діяльності організації;<br>- проектування інфологічної схеми бази даних<br>- застосовувати стандарти з метою структуризації і впорядкування зберігання інформаційних ресурсів і доступу до них;<br>- застосовувати міжнародні стандарти опису інформаційних ресурсів;<br>- застосовувати відповідну стратегію пошуку у масивах документальної і довідкової інформації;<br>- здійснювати аналіз і синтез інформації<br>- проводити експертизу цінності документів, підготувати їх до архівування або знищення<br>- уточнення складу і структури інформаційних матеріалів, створюваних для забезпечення управлінських рішень;<br>- уміти проводити системний аналіз документних потоків структурних підрозділів і визначати можливості їх автоматизації.<br>- пошук інформації у документно-інформаційних системах відповідно до запитів користувачів інформації |

*Організація*

| ***Типове завдання діяльності*** | ***Уміння*** |
|---|---|
| - підтримка процесів діловодства, контролю місцезнаходження, стану виконання документів, підтримка моніторингу проблемних ситуацій по інформації, яка міститься у документах;<br>- організація інформаційного забезпечення діяльності організації і її співробітників;<br>- створення умов для зберігання нормативної, довідкової та архівної інформації;<br>- автоматизована підтримка технологічних процедур роботи з документами: реєстрації, сортування, розмноження, редагування, друку, оформлення, видання та ін.;<br>- розробка організаційних і нормативно-методичних документів з документального забезпечення управління. | - володіти методами проектування системи підготовки і використання інформаційних ресурсів;<br>- володіти навичками і методикою формування і використання різноманітних баз даних і баз знань, банків даних, проблемно-орієнтованих, тематичних систем;<br>- уміти здійснювати пошук документів в інформаційно-пошукових системах з інтерактивним режимом роботи<br>- уміти здійснювати переклад, редагування наукової і інформаційної літератури;<br>- забезпечувати створення умов для зберігання нормативної, довідкової та архівної інформації. |

*Контроль*

| ***Типове завдання діяльності*** | ***Уміння*** |
|---|---|
| - контроль використання інформаційних ресурсів;<br>- контроль обробки інформації;<br>- контроль виконавчої дисципліни;<br>- захист даних та інформації. | - зберігати документну інформацію в інформаційних системах;<br>- володіти методами оцінювання ефективності використання інформаційних матеріалів;<br>- володіти методами контролю виконання нормативних вимог при роботі з інформацією;<br>- здійснювати контроль місцезнаходження і стану виконання документів |

Таблиця 3

*Підсистема:* ***Управління інформаційною діяльністю***

*Планування*

| ***Типове завдання діяльності*** | ***Уміння*** |
|---|---|
| - розробка стратегічних напрямів розвитку інформаційної діяльності організації, забезпечення конкурентоспроможності;<br>- розробка і впровадження нововведень;<br>- планування розвитку організації з урахуванням впровадження нових інформаційних технологій;<br>- здійснення соціально-психологічного регулювання в трудових колективах | - застосовувати теорію наукової організації, планування розвитку і проектування систем управління;<br>- володіти системною концепцією організації інформаційної діяльності на підприємстві на основі інформаційної технології і створення інформаційної системи як системи, що створює інформаційний ресурс і умови для його ефективного використання;<br>- володіти методами нормування праці в інформаційних службах;<br>- володіти методами підбору і розстановки кадрів в інформаційних службах |

*Організація*

| ***Типове завдання діяльності*** | ***Уміння*** |
|---|---|
| - поєднання усіх видів інформаційних ресурсів з метою досягнення цілей діяльності;<br>- організація процесів управління інформаційною діяльністю;<br>- організація ділових контактів підприємства із зовнішнім середовищем;<br>- розробка раціональних форм інформаційного забезпечення управління;<br>- оцінка значущості окремих напрямів діяльності організації на певних етапах розвитку з метою їх інформаційного забезпечення з використанням комп'ютерних систем. | - володіти методами створення і управління інформаційним середовищем організації;<br>- володіти методами створення центрів інформаційного аналізу, діагностики, експертизи, прогнозування і інформаційно-аналітичного моніторингу;<br>- володіти методами менеджменту персоналу для мотивації впровадження інформаційних технологій;<br>- матеріальне стимулювання в інформаційних службах;<br>- визначати цілі інформаційної діяльності |

*Контроль*

| ***Типове завдання діяльності*** | ***Уміння*** |
|---|---|
| - контроль використання інформаційно-ресурсного потенціалу підприємства;<br>- контроль форм і методів подання інформації користувачам віртуального середовища;<br>- контроль структури зовнішніх і внутрішніх інформаційних потоків;<br>- оцінка якості інформації, що надходить із зовнішнього середовища і застосовується для прийняття управлінських рішень | - уміти виявляти проблеми інформаційно-документаційного забезпечення з урахуванням новітніх досягнень інформаційних технологій;<br>- володіти методами проектування автоматизованих систем обліку, реєстрації, контролю документів |

Таблиця 4

*Підсистема**: Комунікації***

*Планування*

| ***Типове завдання діяльності*** | ***Уміння*** |
|---|---|
| - застосування інформаційних технологій для здійснення ефективних комунікацій як всередині організації, так і з зовнішнім середовищем;<br>- визначення раціональної конфігурації комунікаційних мереж;<br>- планування зовнішніх і внутрішніх комунікацій, підтримка доступу до віддалених інформаційних джерел і фондів;<br>- оцінка ефективності основних каналів надходження інформації;<br>- аналіз і планування номенклатури інформаційної продукції і послуг, які надходять від організації у зовнішнє середовище;<br>- вивчення потреб працівників підприємства у зовнішній інформації; | - володіти методами менеджменту для організаційно-психологічного проектування впровадження інформаційних технологій;<br>- оцінювати інформаційно-ресурсний потенціал підприємства;<br>- володіти методами аналітико--синтетичної переробки інформації;<br>- прогнозувати інформаційний попит;<br>- уміти оптимізувати форми і диверсифікувати методи представлення інформації користувачам віртуального середовища;<br>- уміти застосовувати сучасні засоби телекомунікацій з метою представлення підприємства у зовнішньому середовищі;<br>- володіти методами вивчення характеру і структури зовнішніх і внутрішніх інформаційних потоків;<br>- оцінювати якість інформації, що надходить із зовнішнього середовища і застосовуються для прийняття управлінських рішень;<br>- володіти методами розробки інформаційна структура INTRANET-сервера. |

*Організація*

| ***Типове завдання діяльності*** | ***Уміння*** |
|---|---|
| - організація комунікацій у глобальному інформаційному середовищі мережі Інтернет: організація ділових контактів за допомогою мережі, участь у проектах із створення “віртуальних корпорацій”, “електронних бібліотек”;<br>- адаптація інформаційних ресурсів підприємства до розповсюдження їх через глобальні інформаційні мережі | - уміти проектувати WWW-сторінки для доступу до інформаційних ресурсів організації;<br>- володіти методами адаптації інформаційних ресурсів підприємства до розповсюдження їх через глобальні інформаційні мережі;<br>- володіти методами інформаційного наповнення WEB-сайта маркетинговою, рекламною, бібліографічною інформацією, повнотекстовими базами даних;<br>- здійснювати пошук інформації в мережі Інтернет з метою задоволення інформаційних потреб користувачів інформації;<br>- здійснювати розробку рекламно-інформаційних матеріалів для розміщення їх в мережі Інтернет. |

*Контроль*

| ***Типове завдання діяльності*** | ***Уміння*** |
|---|---|
| - інформаційно-аналітичний моніторинг документного потоку мережі Інтернет; | - уміти здійснювати контроль якості і достовірності інформації, що циркулює всередині організації і тієї, що надходить із зовнішніх джерел |

## ТЕМА 3:

## «Загрози інформаційній безпеці та необхідність захисту інформації на підприємстві»

## ПЛАН

3.1. Причини захисту інформації
3.2. Поняття та класифікація загроз інформаційній безпеці підприємства

### Література:


1. Игнатьев В.А. Інформаційна безпека сучасного комерційного підприємства: Монография. – Старий Оскол: ООО «ТНТ», 2005. – 448 с.
2. Анапский Е.В. Захист інформації основа безпеки бізнесу [Електронний ресурс] – Джерело доступу: http://www.bezpeka.com/.
3. Исаев В. Як обґрунтувати витрати на інформаційну безпеку? [Електронний ресурс] – Джерело доступу: http://www.isaca.ru/.
4. Кузнецов И.Н. Інформація: збір, захист, аналіз. М.: ООО Изд. Яуза, 2001. – 255 с.
5. Лаврентьев А.В. Рекомендації щодо організації системи захисту інформації [Електронний ресурс] – Джерело доступу: http://www.bezpeka.com/.
6. Маслянко П.П. Концепція управління безпекою інформації в корпоративних структурах [Електронний ресурс] – Джерело доступу: http://www.bezpeka.com/.
7. Кавун С.В. Інформаційна безпека в бізнесі. Наукове видання. – Харків: Изд. ХНЭУ, 2007. – 408 с.
8. Петраков А.В. Основи практичної захисту інформації. Навч. посібник. – 2-е вид. – М.: Радіо і звязок, 2000. – 368 с.


### 3.1. Причини захисту інформації

Безпека підприємницької діяльності – це той випадок, коли краще попередити можливі неприємності, ніж вирішувати проблеми. Багато ризиків в підприємницької діяльності можна прорахувати заздалегідь. Найкраще задуматися про безпеку бізнесу в той момент, коли прийшла ідея створити своє підприємство, витратити деяку кількість сил і засобів на початковому етапі та виправити свої можливі прорахунки і помилки на папері, коли уявлення про те, що таке власний бізнес, як він виглядає, як розвиватиметься, чи ще тільки формується – значно простіше і дешевше, ніж ламати вже вибудуваний і працюючий механізм. Крім того, замислюватися про проблеми безпеки треба щоразу, коли бізнес зазнає будь-яких змін. Треба постаратися відповісти на питання: хто від цих змін може постраждати (хоча б опосередковано)? Наприклад: вирішено встановити систему автоматизації бухгалтерського

обліку. У результаті двоє з чотирьох працівників бухгалтерії стають не потрібні. Одна з працівниць переводиться на нову ділянку, інша звільняється, і вона спрямовує на підприємство податкову інспекцію. Навіть, якщо перевірка податковими органами нічого кримінального не виявить, то час і нерви відніме точно. Інший варіант: вирішено впровадити нову технологію, що істотно спрощує і здешевлює певний виробничий процес. Можна не сумніватися, що компанії зайняті в цій галузі зроблять все, щоб нове технічне рішення так і залишилося нереалізованим – для них це втрата доходу (ринок любить стабільність і добровільно починати цінові війни, переділ зон впливу ніхто не хоче). Ще варіант. Вирішено поширити через мережу роздрібної торгівлі новий вид товару, що відрізняється від того, що зараз представлена на ринку. І все починається досить непогано – попит високий, продажі ростуть. Але при цьому продукція когось іншого, хто на цьому ринку працював до Вас, безнадійно "встала". Швидше за все, цей «хтось» обов'язково поцікавиться, хто Ви такий, наскільки Ви сильні і чи не можна Вас якимось чином «потіснити».

Базисом, на якому будується безпека бізнесу, є комплекс ресурсів, яким володіє будь-який бізнес. Що це за ресурси?

У першу чергу - *підприємницький ресурс* - це потенціал керівника (власника) бізнесу та вищої управлінської ланки: їх освіта, досвід, кваліфікація, нарешті, інтуїція. Саме ці люди приймають рішення про те, куди буде рухатися бізнес, якою буде поведінка фірми на ринку, які кінцеві цілі.

*Матеріальні ресурси* - це і сировина, з якого виробляється кінцевий продукт, що йде на продаж, і кошти на виробництво, основні та оборотні засоби , які є кров'ю бізнесу. Безпека цього сегменту бізнесу безпосередньо залежить від того, якою мірою керівник контролює інфраструктуру обороту, тобто весь ланцюжок надходження та функціонування матеріальних ресурсів. Такий багаторівневий і щільний контроль за матеріальним ресурсом можливий в одному випадку - якщо всі ці ресурси знаходяться в особистій або хоча б колективній власності. У цьому випадку власник має реальні важелі впливу на функціонування ресурсу на різних рівнях.

Наступний ресурс - *інтелектуальний* - це програми, патенти, технології, ліцензії, інформаційні системи. За великим рахунком це те, що забезпечує прогрес у виробництві та захисті комерційної таємниці. Однак тут є суттєва проблема - успішний захист комерційної таємниці, інтелектуальної власності можливий лише в рамках усталеного, регульованого, чітко окресленого правового поля. Закони прописані дуже приблизно, отже, і система їх виконання не працює. Тому підприємець не може реально контролювати інтелектуальний ресурс. Виходячи з такого стану речей, робимо висновок - інтелектуальна безпека бізнесу - справа майбутнього. Може бути - найближчого. Ще один ресурс - *кадровий*. Не викликає сумнівів, що погано навчений, некваліфікований співробітник являє собою пряму загрозу безпеки бізнесу. Однак і постійна зміна персоналу також накладна і підриває добробут фірми. У цій ситуації грамотний керівник (або власник) має повну можливість контролю над ресурсом - впроваджуючи корпоративну ідеологію, вводячи розумну систему заохочень, забезпечуючи соціальні потреби.

Найважливішу роль у захисті бізнесу відіграє інформаційна безпека. Інформація давно перестала бути просто необхідним для виробництва допоміжним ресурсом або побічним проявом всякого роду діяльності. Вона набула вартісної ваги, яка чітко визначається реальним прибутком, одержуваної при її використанні, або розмірами шкоди, з різним ступенем ймовірності завдається власнику інформації. Однак, створення індустрії переробки інформації породжує цілий ряд складних проблем. Однією з таких проблем є надійне забезпечення збереження і встановленого статусу інформації, що циркулює і оброблює в інформаційно-обчислювальних системах і мережах. Дана проблема увійшла в побут під назвою проблеми захисту інформації.

Навіщо захищати інформацію? Відповідей на це питання може бути безліч, залежно від структури і цілей підприємства. Для одних першим завданням є запобігання витоку інформації (маркетингових планів, перспективних розробок тощо) конкурентам. Інші можуть знехтувати конфіденційністю своєї інформації і зосередити увагу на її цілісності. Наприклад, для банку важливо в першу чергу забезпечити незмінюваність оброблюваних платіжних доручень, щоб зловмисник не зміг несанкціоновано дописати в платіжку ще один нулик або змінити реквізити одержувача. Для третіх на перше місце піднімається завдання забезпечення доступності та безвідмовної роботи інформаційних систем. Для провайдера Internet - послуг, компанії, що має Web-сервер, або оператора зв'язку найпершим завданням є саме забезпечення безвідмовної роботи всіх (або найважливіших) вузлів своєї інформаційної системи. Розставити такого роду пріоритети можна тільки за результатами аналізу діяльності підприємства.

Зазвичай, коли мова заходить про безпеку підприємства, його керівництво часто недооцінює важливість інформаційної безпеки. Основний наголос робиться на фізичну безпеку (пропускний режим, охорону, систему відеоспостереження і т.д.). Однак, за останні роки ситуація суттєво змінилася. Для того, щоб проникнути в таємниці підприємства, досить проникнути в інформаційну систему або вивести з ладу будь-який вузол корпоративної мережі. Все це призведе до величезного збитку. Причому не тільки до прямого збитку, який може виражатися в цифрах з багатьма нулями, а й до непрямого. Наприклад, несправність того чи іншого вузла призводить до витрат на відновлення його працездатності, які полягають в оновленні або заміні програмного забезпечення, зарплату обслуговуючого персоналу. Атака на публічний Web-сервер підприємства і заміна його вмісту на будь-яке інше може привести до зниження довіри до фірми і, як наслідок, втрати частини клієнтури і зниження доходів. Від кого ж треба захищатися ? Якщо поставити це питання звичайній людині, то в абсолютній більшості випадків буде відповідь : «Від хакерів». Не вдаючись в термінологію, можна сказати, що, на думку більшості наших співгромадян, основна небезпека виходить саме від зовнішніх зловмисників, які проникають в комп'ютерні системи банків, військових організацій і т.д. Така небезпека існує і не можна її недооцінювати, але вона занадто перебільшена. Звернемося до статистики. Більше половини всіх комп'ютерних злочинів пов'язані з внутрішніми порушеннями, тобто

здійснюються співробітниками своєї компанії, що працюють або звільненими. Свій співробітник може реально оцінити вартість тієї чи іншої інформації, і найчастіше він володіє привілеями, які зайві для нього. « Навіщо моєму співробітнику обкрадати мене?» – може подумати власник підприємства. Причин безліч. найпоширеніша – незадоволеність своїм становищем або зарплатою. Інший приклад - співробітник при звільненні затаїв образу і хоче помститися своїм кривдникам, тобто підприємству або його керівництву. Якщо у своїй роботі він мав досить широкі права, використовуючи їх, він може дуже істотно нашкодити і після свого відходу.

Проте великих бід можна очікувати не від звільнених або скривджених звичайних співробітників (наприклад, операціоністів), а від тих, хто наділений дуже великими повноваженнями і має доступ до широкого спектру різної інформації – це співробітники відділів автоматизації, інформатизації та телекомунікації, які знають паролі до всіх системам, використовуваних в організації. Їх кваліфікація, знання та досвід, використовувані для заподіяння шкоди, можуть призвести до дуже великих проблем. Крім того, таких фахівців важко виявити, оскільки вони володіють достатніми знаннями про систему безпеки організації, щоб обійти використовувані захисні механізми. Тому при побудові системи захисту необхідно захищатися не тільки і не стільки від зовнішніх зловмисників, скільки від зловмисників внутрішніх. На жаль, доводиться констатувати той факт, що багато бізнесменів, керівники комерційних структур, банків належним чином не приділяють цьому постійної уваги і починають турбуватися тоді, коли вже виявлено витік інформації. Проблема полягає не тільки в тому, що злочинні елементи або угруповання збагачуються за рахунок об'єктів злочинної діяльності, а в тому, що це призводить, в кінцевому рахунку, до підриву економіки держави. За уявленнями багатьох бізнесменів турбуватися про можливий витік інформації слід тільки в тому випадку, коли в його діях є кримінал і, як, кажуть, під нього «копають». Насправді це не так. *Що може створювати небезпеку для бізнесменів, зацікавлених, зрозуміло, у дотриманні комерційної таємниці ? Як правило, це:*

- розвідувальна діяльність конкурентів;
- несанкціоновані дії співробітників власної фірми;
- неправильна політика фірми в області безпеки. Інформація, що представляє інтерес при зборі і аналіз відомостей:

а) відомості комерційного змісту:

- статутні документи фірми;
- зведені звіти по фінансовій діяльності фірми (щомісячні, квартальні, річні, за кілька років);
- кредитні договори з банками;
- договори купівлі та продажу;
- відомості про перспективні ринки збуту, джерела коштів або сировини, товарах, про вигідні партнерах;
- будь-яка інформація, надана партнерами, якщо за її розголошення передбачені штрафні санкції;

- дані про конкурентів, їх слабкі і сильні сторони;
- умови фінансової діяльності;
- технологічні секрети;
- заходи, що вживаються конкурентами щодо своїх супротивників;
- дані про потенційних партнерів, перевірка їх на недобросовісність;
- інформація про місце зберігання вантажів, часу і маршрути їх перевезення;
- виявлення вразливих ланок серед співробітників;
- виявлення осіб, перспективних для вербування шляхом підкупу, шантажу чи іншого методу;
- зв'язки і можливості керівництва;
- виявлення кола постійних відвідувачів,

б) відомості особистого характеру:
- джерела доходів;
- справжнє ставлення до тих чи інших суспільних явищ, «сильним світу цього»;
- уклад особистого життя керівника і членів його сім'ї;
- розклад і адреси зустрічей - ділових і особистих;
- дані про розміри фінансового благополуччя;
- інформація про людські слабкості;
- згубні пристрасті;
- шкідливі звички;
- сексуальна орієнтація;
- дані про друзів, подруг, місцях проведення дозвілля, способах і маршрутах пересування;
- інформація про місця зберігання цінностей;
- місце проживання;
- подружня невірність;
- проблеми батьків і дітей.

Необхідно відзначити, що безпека як система заходів вимагає забезпечення необхідного рівня захищеності по ряду напрямків:
- захист від організованої злочинності;
- захист від порушень закону;
- захист від недобросовісної конкуренції;
- захист від правоохоронних і контролюючих органів,

Gartner Group виділяє 4 рівні зрілості компанії з точки зору забезпечення інформаційної безпеки:

0-й рівень:
- інформаційною безпекою в компанії ніхто не займається, керівництво компанії не усвідомлює важливості проблем інформаційної безпеки;
- фінансування відсутнє;

- Інформаційна безпека реалізується штатними засобами операційних систем, СУБД і додатків (парольний захист, розмежування доступу до ресурсів і сервісів).

1- й рівень:

- інформаційна безпека розглядається керівництвом як чисто «технічна» проблема, відсутня єдина програма (концепція, політика) розвитку системи забезпечення інформаційної безпеки (СЗІБ) компанії;

- фінансування ведеться в рамках загального бюджету;

- інформаційна безпека реалізується засобами нульового рівня плюс кошти резервного копіювання, міжмережеві екрани, засоби організації VPN (побудови віртуальних приватних мереж).

2- й рівень:

- інформаційна безпека розглядається керівництвом як комплекс організаційних і технічних заходів, існує розуміння важливості інформаційної безпеки для виробничих процесів, є затверджена керівництвом програма розвитку СЗІБ компанії;

- фінансування ведеться в рамках окремого бюджету;

- інформаційна безпека реалізується засобами першого рівня плюс кошти посиленою аутентифікації, середовища аналізу поштових повідомлень і web - контенту, IDS (системи виявлення вторгнень), засоби аналізу захищеності, SSO (кошти одноразової аутентифікації ), PKI (інфраструктура відкритих ключів) та організаційні заходи (внутрішній і зовнішній аудит, аналіз ризику, політика інформаційної безпеки, положення, процедури, регламенти та керівництва ).

3-й рівень:

- інформаційна безпека є частиною корпоративної культури, призначений CISA (старший адміністратор йо питань забезпечення інформаційної безпеки);

- фінансування ведеться в рамках окремого бюджету;

- інформаційна безпека реалізується засобами другого рівня плюс системи управління інформаційною безпекою, CSIRT (група реагування на інциденти порушення інформаційної безпеки), SLA (угода про рівень сервісу).

За інформацією Gartner Group (дані наводяться за 2015 рік) процентне співвідношення компаній щодо описаних чотирьох рівнів виглядає наступним чином:

0 рівень - 30%,
1 рівень - 55%,
2 рівень - 10%,
3 рівень - 5%.

Прогноз Gartner Group на 2020 рік виглядає наступним чином:

0 рівень - 15%,
1 рівень - 35%,
2 рівень - 35%,
3 рівень - 15%.

Статистика показує, що більшість компаній (55%) зараз впровадили мінімально необхідний набір традиційних технічних засобів захисту (1 рівень). Впровадження додаткових засобів захисту (перехід на рівні 2 і 3) вимагає істотних фінансових вкладень і відповідного обґрунтування. Відсутність єдиної програми розвитку СЗІБ, схваленої і підписаної керівництвом, загострює проблему обґрунтування вкладень у безпеку. В якості такого обґрунтування можуть виступати результати аналізу ризику і статистика, накопичена по інцидентах. Механізми реалізації аналізу ризику та накопичення статистики мають бути прописані в політиці інформаційної безпеки компанії. Процес аналізу ризику складається з 6 послідовних етапів:

- ідентифікація та класифікація об'єктів захисту ( ресурсів компанії, які підлягають захисту);
- категоріювання ресурсів;
- побудова моделі зловмисника;
- ідентифікація, класифікація та аналіз загроз і вразливостей;
- оцінка ризику;
- вибір організаційних заходів і технічних засобів захисту.

На етапі ідентифікації та класифікації об'єктів захисту необхідно провести інвентаризацію ресурсів компанії за наступними напрямками:

- інформаційні ресурси (конфіденційна та критична інформація компанії);
- програмні ресурси (ОС, СУБД, критичні додатки, наприклад ERP);
- фізичні ресурси (сервера, робочі станції, мережеве та телекомунікаційне обладнання);
- сервісні ресурси (електронна пошта, www).

Категоріювання полягає у визначенні рівня конфіденційності та критичності ресурсу. Під конфіденційністю розуміється рівень секретності відомостей, які зберігаються, обробляються і передаються ресурсом. Під критичністю розуміється ступінь впливу ресурсу на ефективність функціонування виробничих процесів компанії (наприклад, у разі простою телекомунікаційних ресурсів компанія-провайдер може розоритися). Присвоївши параметрам конфіденційності та критичності певні якісні значення, можна визначити рівень значимості кожного ресурсу, з точки зору його участі у виробничих процесах компанії. Для визначення значимості ресурсів компанії з точки зору інформаційної безпеки можна скористатися табл. 1.

Таблиця 1

Значимість ресурсів компанії

| Параметр / Значення | Критичний | Значний | Незначний |
|---|---|---|---|
| Строго конфіденційний | 7 | 6 | 5 |
| Конфіденційний | 6 | 5 | 5 |
| Для внутрішнього користування | 5 | 4 | 3 |
| Відкритий | 4 | 3 | 2 |

Наприклад, файли з інформацією про рівень зарплат співробітників компанії мають значення «строго конфіденційно» (параметр конфіденційності)

і значення «незначний» (параметр критичності). Підставивши ці значення в таблицю, можна отримати інтегральний показник значущості даного ресурсу. Різні варіанти методик категорірованія наведені у міжнародному стандарті ISO TR 13335.

**Побудова моделі зловмисника** – це процес класифікації потенційних порушників за такими параметрами:

- тип зловмисника (конкурент, клієнт, розробник, співробітник компанії тощо);
- положення зловмисника по відношенню до об'єктів захисту (внутрішній, зовнішній);
- рівень знань про об'єкти захисту та оточенні (високий, середній, низький);
- рівень можливостей з доступу до об'єктів захисту (максимальні, середні, мінімальні);
- час дії ( постійно, у певні часові інтервали);
- місце дії (передбачуване місце розташування зловмисника під час реалізації атаки).

Присвоївши перерахованим параметрам моделі зловмисника якісні значення можна визначити потейціал зловмисника (інтегральну характеристику можливостей зловмисника з реалізації загроз). Ідентифікація, класифікація та аналіз загроз і вразливостей дозволяють визначити шляхи реалізації атак на об'єкти захисту.

**Вразливості** - це властивості ресурсу або його оточення, використовувані зловмисником для реалізації загроз.

Загрози класифікуються за такими ознаками:

- найменування загрози;
- тип зловмисника;
- засоби реалізації;
- використовувані уразливості;
- скоєних дії;
- частота реалізації.

Основний параметр – частота реалізації загрози. Вона залежить від значень параметрів «потенціал зловмисника» і «захищеність ресурсу». Значення параметра «захищеність ресурсу» визначається шляхом експертних оцінок. При визначенні значення параметра приймаються до уваги суб'єктивні параметри зловмисника: мотивація для реалізації загрози і статистика щодо кількості спроб реалізації загроз даного типу (у разі її наявності). Результатом етапу аналізу загроз і вразливостей є оцінка параметра «частота реалізації» по кожній з загроз. На етапі оцінки ризику визначається потенційний збиток від загроз порушення інформаційної безпеки для кожного ресурсу чи групи ресурсів.

Якісний показник збитку залежить від двох параметрів:

- значимість ресурсу;
- частота реалізації загрози на цей ресурс.

Виходячи з отриманих оцінок збитку, обґрунтовано вибираються адекватні організаційні заходи та технічні середовища захисту.

Єдиним вразливим місцем у пропонованій методиці оцінки ризику і відповідно обґрунтуванні необхідності впровадження нових або зміни існуючих технологій захисту є визначення параметра «частота реалізації загрози». Єдиний шлях отримання об'єктивних значень цього параметра – накопичення статистики по інцидентах. Накопичена статистика, наприклад, за рік, дозволить визначити кількість реалізацій загроз (певного типу) на ресурс (певного типу). Роботу з накопичення статистики доцільно вести в рамках процедури обробки інцидентів. Вона складається з наступних процесів:

- ідентифікація порушення;
- фіксація порушення;
- прийняття рішення про обробку інциденту;
- реєстрація інциденту;
- призначення виконавців;
- супровід обробки інциденту;
- фіксація дій і результатів розслідування;
- визначення шкоди;
- закриття процесу.

Накопичення статистики про інциденти, крім отримання об'єктивних даних, необхідних для обґрунтування вкладень в ІБ, дозволяє оцінити ефективність функціонування СЗІБ. Накопичена за певний часовий інтервал статистика дозволяє відстежити загальну тенденцію у бік зменшення або збільшення кількості інцидентів. Отримати достовірну інформацію про діяльність фірми незаконним шляхом досить важко, якщо фірма з розумінням ставиться до збереження комерційної таємниці та створення відповідної системи захисту. У той же час багато під безпекою розуміють, перш за все, фізичну захищеність, іноді включаючи окремі вимоги інформаційного захисту комерційних інтересів, що не сприяє вирішенню проблем безпеки в комплексі. Кожен комерційний об'єкт повинен будувати свою систему захисту інформації на концептуальній основі, виходячи з призначення об'єкта, його розмірів, умов розміщення, характеру діяльності і т.д. При розробці концепції захисту необхідно виходити з детального аналізу напрямків діяльності підприємницької структури і комплексних вимог захисту. Особливо, якщо структури застосовують у своїй діяльності засоби інформатики.

Враховуючи різноманіття потенційних загроз інформації в системі обробки даних, складність структури і функцій, а також участь людини в технологічному процесі обробки інформації, мети захисту інформації можуть бути досягнуті тільки шляхом створення системи захисту інформації на основі комплексного підходу. І починати створення системи треба з оцінки загроз безпеки діяльності комерційного об'єкта, а виходячи з отриманих результатів аналізу, приймається рішення про побудову всієї системи захисту, і вибираються необхідні кошти.

### 3.2. Поняття та класифікація загроз інформаційній безпеці підприємства

Загрози інформаційній безпеці об'єкта можна розмежувати на внутрішні і зовнішні. Внутрішні загрози безпеки об'єкта захисту:

- некваліфікована корпоративна політика з організації корпоративних інформаційних технологій та управління безпекою корпорації;
- відсутність належної кваліфікації персоналу щодо забезпечення діяльності та управління об'єктом захисту;
- навмисні і ненавмисні дії персоналу з порушення безпеки;
- зрада персоналу;
- техногенні аварії та руйнування, пожежі.

Зовнішні загрози безпеки об'єкта захисту:

- негативні впливи недобросовісних конкурентів і державних структур;
- навмисні і ненавмисні дії зацікавлених структур і фізичних осіб (збір інформації, шантаж, спотворення іміджу, загрози фізичного впливу тощо);
- витік конфіденційної інформації з носіїв інформації і обумовлених каналів зв'язку;
- несанкціоноване проникнення на об'єкт захисту;
- несанкціонований доступ до носіїв інформації і обумовлених каналів зв'язку з метою розкрадання, спотворення, знищення, блокування інформації;
- стихійні лиха та інші форс-мажорні обставини;
- навмисні і ненавмисні дії системних інтеграторів і постачальників послуг із забезпечення безпеки, постачальників технічних і програмних продуктів, кадрів.

***Загальна класифікація загроз автоматизованій інформаційній системі об'єкту виглядає наступним чином:***

**1.** Загрози конфіденційності даних і програм. Реалізуються при несанкціонованому доступі до даних (наприклад, до відомостей про стан рахунків клієнтів банку), програмами або каналах зв'язку. Інформація, що обробляється на комп'ютерах або передається по локальних мережах передачі даних, може бути знята через технічні канали витоку. При цьому використовується апаратура, що здійснює аналіз електромагнітних випромінювань, що виникають при роботі комп'ютера. Таке знімання інформації являє собою складні технічні завдання і вимагає залучення кваліфікованих фахівців. За допомогою приймального пристрою, виконаного на базі стандартного телевізора, можна перехоплювати інформацію, виведену на екрани дисплеїв комп'ютерів з відстані в тисячу і більше метрів. Певні відомості про роботу комп'ютерної системи витягуються навіть у тому випадку, коли ведеться спостереження за процесом обміну повідомленнями без доступу до їх змісту.

**2.** Загрози цілісності даних, програм, апаратури. Цілісність даних і програм порушується при несанкціонованому знищенні, додаванні зайвих елементів і модифікації записів про стан рахунків, зміну порядку розташування

даних, формуванні фальсифікованих платіжних документів у відповідь на законні запити, за активної ретрансляції повідомлень з їх затримкою. Несанкціонована модифікація інформації безпеки системи може призвести до несанкціонованих дій (невірної маршрутизації або втраті передаваних даних) або спотворення сенсу переданих повідомлень. Цілісність апаратури порушується при її пошкодженні, викраденні або незаконній зміні алгоритмів роботи.

**3.** Загрози доступності даних. Виникають в тому випадку, коли об'єкт (користувач або процес) не отримує доступу до законно виділених йому служб або ресурсів. Ця загроза реалізується захопленням всіх ресурсів, блокуванням ліній зв'язку несанкціонованим об'єктом в результаті передачі по них своєї інформації або виключенням необхідної системної інформації. Ця загроза може призвести до ненадійності або поганої якості обслуговування в системі і, отже, потенційно впливатиме на достовірність і своєчасність доставки платіжних документів.

**4.** Загрози відмови від виконання трансакцій. Виникають в тому випадку, коли легальний користувач передає або приймає платіжні документи, а потім заперечує це, щоб зняти з себе відповідальність. Оцінка вразливості автоматизованої інформаційної системи та побудова моделі впливів припускають вивчення всіх варіантів реалізації перерахованих вище загроз і виявлення наслідків, до яких вони призводять. Загрози інформаційної безпеки можуть обумовлюватися як людськими чинниками, так і людино-машинними і машинними чинниками.

*Людські фактори* поділяються на: пасивні загрози (загрози, викликані діяльністю, що носить випадковий, ненавмисний характер) і активні загрози (загрози, зумовлені навмисними діями людей). Це загрози, пов'язані з:

- передачею, спотворенням і знищенням наукових відкриттів, винаходів, секретів виробництва, нових технологій з корисливих та іншим антигромадських мотивів (документація, креслення, описи відкриттів і винаходів та інші матеріали);
- переглядом і передачею різної документації, переглядом «сміття»;
- підслуховуванням і передачею службових та інших науково-технічних і комерційних розмов;
- цілеспрямованим «витоком умів», знань, інформації (наприклад, у зв'язку з отриманням іншого громадянства, з корисливих мотивів).

*Людино-машинні та машинні фактори поділяються на:*

пасивні загрози – це загрози, пов'язані з:

- помилками процесу проектування, розробки та виготовлення систем та їх компонентів (будівлі, споруди, приміщення, комп'ютери, засоби зв'язку, операційні системи, прикладні програми);
- помилками в роботі апаратури через неякісне її виготовлення; з помилками процесу підготовки та обробки інформації (помилки програмістів і користувачів через недостатню кваліфікацію і неякісне обслуговування,

помилки операторів при підготовці, введенні та виведенні даних, коригуванні та обробці інформації).

активні загрози – це загрози, що:

- пов'язані з несанкціонованим доступом до ресурсів автоматизованої інформаційної системи (внесення технічних змін в засоби обчислювальної техніки та засоби зв'язку, підключення до засобів обчислювальної техніки і каналів зв'язку, розкрадання різних видів носіїв інформації: дискет, описів, роздруківок і інших матеріалів, перегляд даних, що вводяться, роздруківок, перегляд «сміття»);

- реалізуються безконтактним способом (збір електромагнітних випромінювань, перехоплення сигналів, що наводяться в ланцюгах, візуально-оптичні способи видобутку інформації, підслуховування службових та науково-технічних розмов).

Існують загрози нанесення збитку системам обробки даних, що викликаються фізичними впливами стихійних природних явищ, які не залежать від людини. Однак більш широке і небезпечне коло штучних загроз, викликаних людською діяльністю, серед яких, виходячи з мотивів, можна виділити:

- ненавмисні загрози, викликані помилками в проектуванні, підготовці, обробці та передачі інформації (науково-технічної, комерційної, валютно-фінансової та ін); помилками в діях обслуговуючого персоналу, програмного забезпечення, випадковими збоями в роботі засобів обчислювальної техніки і ліній зв'язку, енергопостачання, помилками користувачів, впливом на апаратуру фізичних нулів і т.д. Це загрози, пов'язані з помилками процесу; з нецiленапрямленим «витоком мізків», знань, інформації (наприклад, у зв'язку з міграцією населення, виїздом в інші країни для возз'єднання з родиною і т. п.);

- навмисні загрози, зумовлені несанкціонованими діями обслуговуючого персоналу та несанкціонованим доступом (НСД) до інформації сторонніх осіб.

Загрози, не пов'язані з діяльністю людини. Найбільш типовою природною загрозою системам обробки даних, не завжди пов'язаної з діяльністю людини, є пожежа. Тому при проектуванні та експлуатації систем обробки даних в обов'язковому плані вирішуються питання протипожежної безпеки. Особливу увагу при цьому слід приділити захисту від пожежі носіїв комп'ютерних даних, файл-серверів, окремих обчислювальних машин, центрів зв'язку, архівів та іншого устаткування і приміщень або спеціальних контейнерів, де сконцентровані величезні масиви дуже важливої інформації. Для цих цілей можуть бути використані спеціальні вогнетривкі сейфи, контейнери та ін. Інша загроза для систем обробки даних у комп'ютерних системах - удари блискавки. Ця проблема виникає не часто, але збиток може бути завданий дуже великий. Якщо не застосовані необхідні технічні заходи захисту від потужних електромагнітних випромінювань грозових розрядів, виходять з ладу окремі робочі станції або сервери мережі, і на значний час паралізується робота об'єкта, всі операції припиняються. Фірма і особливо банк у такій ситуації втрачає свій імідж надійного партнера і, як наслідок, клієнтів. Для більшості організацій втрата імені, поява чуток про внутрішні проблеми набагато

неприємніше фінансових втрат, часом навіть і досить відчутних. Для будівель, де розміщуються технічні засоби обробки інформації, розташованих в долинах річок або на узбережжі, досить імовірною загрозою є затоплення. У цих випадках апаратні засоби не повинні встановлюватися на нижніх поверхах будівель і повинні застосовуватися інші запобіжні заходи. Нанесення збитку ресурсам систем обробки даних може також бути викликане землетрусами, ураганами, вибухами газу і т.д. Збиток може бути нанесений при технічних аваріях, наприклад, при раптовому відключенні електроживлення і т.д.

Загрози, пов'язані з діяльністю людини. Цей вид загроз можна розділити на:

- загрози системі обробки інформації в результаті несанкціонованого використання штатних технічних і програмних засобів, а також їх розкрадання, псування, руйнування;

- загрози в результаті використання спеціальних засобів, що не входять до складу системи обробки даних (побічні випромінювання, наведення по ланцюгах харчування, використання апаратури звукопідсилення, прийом сигналів з ліній зв'язку, акустичні канали);

- загрози використання спеціальних методів і технічних засобів (фотографування, електронні закладки, руйнують або спотворюють інформацію);

- опромінення технічних засобів зондуючими сигналами, в результаті чого може відбуватися спотворення або руйнування інформації, а при значній потужності опромінення і виведення з ладу апаратури.

Основними типовими шляхами витоку інформації і несанкціонованого доступу до автоматизованих інформаційним системам, в тому числі через канали телекомунікації, є наступні:

- примусове електромагнітне опромінення (підсвічування) ліній зв'язку з метою отримання паразитної модуляції несучої частоти;

- перехоплення електронних випромінювань;

- застосування підслуховуючих пристроїв (закладок);

- дистанційне фотографування;

- перехоплення акустичних випромінювань і відновлення тексту принтера;

- розкрадання носіїв інформації і виробничих відходів;

- зчитування даних у масивах інших користувачів;

- читання залишкової інформації в пам'яті системи після виконання санкціонованих запитів;

- копіювання носіїв інформації з подоланням заходів захисту;

- маскування під зареєстрованого користувача;

- містифікація (маскування під запити системи);

- незаконне підключення до апаратури та ліній зв'язку;

- зловмисний виведення з ладу механізмів захисту;

- використання «програмних пасток».

Можливими каналами навмисного несанкціонованого доступу до інформації за відсутності захисту в автоматизованій інформаційній системі можуть бути:

- штатні канали доступу до інформації (термінали користувачів, засоби відображення та документування інформації, носії інформації, засоби завантаження програмного забезпечення, зовнішні канали зв'язку) при їх незаконному використанні;
- технологічні пульти та органи управління;
- внутрішній монтаж апаратури;
- лінії зв'язку між апаратними засобами;
- побічне електромагнітне випромінювання, що несе інформацію;
- побічні наведення на ланцюгах електроживлення, заземлення апаратури, допоміжних і сторонніх комунікаціях, розміщених поблизу комп'ютерної системи.

Способи впливу загроз на об'єкти інформаційної безпеки поділяються на інформаційні, програмно-математичні, фізичні, радіоелектронні та організаційно-правові.

*Інформаційні:*

- порушення адресності та своєчасності інформаційного обміну, протизаконний збір і використання інформації;
- несанкціонований доступ до інформаційних ресурсів;
- маніпулювання інформацією (дезінформація, приховування або перекручення інформації);
- незаконне копіювання даних в інформаційних системах;
- порушення технології обробки інформації.

*Програмно-математичні:*

- впровадження комп'ютерних вірусів;
- встановлення програмних та апаратних закладних пристроїв;
- знищення або модифікація даних в автоматизованих інформаційних системах.

*Фізичні:*

- знищення або руйнування засобів обробки інформації та зв'язку;
- знищення, руйнування або розкрадання машинних або інших оригінальних носіїв інформації;
- розкрадання програмних або апаратних ключів і засобів криптографічного захисту інформації;
- вплив на персонал;
- поставка «заражених» компонентів автоматизованих інформаційних систем.

*Радіоелектронні:*

- перехоплення інформації в технічних каналах її можливого витоку;
- впровадження електронних пристроїв перехоплення інформації в технічні засоби та приміщення;

- перехоплення, дешифрування і нав'язування помилкової інформації в мережах передачі даних і лініях зв'язку;

- вплив на парольно-ключові системи;

- радіоелектронне придушення ліній зв'язку та систем управління.

*Організаційно-правові:*

- невиконання вимог законодавства та затримки в прийнятті необхідних нормативно-правових положень в інформаційній сфері;

- неправомірне обмеження доступу до документів, що містять важливу для громадян і організацій інформацію.

З усього різноманітного комплексу засобів технічного шпигунства актуальним практично для всіх фірм і організацій, незалежно від виду власності і роду діяльності, є наслідки знімання мовної інформації і випромінювань, які можуть виникати при обробці інформації, в першу чергу за допомогою ЕОМ. Інформація, особливо з обмеженим доступом, повинна працювати, вона марна, якщо замкнена в сейфі (правда, це самий надійний спосіб її зберегти; надійніше може бути тільки знищення інформації разом з її носієм). Тому інформацію обговорюють, обробляють на ЕОМ, зберігають у базах даних, виводять на дисплей, розмножують за допомогою копіювальних апаратів. При цьому з'являється можливість її несанкціонованого перехоплення, виникають технічні канали витоку інформації.

Для більшості фірм і організацій досить складним завданням є прийняття правильного рішення про необхідність і обсяги проведенні заходів з технічного захисту інформації. Пов'язано це з тим, що, на відміну від матеріальних цінностей, не завжди можливо однозначно визначити збитки від витоку інформації. У результаті заходів щодо захисту інформації можуть бути неадекватні можливим загрозам. У ряді випадків керівництво фірм недооцінює ризик витоку інформації, що може призвести до значного збитку. Іноді витрати на захист можуть значно перевищувати можливі втрати від її витоку. Не маючи можливості самостійно провести перевірку об'єктів і створити адекватну систему захисту, керівництво змушене звертатися до фахівців. При цьому існує небезпека зловживання з боку недобросовісних виконавців, які з корисливою метою можуть перебільшити небезпеку і завищити обсяг робіт. Перш за все, керівництву фірми необхідно оцінити небезпеку застосування технічних засобів розвідки (ТСР). Критерієм небезпеки може бути ймовірність застосування тих чи інших ТСР або їх сукупності з урахуванням технічних можливостей різних засобів розвідки з відновлення перехопленої інформації. Достовірна статистика або кількісні критерії визначення ймовірності застосування ТСР відсутні, тому оцінка їх небезпеки і вибір необхідного рівня захисту носять якісний характер, заснований на об'єктивних оцінках. Імовірність застосування ТСР в першу чергу залежить від характеристик діяльності фірми. Для державних установ визначальним, природно, є гриф секретності інформації з обмеженим доступом.

Для комерційних структур, що не використовують секретних відомостей, основними критеріями, що визначають загрозу застосування ТСР, є наступні:

- річний оборот;
- кількість співробітників, що мають доступ до інформації з обмеженим доступом;
- оцінка керівництвом фірми зацікавленості в її інформації.

Чим більший річний оборот, тим вище ймовірність використання ТСР ймовірним противником. Вона незначна при річному обороті в тисячах USD, і досить висока при обороті в мільйони USD. З зростанням обороту зростає загроза застосування ТСР.

Цілком очевидно, що чим менше співробітників допущено до певної, досить важливої інформації, тим вище ймовірність застосування «противником» ТСР для її отримання. При великій кількості поінформованих співробітників різко зростає небезпека витоку інформації через них, без застосування ТСР. Можуть бути застосовані наступні критерії оцінки - від мінімальної загрози до максимальної. Допущені до інформації:

1) усі співробітники;
2) окремі підрозділи;
3) керівники підрозділів;
4) керівництво фірми.

Оцінка керівництвом фірми про зацікавленість в її інформації. Думка керівництва досить суб'єктивна, вона може дати як завищену, так і занижену оцінку. Однак, рішення про захист інформації приймає керівництво і його думки не можна не враховувати. Крім того, інші критерії більш об'єктивні і якоюсь мірою компенсують суб'єктивність самооцінки. Загалом ця оцінка менше впливає на кінцевий результат. Рівні загроз за даним критерієм можна визначити на підставі відповіді керівництва на питання: «Чи становить інтерес для «противника» інформація про фірму?»:

1. ні;
2. малоймовірно;
3. не виключено;
4. цілком можливо;
5. безумовно.

Додатковим фактором, що має суттєве значення при прийнятті рішення про обсяг заходів щодо захисту інформації від технічних розвідок є, так звані, умови розташування. Мінімальний ризик буде мати місце, якщо організація (фірма) має власну будівлю з прилеглою територією, що охороняється. Істотно складніше і дорожче обійдеться система захисту в будинку, що має кілька власників (орендарів). У будь-якому випадку вимоги до системи захисту істотно зростають, якщо поблизу офісу, що охороняється, розташовані (або можуть розташовуватися) структури, зацікавлені в отриманні конфіденційної інформації. У результаті можна оцінити загальний рівень загрози трансформаційних змін ТСР і розробити відповідну систему захисту.

## ТЕМА 4:

## «Канали витоку інформації на підприємстві»

## ПЛАН

4.1. Групи каналів витоку інформації на підприємстві

4.2. Витік акустичної інформації через застосування підслуховуючих пристроїв

4.2.1. Мікрофони

4.2.2. Диктофони та магнітофони

4.2.3. Радіомікрофони

4.3. Витік інформації за рахунок таємного і дистанційного відеоспостереження, лазерного збору мовної інформації

4.4. Шляхи витоку інформації в обчислювальних системах

4.5 Витік інформації за рахунок ПЕМВН, витік інформації при використанні засобів зв'язку і різних провідних комунікацій

## Література:


1. Игнатьев В.А. Информационная безопасность современного коммерческого предприятия: Монография. – Старый Оскол: ООО «ТНТ», 2005. – 448 с.

2. Защита информации в компьютерных системах / Под ред. Э.М.Шмакова. – СПб.: СПбГТУ, 1993. – 100 с.

3. Защита информации в персональных ЭВМ / А.В. Спесивцев, В.А. Вегнер, А.Ю. Крутяков и др. – М.: Радио и связь, МП "Веста", 1992. – 192 с.

4. Герасименко В.А. Основы защиты информации / В.А. Герасименко, А.А. Малюк. – М.: МОПО РФ – МГИФИ, 1997. – 538 с.

5. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ-Санкт-Петербург, 2000. – 384 с.

6. Стенг Дэвид. Секреты безопасности сетей / Дэвид Стенг, Сильвия Муи. – К.: "Диалектика", Информейшн Компьютер Энтерпрайз, 1996. – 544 с.

7. Ухлинов Л.М. Управление безопасностью информации в автоматизированных системах. – М.: МИФИ, 1995. – 128 с.

8. Ярочкин В.И. Безопасность информационных систем. – М.: Ось-89, 1997. – 320 с.


### 4.1. Групи каналів витоку інформації на підприємстві

Можливі канали витоку інформації на підприємстві можна розбити на чотири групи.

1-а група - канали, пов'язані з доступом до елементів системи обробки даних, але не потребують зміни системи. До цієї групи відносяться канали, які утворюються за рахунок:

- дистанційного прихованого відеоспостереження або фотографування;

- застосування підслуховуючих пристроїв;

- перехоплення електромагнітних випромінювань і наведень і т.д.

2- а група - канали, пов'язані з доступом до елементів системи і зміною, структури її компонентів. До другої групи належать:

- спостереження за інформацією з метою її запам'ятовування в процесі обробки;

- розкрадання носіїв інформації;

- збір виробничих відходів, що містять оброблювану інформацію;

- навмисне зчитування даних з файлів інших користувачів;

- читання залишкової інформації, тобто даних, що залишаються на магнітних носіях після виконання завдань;

- копіювання носіїв інформації;

- навмисне використання для доступу до інформації терміналів зареєстрованих користувачів;

- маскування під зареєстрованого користувача шляхом викрадення паролів та інших реквізитів розмежування доступу до інформації, використовуваної в системах обробки;

- використання для доступу до інформації так званих « люків », дір і « лазівок », тобто можливостей обходу механізму розмежування доступу, що виникають внаслідок недосконалості загальносистемних компонентів програмного забезпечення ( операційних систем, систем управління базами даних тощо) і неоднозначною мов програмування застосовуються в автоматизованих системах обробки даних.

3-тя група - до якої належать:

- незаконне підключення спеціальної реєструючої апаратури до пристроїв системи або ліній зв'язку (перехоплення модемного і факсимільного зв'язку);

- зловмисне зміна програм таким чином, щоб ці програми поряд з основними функціями обробки інформації здійснювали також несанкціонований збір і реєстрацію інформації, що захищається;

- зловмисне виведення з ладу механізмів захисту.

4- а група - до якої належать:

- несанкціоноване отримання інформації шляхом підкупу чи шантажу посадових осіб відповідних служб;

- отримання інформації шляхом підкупу і шантажу співробітників, знайомих, обслуговуючого персоналу або родичів, які знають про рід діяльності.

Канали несанкціонованого доступу (НСД) до інформації, за якими можна здійснити її розкрадання, зміна або знищення можна класифікувати таким чином:

Доступ через людину:

- розкрадання носіїв інформації;

- читання інформації з екрана або клавіатури;

- читання інформації з роздруківки.

Доступ через програму:

- перехоплення паролів;

- дешифрування зашифрованої інформації;
- копіювання інформації з носія.

Доступ через апаратуру:

- підключення спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;
- перехоплення побічних електромагнітних випромінювань від апаратури, ліній зв'язку, мереж електроживлення і т.д.

## 4.2. Витік акустичної інформації через застосування підслуховуючих пристроїв

Для перехоплення та реєстрації акустичної інформації існує величезний арсенал різноманітних засобів розвідки: мікрофони, електронні стетоскопи, радіомікрофони або так звані «радіозакладки», спрямовані й лазерні мікрофони, апаратура магнітного запису. Набір засобів акустичної розвідки, використовуваних для вирішення конкретного завдання, залежить від можливості доступу агента в контрольоване приміщення або до зацікавлених осіб.

Застосування тих чи інших засобів акустичного контролю залежить від умов застосування, поставленого завдання, технічних і, перш за все, фінансових можливостей організаторів підслуховування.

### 4.2.1. Мікрофони

У тому випадку, якщо є постійний доступ до об'єкта контролю, можуть бути використані найпростіші мініатюрні мікрофони, сполучні лінії яких виводять в сусідні приміщення для реєстрації і подальшого прослуховування акустичної інформації. Такі мікрофони діаметром 2,5 мм можуть вловлювати нормальний людський голос з відстані до 10-15 м. Разом з мікрофоном в контрольованому приміщенні, як правило, приховано встановлюють мініатюрний підсилювач з компресором для збільшення динамічного діапазону акустичних сигналів і забезпечення передачі акустичної інформації на значні відстані. Ці відстані в сучасних виробах досягають до 500 метрів і більше, тобто служба безпеки фірми, що займає багатоповерховий офіс (або зловмисник ), може прослуховувати будь-яке приміщення в будівлі. При цьому провідні лінії найчастіше від декількох приміщень зводяться в одне на спеціальний пульт і операторові залишається лише вибірково прослуховувати будь-яке з них і, при необхідності, записувати розмови на магнітофон або жорсткий диск комп'ютера для збереження і подальшого прослуховування. Для одночасної реєстрації акустичних сигналів від окремих приміщень (від 2-х до 32-х) існують багатоканальні реєстратори створені на базі ПЕОМ. Такі реєстратори найчастіше використовуються для контролю акустичної інформації приміщень та телефонних розмов. Вони мають різні додаткові функції, такі як визначення вхідних і вихідних номерів телефонів, ведення журналів і протоколів сеансів зв'язку.

Мікрофони можуть бути введені через вентиляційні канали на рівень контрольованого приміщення, яке може прослуховуватися з іншого приміщення, горища будівлі або з даху в місцях виходу вентиляційного колодязя. При цьому не обов'язково сидіти на даху, досить встановити диктофон з можливістю запису на кілька годин і отримати можливість управління записом за рівнем акустичного сигналу, що дозволяє всі розмови в контрольованому приміщенні записувати досить тривалий час без зміни касет. Крім безпосереднього перехоплення звукових коливань окремі мікрофони (т.зв. мікрофони-стетоскопи) можуть сприймати звукові коливання, що розповсюджуються з контрольованого приміщення по будівельних конструкціях будівлі (стіни, труби опалення, двері, вікна тощо). Їх використовують для прослуховування розмов крізь стіни, вікна, двері. Контрольний пункт для прослуховування розмов за допомогою мікрофонів-стетоскопов може бути обладнаний в безпечному місці будівлі на значній відстані від контрольованого приміщення. Сучасною промисловістю випускаються багато модифікацій мікрофонів спрямованої дії, які сприймають і підсилюють звуки, що йдуть з одного виправлення і послаблюють всі інші звуки. Конструкції вузькоспрямованих мікрофонів самі різні. Це і форма тростини або парасольки, і мікрофони, які використовують параболічні концентратори звуку трубки органного типу або акустичні решітки. Так, направлений мікрофон з параболічним концентратором діаметром 43 см, підсилювачем і головними телефонами, дозволяє прослуховувати розмови на відкритому місці з відстаней до 1 км.

### 4.2.2. Диктофони та магнітофони

Якщо зловмисник не має постійного доступу до об'єкта, але є можливість його короткочасного відвідування під різними приводами, то для акустичної розвідки використовуються радіомікрофони, мініатюрні диктофони і магнітофони, закамуфльовані під предмети повсякденного побуту: книгу, письмові прилади, пачку сигарет, авторучку. Крім цього, диктофон може перебувати у одного з осіб, присутніх на закритій нараді. У цьому випадку часто використовують виносний мікрофон, захований під одягом або закамуфльований під годинник, авторучку, гудзик. Приховано встановлений в аташе-кейсі малогабаритний магнітофон може непомітно включатися за допомогою простої кулькової ручки.

Сучасні диктофони забезпечують безперервний запис мовної інформації від 30 хвилин до декількох годин, вони оснащені системами акустопуска (VOX, VAS ), тобто управлінням по рівню акустичного сигналу, автореверса, індикації дати і часу запису, дистанційного керування. Вибір диктофонів сьогодні дуже великий. З описаними функціями можна підібрати модель диктофона фірм Olympus, Sony, Pansonic, Uher тощо. У деяких моделях диктофонів як носій інформації використовуються цифрові мікрочіпи і міні-диски, записану на такому диктофоні мовну інформацію можна переписувати на жорсткі диски комп'ютерів для зберігання, архівації і подальшого прослуховування.

Серйозною перевагою цифрових диктофонів є те, що вони не виявляють себе при роботі, на відміну від касетних, які виявляються спеціальними приладами по електромагнітним випромінюванням працюючого двигуна механізму протягування стрічки і характерним клацаннях при переході на іншу доріжку в режимі автореверса.

### 4.2.3. Радіомікрофони

Радіомікрофони є найпоширенішими технічними засобами знімання акустичної інформації. Їх популярність пояснюється простотою користування, відносною дешевизною, малими розмірами і можливістю камуфляжу. Різноманітність радіомікрофонів або, так званих «радіозакладок» настільки велике, що потрібна окрема класифікація. Радіомікрофони поділяють на:

- радіомікрофони з параметричною стабілізацією частоти;
- радіомікрофони з кварцовою стабілізацією частоти. Параметрична стабілізація частоти не може претендувати на високу якість передачі через відхід частоти в залежності від місця розташування, температури та інших дестабілізуючих факторів (особливо, якщо радіомікрофон виконаний як ношений варіант і розміщується на тілі людини ). Кварцова стабілізація частоти або як називають часто фахівці «кварцованні закладки» позбавлені цього недоліку.

Всі заставні пристрої можна розділити на кілька типів:

- що працюють постійно;
- з вбудованими таймерами, що включаються в певний час;
- керовані дистанційно;
- що працюють в режимі очікування.

Радіозакладки працюють як звичайний передавач. Як джерело електроживлення радіозакладок використовуються малогабаритні акумулятори. Термін роботи подібних закладок визначається часом роботи акумулятора. При безперервній роботі це 1-2 доби. Закладки можуть бути досить складними (використовувати системи накопичення і передачі сигналів, пристрої дистанційного накопичення). Найпростіші радіозакладки містять три основних вузла, що визначають технічні можливості та методи їх використання:

- мікрофон, що визначає зону акустичної чутливості радіозакладки;
- радіопередавач, що визначає дальності дії і таємність роботи;
- джерело живлення, від якого залежить тривалість безперервної роботи.

Для підвищення таємності роботи потужність передавача робиться невеликою, достатньою для перехоплення високочутливим приймачем з невеликої відстані. Висока таємність нерідко досягається і вибором робочої частоти, коли частота вибирається поблизу несучої потужної радіостанції і маскуються її сигналами. Мікрофони, використовувані в радіозакладках, можуть бути вбудованими або виносними і бувають двох типів:

- акустичні (чутливі в основному до дії звукових коливань повітря і призначені для перехоплення мовних повідомлень);

- вібраційні (перетворюють в електричні сигнали коливання, що у різноманітних жорстких конструкціях).

Робоча частота радізакладок може бути будь-яка, але в даний час найбільше застосування знаходять радіокапсули діапазону від 40 МГц до 1,5 ГГц. У тих випадках, коли неможлива установка радіозакладки безпосередньо на об'єкті, застосовуються стетоскопні датчики, які дозволяють прослухати переговори через перешкоду, стіни, скло, корпус автомобіля і т.д., причому, чим твердішою і одно ріднішою є перешкода, тим краще вони працюють. Радіозакладки можна також класифікувати за такими ознаками:

- діапазону використовуваних частот (від 20 МГц до 1.5 ГГц);
- довготривалості роботи (від 30 хвилин до 25 років);
- дистанції передачі ( від 15 м до 10 км);
- виду модуляції.

Фізична таємність радіозакладок визначається їх маскуванням в контрольованому приміщенні. Проте в кожному приміщенні є цілий ряд пристроїв, які виглядають цілком звичайними і можуть перебувати на видному місці, не викликаючи навіть найменшої підозри, тому що найчастіше радіомікрофони виготовляються в камуфльованому вигляді (авторучки, запальнички, картонки, предмети інтер'єру і т.д.). Дальність дії радіомікрофонів в основному залежить від потужності передавача, несучої частоти, виду модуляції і властивостей приймального пристрою. Час безперервної роботи багато в чому залежить від організації живлення виробу. Якщо радіомікрофон живиться від мережі 220 В, а такого типу « закладки » найчастіше виконуються у вигляді трійників, розеток, подовжувачів, то час роботи не обмежений. Якщо живлення здійснюється від батарей або акумуляторів, то вихід з положення знаходять у застосуванні режиму акустопуска (управління голосом), використання дистанційного керування (ДУ) включенням або збільшенням ємності батарей. З цього короткого опису випливає, що дальність дії, габарити і час безперервної роботи дуже взаємопов'язані. Справді, для збільшення дальності треба підняти потужність передавача, одночасно зростає струм споживання від джерела живлення, а значить, скорочується час безперервної роботи. Щоб збільшити цей час, збільшують ємність батарей живлення, але при цьому ростуть габарити радіомікрофона. Крім того, слід враховувати, що збільшення потужності передавача знижує його таємність, тобто його легше виявити застосовуючи навіть не дуже складну і дорогу пошукову техніку.

*Приймальні пристрої.* Прийом сигналів з радіомікрофонів здійснюється на стандартні FM-приймачі або спеціально виготовлені контрольні пункти з можливістю звукозапису. Найчастіше для прийому акустичних сигналів від радіомікрофонів застосовують скануючі приймачі ( сканери ), використовують також побутові радіоприймачі з встановленим конвертером для прийому сигналів в потрібному діапазоні частот. Переважним є застосування магнітол, тому що з'являється можливість одночасного прослуховування та ведення запису. Скануючі приймачі і створювані на їх основі комплекси, крім функцій звичайного радіоприйому, виконують радіомоніторинг широкого спектру радіочастот. Спільно з програмами управління вони забезпечують в

автоматизованому та автоматичному режимах відображення радіообстановки на екрані комп'ютера, накопичення інформації за прийнятими сигналами, аналіз поточної і архівної інформації з формуванням звітів про виконану роботу.

Вони виконують такі завдання:

- виявлення випромінювань спеціальних технічних засобів несанкціонованого знімання інформації і їх локалізацію;
- виявлення інформативних побічних електромагнітних випромінювань і наведень, що виникають при роботі обчислювальної техніки, засобів зв'язку, оргтехніки;
- оцінку ефективності використання технічних засобів захисту інформації;
- контроль виконання обмежень і дотримання дисципліни зв'язку при використанні відкритих каналів радіозв'язку радіоелектронними засобами;
- контроль сіток частот різних систем радіозв'язку; накопичення даних з радіоелектронної обстановки в точці прийому та виявлення нових сигналів;
- контроль списку фіксованих частот радіоелектронних засобів з різними параметрами випромінюваного сигналу;
- оцінку завантаженості заданих діапазонів та інтенсивності використання фіксованих частот;
- оцінку електромагнітної сумісності радіоелектронних засобів (РЕЗ);
- аналіз індивідуальних особливостей спектру окремого радіосигналу.

### 4.3. Витік інформації за рахунок таємного і дистанційного відеоспостереження, лазерного збору мовної інформації

З предметів даного типу найбільш широко застосовуються та приховано встановлюються фото-, кіно-, і відеокамери з вихідним отвором об'єктива кілька міліметрів. Використовуються також мініатюрні відео системи, що складаються з мікровідеокамери з високою чутливістю і мікрофону. Для конспіративного спостереження використовуються також мікровідеокамери в настінних годинах, в датчиках пожежної сигналізації, невеликих радіомагнітолах, а також у краватці або ремені брюк. Відеозображення може записуватися на малогабаритний відеомагнітофон або передаватися за допомогою малогабаритного передавача по радіоканалу в інше приміщення чи автомашину на спеціальний або стандартний телеприймач. Відстань передачі, залежно від потужності передачі сягає від 200 метрів до 1 км. При використанні ретрансляторів відстань передачі може бути значно збільшено.

Для дистанційного перехоплення інформації (мови) з приміщень іноді використовують лазерні пристрої. З пункту спостереження в напрямку джерела звуку надсилається зондуючий промінь. Зондуючий промінь зазвичай спрямовується на скло вікон, дзеркала, інші відбивачі. Всі ці предмети під дією мовних сигналів циркулюючих в приміщенні, коливаються і своїми коливаннями модулюють лазерний промінь, прийнявши який у пункті спостереження, можна шляхом нескладних перетворень відновити всі мовні сигнали, циркулюючі в контрольованому приміщенні. На сьогоднішній день створено ціле сімейство лазерних засобів акустичної розвідки. Такі пристрої

складаються з джерела випромінювання (гелій-неоновий лазер), приймачів цього випромінювання з блоком фільтрації шумів, пари головних телефонів, акумулятора живлення та штатива. Наводка лазерного випромінювання на віконне скло потрібного приміщення здійснюється за допомогою телескопічного візира. Знімання мовної інформації з віконних рам з подвійними скельцями з гарною якістю забезпечується з відстані до 250 метрів. Такою можливістю, зокрема, володіє система SIPE LASER 3- DA SUPER виробництва США.

Однак, на якість прийнятої інформації, крім параметрів системи впливають такі чинники:

- параметри атмосфери (розсіяння, поглинання, турбулентність, рівень фону);
- якість обробки зондуючої поверхні (шорсткості і нерівності, зумовлені як технологічними причинами, так і впливом середовища - бруд, подряпини);
- рівень фонових акустичних шумів;
- рівень перехопленого мовного сигналу.

Крім того, застосування подібних засобів вимагає великих витрат не тільки на саму систему, а й на обладнання з обробки отриманої інформації. Застосування такої складної системи вимагає високої кваліфікації і серйозної підготовки операторів. З усього цього можна зробити висновок, що застосування лазерного знімання мовної інформації дороге задоволення і досить складне, тому треба ретельно оцінити необхідність захисту інформації від цього виду розвідки.

### 4.4. Шляхи витоку інформації в обчислювальних системах

Питання безпеки обробки інформації в комп'ютерних системах є предметом заклопотаності спеціалістів, так як з'явилася велика кількість фірм і установ, ефективна діяльність яких практично немислима без використання комп'ютерів. Зарубіжний досвід підказує, що саме на стадії обробки інформації існують максимально сприятливі умови для проникнення до неї. Розглянемо класифікацію і принципи оцінки безпеки комп'ютерних систем, які використовуються в США.

Розрізняють два типи некоректного використання ЕОМ:

- доступ до ЕОМ осіб, які не мають на це права;
- неправильні дії тих осіб, які мають право на доступ до ЕОМ (так званий санкціонований доступ).

Зазвичай, розробників систем хвилює тільки рішення другої проблеми. Аналіз ймовірних шляхів витоку інформації або її спотворення показує, що за відсутності спеціальних заходів захисту забезпечують виконання функцій, покладених на обчислювальну систему, можливо:

- зняття дистанційними технічними засобами секретних повідомлень з моніторів ЕОМ, з принтерів (перехоплення електромагнітних випромінювань;
- отримання інформації оброблюваної в ЕВМ.по ланцюгах харчування;
- акустична або електроакустична витік інформації, що вводиться;

- перехоплення повідомлень в каналі зв'язку;
- нав'язування помилкового повідомлення;
- зчитування (зміна) інформації ЕОМ при несанкціонованому доступі;
- розкрадання носіїв інформації і виробничих відходів;
- читання залишкової інформації в системі після виконання санкціонованих запитів;
- копіювання носіїв інформації;
- несанкціоноване використання терміналів зареєстрованих користувачів;
- маскування під зареєстрованого користувача за допомогою розкрадання паролів і інших реквізитів розмежування доступу;
- маскування несанкціонованих запитів під запити операційної системи (містифікація);
- використання програмних пасток;
- отримання даних, що захищаються за допомогою серії запитів;
- використання недоліків мов програмування і операційних систем;
- навмисне включення до бібліотеки програм спеціальних блоків типу «троянських коней»;
- зловмисне виведення з ладу механізмів захисту. В окрему групу слід виділити спеціальні закладки для знімання інформації з комп'ютерів.

Мініатюрний радіомаяк, вбудований в упаковку, дозволяє простежити весь шлях прямування закупленої ЕОМ, транслюючи сигнали на спеціальний передавач. Дізнавшись таким шляхом, де встановлена машина, можна приймати будь-яку оброблену комп'ютером інформацію через спеціально вмонтовані електронні блоки, що не відносяться до ЕОМ, але беруть участь у її роботі. Найефективніший захист від цієї закладки - екрановане приміщення для обчислювального центру. На думку фахівців універсальних «комп'ютерних закладок» сьогодні не буває. Ті закладки, які вдавалося виявити, можна умовно розділити на три типи:
- закладки, які вибирають інформацію за ключовими словами або знакам;
- закладки, які передають всю інформацію, що знаходиться на вінчестері ЕОМ;
- закладки, що знищують інформацію.

### 4.5. Витік інформації за рахунок ПЕМВН, витік інформації при використанні засобів зв'язку і різних провідних комунікацій

Однією з найбільш ймовірних загроз перехоплення інформації в системах обробки даних вважається витік за рахунок перехоплення побічних електромагнітних випромінювань і наведень (ПЕМВН), створюваних технічними засобами. ПЕМВН існують в діапазоні частот від одиниць Гц до півтора ГГц і здатні переносити (поширювати) повідомлення, оброблювані в автоматизованих системах. Дальність розповсюдження ПЕМІ обчислюється десятками, сотнями, а іноді й тисячами метрів. Найбільш небезпечними джерелами ПЕМВН є дисплеї, провідні лінії зв'язку, накопичувачі на магнітних дисках і літеродрукувальні апарати послідовного типу. Наприклад, з дисплеїв

можна зняти інформацію за допомогою спеціальної апаратури на відстані до 500-1500 метрів, з принтерів до 100-150 метрів. Перехоплення ПЕМВН може здійснюватися і за допомогою портативної апаратури. Така апаратура може являти собою широкосмуговий автоматизований приймач. У якості пристроїв реєстрації прийнятих сигналів (повідомлень) може використовуватися магнітний носій або дисплей.

Витік інформації при використанні засобів зв'язку і різних провідних комунікацій.

В даному випадку, коли мова заходить про можливість перехоплення інформації при використанні ліній зв'язку та провідних комунікацій, слід мати на увазі, що перехоплення може здійснюватися не тільки з телефонних ліній і не тільки мовної інформації. У цей розділ можна віднести:

- прослуховування і запис переговорів по телефонних лініях;
- використання телефонних ліній для дистанційного знімання аудіо-інформації з контрольованих приміщень;
- перехоплення факсимільної інформації;
- перехоплення розмов по радіотелефону і стільниковому зв'язку;
- використання мережі 220 В і ліній охоронної сигналізації для передачі акустичної інформації з приміщень;
- перехоплення пейджингових повідомлень.

## ТЕМА 5:

## «Стандарти інформаційної безпеки»

## ПЛАН

5.1. Поняття та види стандартів інформаційної безпеки в Україні та світі
5.2. Основні положення "Критеріїв ДСТС ЗІ СБУ" (Держспецзв'язку)

### Література:


1. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч. 2 / С.В. Кавун, В.В. Носов, О.В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 196 с.
2. Кавун С.В. Информационная безопасность в бизнесе. Научное издание. / С.В. Кавун. – Харьков: Изд. ХНЭУ, 2007. – 408 с.
3. Анин Б.Ю. Защита компьютерной информации / Анин Б.Ю. – СПб.: БХВ-Санкт-Петербург, 2000. – 384 с.
4. Гайкович В.Ю. Безопасность электронных банковских систем / В.Ю. Гайкович, А.Ю. Першин. – М.: Единая Европа, 1994. – 363 с.
5. Гаффин Адам. Путеводитель по глобальной компьютерной сети. – М.: ТПП «Сфера», 1995. – 282 с.
6. Герасименко В.А. Основы защиты информации / В.А. Герасименко, А.А. Малюк. – М.: МОПО РФ – МГИФИ, 1997. – 538 с.
7. Защита прав создателей и пользователей программ для ЭВМ и баз данних. – М.: Ось, 1996. – 186 с.
8. Защита информации в персональных ЭВМ / А.В. Спесивцев, В.А. Вегнер, А.Ю. Крутяков. – М.: Радио и связь, МП "Веста", 1992. – 192 с.
9. Олейников Е. А. Экономическая и национальная безопасность: учебник для вузов. – М.: Экзамен, 2005. – 766 с.
10. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньш. – М.: ДМК Пресс, 2002. – 656 с.
11. Специвцев А.В. Защита информации в персональных ЭВМ / А.В. Специвцев, В.А. Вегнер, А.Ю. Крутяков. – М.: Радио и связь, 1992. – 192 с.


### 5.1. Поняття та види стандартів інформаційної безпеки в Україні та світі

В Україні нормативно-правову базу щодо захисту інформації в КС від несанкціонованого доступу (НСД) складають відкриті документи, які, на думку вітчизняних фахівців у цій сфері, повною мірою не відображають сучасну трансформацію поглядів на процеси обробки інформації та новітні підходи до вирішення проблеми забезпечення ІБ. Новий погляд на проблему безпеки інформаційних технологій був закріплений у міжнародному стандарті ISO/IEC

15408 "Загальні критерії оцінки безпеки інформаційних технологій". Для розуміння основних положень цих документів необхідно розглянути елементи теорії захисту інформації в КС.

Розглядаючи питання безпеки інформації в КС, перш за все, вводять абстрактну модель комп'ютерної системи, і далі говорять про наявність деяких "бажаних" станів даних систем.

Ці бажані стани описують (у термінах моделі власне комп'ютерної системи) ступінь "захищеності" системи. Властивість "захищеності" принципово не відрізняється від будь-яких інших властивостей технічної системи, наприклад, описуваних поняттям "надійної роботи", і є для системи зовнішньою, апріорно заданою.

Поняття "захищеність" взаємопов‘язане з поняттями "джерело загрози" (позначення зовнішньої причини для виведення системи із стану "захищеності"), "загроза" (поняття, що знеособлює причину виведення системи із захищеного стану через дії джерела загрози) і "вразливість" (позначення властивості елемента системи, за допомогою якого реалізується загроза).

Інтегральною характеристикою, що описує властивості системи, яка потребує захисту, є ПБ (політика безпеки) – якісний (або якісно-кількісний) опис властивостей захищеності, виражений у термінах, що описують систему.

У теорії комп‘ютерної безпеки практично завжди розглядається модель довільної КС у вигляді кінцевої множини елементів. Існує два підходи до розподілу зазначеної множини:

*1. На дві підмножини:*

множина об'єктів;

множина суб'єктів.

Даний розподіл заснований на властивості елемента "бути активним" або "одержувати керування" (застосовуються також терміни "використовувати ресурси" або "користуватися обчислювальною потужністю"). Воно історично склалося на основі моделі обчислювальної системи, що належить фон Нейману, згідно з якою послідовність виконуваних інструкцій (програма, відповідна поняттю "суб'єкт") знаходиться в єдиному середовищі з даними (відповідними поняттю "об'єкт").

Властивості суб'єктів:

людина-користувач сприймає об'єкти та одержує інформацію про стан КС через суб'єкти, якими вона керує і які відображають інформацію в придатному для сприйняття людиною вигляді;

загрози компонентам КС виходять від суб'єктів як активної компоненти інформації, що породжує потоки і змінює стан об'єктів у КС;

суб'єкти можуть впливати один на одного через змінювані ними об'єкти, пов'язані з іншими суб'єктами, породжуючи зрештою в системі суб'єкти (або стани системи), які становлять загрозу для безпеки інформації або для працездатності самої системи.

*2. На дві підмножини:*

множина пасивних об'єктів, над якою виконуються операції;

множина активних об'єктів, які виконують або ініціюють ці операції:

об'єкти-користувачі;

об'єкти-процеси.

Термін "суб'єкт", що вживається відповідно до першого підходу, є суперпозицією об'єкта-користувача і об'єкта-процесу другого підходу.

Згідно з другим підходом, усі об'єкти можуть знаходитися в одному з трьох різних станів: об'єкт-користувач, об'єкт-процес і пасивний об'єкт.

Перехід між станами означає, що об'єкт просто розглядається в іншому контексті. Наприклад, пасивний об'єкт переходить у стан об'єкта-користувача, коли фізична особа "входить" у систему. Взаємодія двох об'єктів КС (звернення активного об'єкта до пасивного з метою отримання певного виду доступу) призводить до появи потоку інформації між об'єктами та/або зміни стану системи.

Цей другий підхід використовується у вітчизняних документах із захисту інформації в КС від НСД.

В обох підходах ПБ пов‘язана з поняттям "доступ". *Доступ* – це категорія, що описує процес виконання операцій суб'єктів над об'єктами (об'єктів-користувачів і об'єктів-процесів над пасивними об'єктами).

Наприклад, ПБ для суб'єктно-об'єктної моделі включає опис:

множини можливих операцій над об'єктами;

для кожної пари "суб'єкт-об'єкт" призначення множини дозволених операцій, що є підмножиною всієї безлічі можливих операцій.

Операції пов'язані з цільовою функцією системи, що захищається (тобто з категорією, що описує призначення системи й вирішувані завдання). ПБ описує в загальному випадку нестаціонарний стан захищеності. Система, що захищається, може змінюватися, доповнюватися новими компонентами (суб'єктами, об'єктами, операціями суб'єктів над об'єктами), відповідно, і ПБ повинна бути підтримана в часі, що досягається *керуванням безпекою.*

Не стаціонарність КС, що захищається, а також питання реалізації ПБ в конкретних конструкціях системи, яка захищається, зумовлюють необхідність розгляду завдання *гарантування заданої ПБ*.

Резюмуючи, можна сказати, що теорія комп'ютерної безпеки вирішує чотири класи взаємопов'язаних завдання:

1. Формулювання і вивчення ПБ.

2. Реалізація політик безпеки.

3. Гарантування заданої ПБ.

4. Керування безпекою.

Типовий життєвий цикл КС складається з наступних стадій:

1. Проектування КС і проектування ПБ.

2. Моделювання ПБ і аналіз коректності ПБ, що включає встановлення ступеня її адекватності цільовій функції КС.

3. Реалізація ПБ і механізмів її гарантування, а також процедур і механізмів керування безпекою.

4. Експлуатація захищеної системи.

З метою формування єдиного та формалізованого підходу до захисту інформації в КС, як було вже зазначено, були розроблені стандарти безпеки або

критерії оцінки захищеності, які включають якісні та кількісні показники захищеності.

Стандарти безпеки ефективно сприяють вирішенню наступних проблем у сфері ІБ:

обґрунтоване формування цілей і структуризація завдань у процесі проектування захищених інформаційних систем;

забезпечення об'єктивності оцінок захищеності ІС і технологій;

створення методологічних і методичних підстав для взаємодії між основними учасниками сфери ІБ: виробниками, споживачами, експертами (рис. 1);

формування базису для формалізації описів цілей, завдань, вимог до захищених систем і самих систем у сфері захищених інформаційних технологій;

створення технологій кваліфікаційного аналізу і синтезу захищених інформаційних систем;

розробка технологій перевірки захищеності систем, а також атестації та сертифікації як окремих елементів систем, так і захищених систем у цілому.


Рис. 1. Необхідність взаємодії між основними учасниками у сфері ТЗІ

На сьогодні існує цілий ряд стандартів безпеки. У цьому напрямку ведуться інтенсивні дослідження, тому існуючі стандарти поповнюються й модифікуються, а також з'являються цілком нові стандарти, які враховують досвід раніше створених. Доречно також зазначити, що такого роду стандарти наповнюються великою кількістю окремих методик. Перелік найбільш відомих стандартів наведено у табл. 1.

Таблиця 1

Перелік найбільш відомих стандартів

| **Найменування стандарту** | **Позначення, країна** | **Коротка характеристика** |
|---|---|---|
| Критерії безпеки КС Міністерства оборони США ("Оранжева книга") | TCSEC, США | Були розроблені Міністерством оборони США в 1983 р. з метою визначення вимог безпеки для КС, що висуваються до апаратного, програмного й спеціального забезпечення, а також з метою вироблення методології аналізу ПБ для інформаційних систем військового призначення. Публікація "Оранжевої книги" стала важливим етапом у роботах за стандартами безпеки, оскільки дала основу для нових розробок |
| Європейські критерії безпеки інформаційних технологій ("Європейські критерії") | ITSEC, Великобританія, Франція, Нідерланди, Німеччина | Були розроблені країнами Європи вслід за виходом "Оранжевої книги". У цих критеріях усі засоби захисту інформації розглядаються на трьох рівнях: з погляду цілей, з погляду функцій захисту і з погляду механізмів, що реалізовують захист |
| ГОСТ Р ИСО/МЭК 15408-2002 (імплементовані "Загальні критерії") | Росія | Починаючи з 1992 р. було опубліковано ряд документів з питань захисту інформації від несанкціонованого доступу. Спочатку була розроблена "Концепція захисту засобів обчислювальної техніки від НСД до інформації", що стала ідейною основою для розробки решти документів |
| Федеральні критерії безпеки інформаційних технологій ("Федеральні критерії") | FCTITS, США | Розроблялися як складова національного стандарту з обробки інформації. Документ став узагальненням досліджень 80–90-х рр. у сфері ІБ. Ці критерії стали базою для розробки й сертифікації компонентів інформаційних технологій з погляду підтримання безпеки |
| Канадські критерії безпеки комп'ютерних систем ("Канадські критерії") | CSSCCSE, Канада | "Канадські критерії" розроблялися як основа для оцінки ефективності засобів підтримання безпеки КС з метою вироблення шкали критеріїв оцінки безпеки систем, створення основи для розробки специфікацій безпечних КС, розробки пропозицій із стандартизації опису характеристик безпечних систем |
| Загальні критерії безпеки інформаційних технологій ("Загальні критерії", "Єдині критерії") | CCITSE, ISO/IEC 15408, США, Великобританія, Франція, Канада, Нідерланди | Роботи за цим проектом були розпочаті в 1993 р. Основною метою було усунення концептуальних і технічних відмінностей між Європейськими, Федеральними і Канадськими критеріями. Загальні критерії розроблялися з орієнтацією на інтереси виробників, споживачів і експертів стосовно кваліфікації рівня безпеки |
| Критерії оцінки захищеності інформації в КС від НСД ("Критерії ДСТС ЗІ СБУ" (Держспецзв‘язку)) | Україна | Були введені в 1999 р. Головним управлінням технічного захисту інформації Департаменту спеціальних телекомунікаційних систем і захисту інформації СБУ як національний стандарт. За своєю структурою нагадують "Канадські критерії" |

Далі розкриємо основні та істотні в контексті даних питань, положення "Критеріїв ДСТС ЗІ СБУ" (Держспецзв‘язку).

### 5.2. Основні положення "Критеріїв ДСТС ЗІ СБУ" (Держспецзв'язку)

"Критерії ДСТС ЗІ СБУ" (Держспецзв'язку) розглядають чотири типи загроз:

загрози конфіденційності інформації;

загрози цілісності інформації;

загрози порушення працездатності ІС;

загрози аудиту (спостереженості) системи.

У стандарті використовується поняття об'єкта інформаційного обміну, що відрізняється від інших. Сутність КС розглядається як сукупність об'єктів, а їх взаємодія описується трійкою:

об'єкт-користувач;

об'єкт-процес, що діє від імені користувача;

об'єкт як пасивний елемент.

Такий підхід дозволяє за ситуації, коли один користувач запускає багато процесів, використовувати для опису цієї ситуації один об'єкт-користувач і безліч асоційованих з ним об'єктів-процесів. При цьому ПБ розрахована на одного користувача, що здійснює доступ до об'єктів за допомогою декількох процесів.

Загальна оцінка рівня безпеки системи складається з потужності функціональних вимог комплексу засобів захисту (КЗЗ) і рівня вимог адекватності їх реалізації (рис. 2).


Рис. 2. Складові загальної оцінки рівня безпеки системи

Для забезпечення максимального ступеня абстрагованості та інваріантності щодо ПБ і методів її реалізації у стандарті використовується поняття "Атрибути доступу", що позначає сукупність атрибутів безпеки, які асоціюються з користувачем, процесом або об'єктом. Як атрибут доступу користувача, процесу або об'єкта можуть виступати відповідний унікальний ідентифікатор, мітка безпеки або цілісності, криптографічний ключ, таблиця прав доступу або інші атрибути відповідно до реалізованої в комп'ютерній системі ПБ.

Функціональні можливості використовуваних засобів захисту характеризуються окремими показниками забезпечуваного рівня безпеки стосовно однієї з чотирьох загроз. Рівень адекватності реалізації (гарантій) ПБ має один узагальнений параметр (Г-1…Г-7).

Стисло розглянемо ранжування вимог "Критеріїв ДСТС ЗІ СБУ" (Держспецзв‘язку).

На рис. 3 показані окремі показники критеріїв конфіденційності.


| Рівень | Найменування | Пов'яз. рів. |
|---|---|---|
| КД-1 | Мінімальна довірча конфіденційність | НИ-1 |
| КД-2 | Базова довірча конфіденційність | |
| КД-3 | Повна довірча конфіденційність | КО-1, НИ-1 |
| КД-4 | Абсолютна довірча конфіденційність | |
| КА-1 | Мінімальна адміністративна конфіденційність | НО-1,НИ-1 |
| КА-2 | Базова адміністративна конфіденційність | |
| КА-3 | Повна адміністративна конфіденційність | КО-1, НО-1, НИ-1 |
| КА-4 | Абсолютна адміністративна конфіденційність | |
| КК-1 | Виявлення прихованих каналів | КО-1, Г-3 |
| КК-2 | Контроль прихованих каналів | КО-1, НР-1,Г-3 |
| КК-3 | Перекриття прихованих каналів | КО-1, Г-3 |
| КВ-1 | Мінімальна конфіденційність при обміні | - |
| КВ-2 | Базова конфіденційність при обміні | НО-1 |
| КВ-3 | Повна конфіденційність при обміні | НО-1, НВ-1 |
| КВ-4 | Абсолютна конфіденційність при обміні | НО-1, НВ-1, НР-1, Г-3 |
| КО-1 | Повторне використання об'єктів | - |

Рис. 3. Показники критеріїв конфіденційності

Особливістю функціональних критеріїв є те, що деякі їх рівні залежать від інших, і для того, щоб задовольнити вимоги цих рівнів, необхідно дотримуватись не тільки наведених у них вимог, але й вимог, пов'язаних розділів інших функціональних критеріїв і критеріїв гарантій у рамках зазначених рівнів.

**Критерії конфіденційності** регламентують захист ресурсів КС від несанкціонованого доступу шляхом реалізації відповідних послуг. Стисло охарактеризуємо ці послуги.

*Довірча конфіденційність (КД-1...КД-4)* дозволяє авторизованим користувачам керувати потоками інформації від об'єктів, що належать їх доменам, до інших користувачів системи. Ранжування вимог проводиться на підставі можливостей механізму контролю, ступеня його деталізації та вибірковості керування.

*Адміністративна конфіденційність (НО-1...НО-4)* дозволяє адміністраторам або спеціально авторизованим користувачам керувати потоками інформації від об'єктів до користувачів системи. Ранжування вимог проводиться на підставі можливостей механізму контролю, ступеня його деталізації та вибірковості керування.

*Повторне використання об'єктів (КО-1)* дозволяє зробити безпечним використання розділюваних об'єктів, одночасно або послідовно доступних декільком процесам. Контроль повинен запобігати збереженню в розділюваних об'єктах залишкової інформації після завершення їх використання одним процесом і перед наданням доступу до них іншому процесу.

*Аналіз прихованих каналів (КК-1...КК-3)* дозволяє виявити й виключити присутність у системі потоків інформації, які не можуть контролюватися іншими засобами захисту. Ранжування вимог проводиться залежно від ступеня аналізу наявності прихованих каналів і можливостей щодо їх контролю й перекриття.

*Конфіденційність при обміні (КВ-1...КВ-4)* дозволяє забезпечити захист від несанкціонованого ознайомлення з об'єктами при їх переміщенні через незахищене середовище. Ранжування вимог проводиться залежно від ступеня захисту й вибірковості керування.

**Критерії цілісності** визначають можливості комп'ютерної системи щодо забезпечення власної цілісності та цілісності оброблюваної інформації, що в ній зберігається. Критерії цілісності передбачають наступні послуги: довірча та адміністративна цілісність, відкат, цілісність при обміні.

На рис. 4 показані окремі показники критеріїв цілісності.

**Критерії цілісності**

| Рівень | Найменування | Пов'яз. рів. |
|---|---|---|
| ЦД-1 | Мінімальна довірча цілісність | НИ-1 |
| ЦД-2 | Базова довірча цілісність | |
| ЦД-3 | Повна довірча цілісність | КО-1, НИ-1 |
| ЦД-4 | Абсолютна довірча цілісність | |
| ЦА-1 | Мінімальна адміністративна цілісність | НО-1,НИ-1 |
| ЦА-2 | Базова адміністративна цілісність | |
| ЦА-3 | Повна адміністративна цілісність | КО-1, НО-1, НИ-1 |
| ЦА-4 | Абсолютна адміністративна цілісність | |
| ЦВ-1 | Мінімальна цілісність при обміні | - |
| ЦВ-2 | Базова цілісність при обміні | НО-1 |
| ЦВ-3 | Повна цілісність при обміні | НО-1, НВ-1 |
| ЦО-1 | Обмежений відкат | НИ-1 |
| ЦО-2 | Повний відкат | |

Розділ: Довірча цілісність; Адміністративна цілісність; Цілісність при обміні; Відкат

Рис. 4. Показники критеріїв цілісності

*Довірча цілісність (ЦД-1...ЦД-4)* дозволяє користувачу керувати потоками інформації від інших користувачів до об'єктів, що належать його домену. Ранжування вимог проводиться на підставі можливостей механізму контролю, ступеня його деталізації та вибірковості керування.

*Адміністративна конфіденційність (ЦА-1...ЦА-4)* дозволяє адміністраторам або спеціально авторизованим користувачам керувати потоками інформації від користувачів системи до об'єктів. Ранжування вимог проводиться на підставі можливостей механізму контролю, ступеня його деталізації та вибірковості керування.

*Відкат (ЦО-1...ЦО-2)* забезпечує можливість відміни послідовності здійснених дій і повернення об'єктів комп'ютерної системи до початкового стану. Ранжування критеріїв цього розділу проводиться залежно від множини операцій, які можуть бути відмінені.

*Цілісність при обміні (ЦВ-1...ЦВ-3)* дозволяє забезпечити захист від несанкціонованої модифікації об'єктів під час їх переміщення через незахищене середовище. Ранжування вимог проводиться залежно від ступеня захисту і вибірковості керування.

**Критерії доступності** регламентують роботу засобів, що забезпечують доступність комп'ютерної системи в цілому, окремих її функцій або ресурсів протягом певного інтервалу часу для авторизованих користувачів, а також гарантувати функціонування КС у разі відмови її окремих компонентів. Як заходи забезпечення доступності розглядаються контроль щодо використання ресурсів системи, забезпечення стійкості системи до відмов, забезпечення живучості й відновлення системи в умовах виходу з ладу її компонентів. На рис. 5 показані окремі показники критеріїв доступності.

**Критерії доступності**

| Рівень | Найменування | Пов'яз. рів. | |
|---|---|---|---|
| ДР-1 | Квоти | НО-1 | Розділ використання ресурсів |
| ДР-2 | Припинення захоплення ресурсів | | |
| ДР-3 | Пріоритетність використання ресурсів | | |
| ДС-1 | Стійкість при обмежених відмовах | НО-1 | Стійкість до відмов |
| ДС-2 | Стійкість з погіршенням характеристик обслуговування | | |
| ДС-3 | Стійкість без погіршення характеристик обслуговування | | |
| ДЗ-1 | Модернізація | НО-1 | Гаряча заміна |
| ДЗ-2 | Обмежена гаряча заміна | НО-1, ДС-1 | |
| ДЗ-3 | Гаряча заміна будь-якого компоненту | | |
| ДВ-1 | Ручне відновлення | НО-1 | Відновлення після збоїв |
| ДВ-2 | Автоматизоване відновлення | | |
| ДВ-3 | Вибіркове відновлення | | |

Рис. 5. Показники критеріїв доступності

*Використання ресурсів (ДР-1...ДР-3)* дозволяє користувачам керувати використанням КС. Вимоги ранжирують залежно від контрольованих ресурсів і можливостей керувати ними.

*Стійкість до відмов (ДС-1...ДС-3)* дозволяє забезпечувати працездатність системи і доступність її ресурсів у разі виходу з ладу окремих компонентів. Вимоги ранжирують залежно від кількості несправностей, за наявності яких зберігається працездатність системи, і від множини ресурсів, доступних в умовах виходу з ладу компонентів системи.

*Гаряча заміна (ДЗ-1...ДЗ-3)* характеризує можливості зберігати працездатність і доступність ресурсів системи у процесі заміни її компонентів, що відмовили. Вимоги ранжирують залежно від повноти реалізації.

*Відновлення після збоїв (ДВ-1...ДВ-3)* дозволяє повернути КС в безпечний стан після відмов або збоїв. Вимоги ранжирують залежно від ступеня автоматизації процесу відновлення.

**Критерії спостереженості** регламентують роботу засобів, що дозволяють встановити відповідальність користувачів за події в системі.

Спостереженість забезпечується наступними засобами (послугами): реєстрація (аудит); ідентифікація й автентифікація; достовірний канал; розмежування обов'язків; цілісність КЗЗ; самотестування; ідентифікація і автентифікація при обміні; автентифікація відправника; автентифікація одержувача.

На рис. 6 відображені окремі показники критеріїв спостереженості.

*Реєстрація (НР-1...НР-5)* дозволяє виявити потенційно небезпечні дії користувачів. Вимоги ранжирують залежно від ступеня їх деталізації, складності процесу аналізу подій і можливості виявляти потенційні загрози безпеки.

*Ідентифікація та автентифікація (НИ-1...НИ-3)* дозволяє КЗЗ перевірити достовірність користувачів, що намагаються отримати доступ до системи та її ресурсів. Ранжування вимог здійснюється залежно від функціональності можливостей її механізмів ідентифікації й автентифікації.

*Достовірний канал (НК-1...НК-3)* забезпечує можливість безпосередньої конфіденційної взаємодії між користувачем і КЗЗ. Вимоги ранжируються залежно від гнучкості механізмів, що забезпечують пряму взаємодію з КЗЗ, і можливостями користувача ініціювати взаємодію з КЗЗ.

*Розмежування обов'язків (НО-1...НО-3)* дозволяє зменшити потенційний збиток від дій користувачів (з наміром і без) і обмежити авторитарність керування. Вимоги ранжирують залежно від вибірковості керування можливостями користувачів і адміністраторів.

*Цілісність комплексу засобів захисту (НЦ-1...НЦ-3)* дозволяє визначати міру здатності КЗЗ захищати себе і гарантувати свою здатність керувати захищеними об'єктами. Вимоги ранжирують залежно від повноти вимог до політики цілісності КЗЗ, функціональності КЗЗ і ступеня контролю на доступ.

*Самотестування (НТ-1...НТ-3)* дозволяє перевірити КЗЗ і гарантувати коректність функціонування і цілісність певної сукупності функцій КС. Вимоги

ранжуються залежно від можливості виконання тестів у процесі запуску або штатного функціонування.

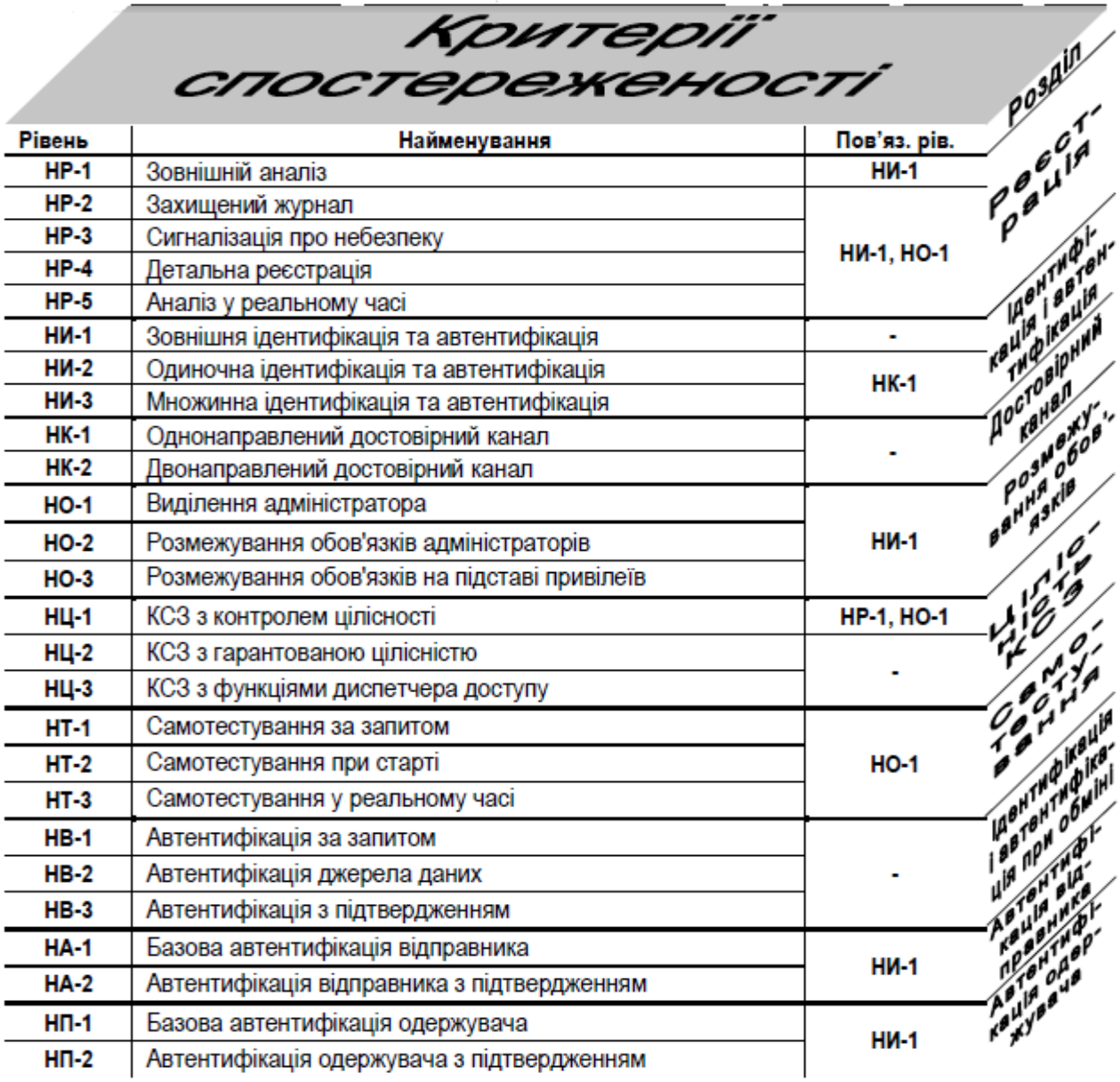


Рис. 6. Показники критеріїв спостереженості

*Ідентифікація і автентифікація при обміні (НВ-1...НВ-3)* дозволяє забезпечити взаємну достовірність між двома КЗЗ перед їх взаємодією. Вимоги ранжируються залежно від повноти реалізації.

*Автентифікація відправника (НА-1,НА-2)* дозволяє забезпечити неможливість відмови певного користувача від факту отримання об'єкта. Вимоги ранжируються залежно від можливості підтвердження результатів перевірки незалежною третьою стороною.

*Автентифікація одержувача (НП-1,НП-2)* дозволяє забезпечити неможливість відмови користувача від авторства створення й відправки об'єкта.

Вимоги ранжируються залежно від можливості підтвердження результатів перевірки незалежною третьою стороною.

**Критерії гарантій** регламентують вимоги до процесу розробки та реалізації КЗЗ, що дозволяють визначити адекватність реалізації ПБ і відображають ступінь довіри до комплексу засобів захисту. Критерії гарантій охоплюють усі стадії та аспекти створення й експлуатації системи і включають розділи, що належать до:

1) архітектури КЗЗ;

2) середовища розробки:

процесу розробки;

керування конфігурацією;

3) послідовності розробки:

розробки функціональних специфікацій:

ПБ;

моделі ПБ;

проекту архітектури;

детального проекту;

його реалізації;

4) середовища функціонування;

5) документації:

керівництва з безпеки для користувача;

керівництва адміністратора безпеки;

6) випробування комплексу засобів захисту.

Вимоги до *архітектури* забезпечують гарантії спроможності КЗЗ реалізовувати ПБ.

Вимоги до *середовища розробки* забезпечують гарантії повної керованості розробником процесами розробки й супроводу оцінюваної КС.

Вимоги до *послідовності розробки* (процесу проектування) забезпечують гарантії існування точного опису КС на кожній стадії проектування й точної відповідності реалізації КС з початковими вимогами до ПБ.

Вимоги до *середовища функціонування* забезпечують гарантії відсутності несанкціонованих модифікацій КС під час постачання замовнику, а також інсталяції та ініціалізації замовником КС так, як це передбачається розробником.

Вимоги до *документації* визначають обов'язкову наявність у вигляді окремих документів або розділів інших документів, опис послуг безпеки (функціональності), що реалізовуються КЗЗ, керівництво адміністратора щодо послуг безпеки, керівництво користувача щодо послуг безпеки.

Вимоги до *випробовування КЗЗ* регламентують порядок аргументування, доказу й перевірки стійкості КЗЗ до атак. Передбачено сім рівнів гарантій (Г1...Г7). Із зростанням номера рівня відбувається конкретизація, доповнення й посилення вимог без зміни їх структури. Рівень гарантій (адекватності) реалізації ПБ характеризує якість усієї системи в цілому.

Порядок оцінки КС на предмет відповідності даним критеріям визначається відповідними нормативними документами Держспецзв‘язку

(ДСТС ЗІ СБУ). Експертна комісія, яка проводить оцінку КС, визначає кількість і рівень реалізованих у КС послуг безпеки і ступінь дотримання вимог гарантій.

Результатом оцінки є рейтинг (функціональний профіль захищеності), який складається з ряду (переліку) літерно-числових комбінацій, що позначають рівні реалізованих послуг, у поєднанні з рівнем гарантій.

Нормативні документи Держспецзв‘язку (ДСТС ЗІ СБУ) вводять *функціональні профілі захищеності*, що є переліком мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи КС, щоб задовольняти певні вимоги до захищеності оброблюваної інформації.

*Стандартні функціональні профілі* формуються на основі існуючих вимог до захисту певної інформації від певних загроз і відомих на сьогодні функціональних послуг, що дозволяють протистояти загрозам і забезпечити виконання цих вимог.

Опис профілю складається з трьох частин:

1) літерно-числового ідентифікатора;

2) знака рівності;

3) переліку рівнів послуг у фігурних дужках.

Ідентифікатор у свою чергу включає:

позначення класу КС (1, 2 або 3);

літерну частину, що характеризує види загроз, від яких забезпечується захист (К, і/або Ц, і/або Д);

номер профілю;

необов'язкове літерне позначення версії.

Усі частини ідентифікатора відокремлюються одна від одної крапкою. Наприклад, 2.К.4 — функціональний профіль номер чотири, що відображає вимоги до КС класу 2, основна вимога щодо захисту оброблюваної інформації – забезпечення конфіденційності.

Відповідно, нормативні документи Держспецзв‘язку (ДСТС ЗІ СБУ) визначають вимоги до профілів захищеності КЗЗ, що входять до складу КС різних класів і призначень (наприклад, КС, які призначені для автоматизації банківської діяльності або органів державної влади).

## ТЕМА 6:

## «Політика інформаційної безпеки організації»

## ПЛАН

6.1. Основи формування політики інформаційної безпеки організації
6.2. Визначення політики інформаційної безпеки
6.3. Принципи політики інформаційної безпеки
6.4. Види політики інформаційної безпеки

### Література:


1. Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников. – М.: Финансы и статистика, 1997. – 198 с.
2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. / В.А. Герасименко. – В 2-х т. – М.: Энергоатомиздат, 1994. – 236 с.
3. Хоффман Л.Дж. Современные методы защиты информации / Хоффман Л.Дж. – Пер. с англ. – М.: Советское радио, 1980. – 390 с.
4. Інформаційна безпека. Організаційні заходи по забезпеченню безпеки. Розподіл відповідальності. [Електронний ресурс]. – Джерело доступу: usufit.org.ua/teaching/MSZBP/DownloadHandler.ashx?pg
5. Домарєв В. Основні поняття та визначення політики інформаційної безпеки. [Електронний ресурс]. – Джерело доступу: http://domarev.com.ua/obuch/lek_14_n6.htm
6. Менеджмент в сфере информационной безопасности [Електронний ресурс]. – Джерело доступу: http://www.intuit.ru/department/itmngt/manofis/1/
7. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учебное пособие. 2-е изд. – М.: Издательско-торговая корпорация «Дашков и К°». 2005. – 336 с.
8. Ярочкин В.И. Информационная безопасность. – М.: Академический Проект. Мир. 2004. – 544 с.
9. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб. БХВ-Петербург, 2003. – 752 с.
10. Голубченко О.Л. Політика інформаційної безпеки. Луганськ: вид-во СНК ім. В.Даля, 2009. – 300 с.
11. Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий. – М.: Радио и связь. 2003. – 342с.
12. Гмурман А.И. Информационная безопасность – М.: «БИТ-М», 2004. – 387с.

## 6.1. Основи формування політики інформаційної безпеки організації

Організація внутрішньооб'єктного режиму та охорони приміщень і територій є частиною загальної роботи підприємства щодо забезпечення збереження майна та безперервності поточної діяльності. Основним завданням забезпечення внутрішньооб'єктного режиму є недопущення сторонніх осіб до інформаційних активів і запобігання загроз інформаційної безпеки.

Основою внутрішньооб'єктного режиму є пропускний режим, у рамках якого, як правило, встановлюються:

• документи, що дають право проходу на територію підприємства - як пропуску і карти доступу, видані самим підприємством, так і документи, видані сторонніми організаціями (наприклад, службові посвідчення посадових осіб деяких органів державної влади);

• категорії перепусток, що використовуються на підприємстві, відповідно до яких (категоріями) обмежується термін дії перепусток, час можливого проходу на територію підприємства (дні тижня, години доби) і деякі інші параметри;

• порядок видачі, обміну, продовження та вилучення перепусток, а також порядок дій співробітників та посадових осіб при втраті пропуску;

• порядок організації пропуску осіб, автотранспорту та проносу (провозу) майна: розміщення та порядок роботи контрольно-пропускних пунктів, можливість пропуску тих чи інших осіб, засобів автотранспорту та вантажів через ті чи інші КПП та ін;

• основні положення документообігу, використовуваного при проході відвідувачів на територію підприємства – вимоги до ведення Журналу реєстрації проходу відвідувачів, вимоги до документів, на основі яких видаються разові перепустки, порядок видачі разових перепусток тощо;

• порядок огляду транспортних засобів, що допускаються на територію підприємства.

Крім того, в рамках організації внутрішньооб'єктного режиму може бути передбачено розділення приміщень і територій на окремі зони з обмеженням доступу (у тому числі на основі поділу приміщень і територій на різні категорії), а також розмежування доступу окремих співробітників (категорій персоналу) і відвідувачів у різні зони; також можуть бути визначені основні вимоги до технічних засобів розмежування доступу та організації їх використання.

З технічної точки зору заходів щодо забезпечення пропускного та внутрішнього режимів можуть бути реалізовані тими ж засобами, які використовуються для забезпечення безпеки в інших сферах, крім інформаційної (захист майна і персоналу, забезпечення безперервності виробничого процесу), – засобами контролю доступу, відеоспостереження, сигналізації та фізичного захисту.

В основі засобів контролю доступу лежать механізми впізнання особистості та порівняння з встановленими параметрами. Політика підприємства може встановлювати як спрощені підходи до розпізнавання, коли

охоронці підприємства перевіряють документи (підтвердження особистості, підтвердження можливості проходу на територію в даний час через даний КПП), так і використання автоматизованих засобів, коли впізнання відвідувача і підтвердження (або заборона) можливості проходу на територію (виходу з території, з будівлі) проводиться автоматизованою системою контролю доступу на основі наявних у відвідувача машинозчитувальних засобів персональної ідентифікації (пластикових карт, жетонів тощо) або на основі зчитування та аналізу його фізичних особливостей (геометрії обличчя, відбитків пальців, малюнка райдужної оболонки ока, голосу і т.п.). При виборі конкретних засобів біометричної ідентифікації фахівцям і керівникам підприємства слід пам'ятати, що різні технології мають різну ступінь надійності, а також можуть бути більш-менш зручними в повсякденному використанні великою кількістю людей. Так, наприклад, вважається, що одна з передових технологій біометричної ідентифікації – ідентифікація по кровоносних судинах пальця (коли інфрачервоний промінь просвічує палець і створює тривимірне зображення унікальною для кожної людини структури кровоносних судин) – істотно менш уразлива для обману, ніж дактилоскопічна ідентифікація.

Фізичний захист об'єктів, як правило, передбачає посилення конструкцій огорож, елементів будівель, споруд та окремих приміщень. До таких засобів відносяться захист віконних прорізів металевими гратами і віконницями, спеціальне скління вікон, використання броньованих дверей, замикаючих пристроїв, сейфів для зберігання засобів обчислювальної техніки і носіїв інформації. Відповідно до особливостей використовуваних приміщень і територій політика безпеки підприємства також може передбачати розташування місць зберігання і обробки інформації (наприклад, архівів або серверних кімнат) у приміщеннях, найменш доступних для проникнення, найбільш віддалених від місць зберігання вибухонебезпечних і легкозаймистих речовин, найменш схильних до затоплення (для об'єктів розташованих в долинах річок і на узбережжі), найбільш захищених від ударів блискавки тощо

З фізичним захистом безпосередньо пов'язано використання засобів сигналізації та відеоспостереження. Залежно від характеру об'єкта, що охороняється (територія, будівля, прохід, приміщення, окрема шафа або сейф) у засобах сигналізації можуть застосовуватися датчики, що працюють на різних фізичних принципах (фотоелектричні датчики, датчики об'єму, акустичні датчики тощо), що мають різні налаштування і використовують різні канали зв'язку. На відміну від засобів сигналізації засоби відеоспостереження дозволяють не тільки встановити факт порушення, але і в деталях відслідковувати його, контролювати ситуацію, а також вести відеозапис, який можна буде використовувати для прийняття подальших заходів (пошук порушників, кримінальне переслідування і т.п.).

Окремим завданням є забезпечення інформаційної безпеки у процесі транспортування носіїв інформації та інших об'єктів, що вимагає використання як спеціальних організаційних прийомів, так і спеціальних технічних засобів. До організаційних методів відноситься залучення спеціально підготовлених кур'єрів, а також поділ носіїв інформації (об'єктів) на частини і їх роздільне

транспортування з метою мінімізації можливостей витоку інформації. До технічних засобів, що застосовуються при транспортуванні об'єктів, відносяться захищені контейнери, спеціальні пакувальні матеріали, а також тонкоплівкові матеріали та голографічні мітки, що дозволяють ідентифікувати достовірність об'єктів і контролювати несанкціонований доступ до них.

Організація режиму секретності в установах і на підприємствах грунтується на вимогах законодавства, що стосується питань державної таємниці, та відповідних підзаконних актів. Відповідно до діючих норм до державної таємниці може бути віднесена інформація, що стосується обороноздатності країни, її економіки, міжнародних відносин, державної безпеки та охорони правопорядку (у тому числі відомості про методи та засоби захисту секретної інформації, а також про державні програми та заходи в області захисту державної таємниці); в законодавстві також спеціально уточнюються галузі діяльності, інформація про яких не може бути віднесена до державної таємниці. Віднесення конкретної інформації до державної таємниці здійснюється рішенням спеціально призначуваних посадових осіб, а загальний Перелік відомостей, віднесених до державної таємниці, затверджується Президентом і підлягає обов'язковому опублікуванню. Для відомостей, що становлять державну таємницю, встановлюються три ступені секретності: "особливої важливості", "цілком таємно" та "таємно ", а носії таких відомостей (документи) повинні мати відповідні реквізити.

Основним елементом організації режиму секретності є допуск посадових осіб та громадян до відомостей, що становлять державну таємницю. Він передбачає виконання керівництвом підприємства і підрозділів із захисту державної таємниці (у взаємодії з уповноваженими правоохоронними органами) наступних основних заходів:

• ознайомлення посадових осіб і громадян до норм законодавства, які передбачають відповідальність за порушення вимог.

• отримання згоди на тимчасові обмеження їх прав відповідно до законодавства.

• отримання згоди на проведення щодо їх перевірочних заходів.

• прийняття рішення про допуск до відомостей, що становлять державну таємницю.

• висновок з особами, які отримали допуск, трудового договору ( контракту), що відображає взаємні зобов'язання таких осіб та адміністрації підприємства (в т.ч. зобов'язання таких осіб перед державою з нерозповсюдження довірених їм відомостей, що становлять державну таємницю).

Крім віднесення відомостей до державної таємниці та допуску посадових осіб та громадян до засекречених відомостей, важливим елементом системи забезпечення режиму секретності є організація інформаційного обміну між підприємствами при спільному виконанні робіт. Зокрема, передача засекречених відомостей від одного підприємства до іншого повинна проводитися з дозволу уповноваженого державного органу, договір на виконання робіт повинен передбачати зобов'язання сторін щодо забезпечення

збереження відомостей, а замовник робіт повинен контролювати виконання нормативних вимог контрагентами за такими договорами (наявність ліцензій, оформлення допуску співробітників) і вживати необхідних заходів у разі виявлення порушень.

Також важливим елементом забезпечення режиму секретності є організація передачі відомостей, що становлять державну таємницю, іншим державам (у тому числі ознайомлення з такими відомостями і надання можливості доступу до них). У кожному окремому випадку рішення про передачу відомостей виноситься Урядом на підставі експертного висновку Міжвідомчої комісії із захисту державної таємниці, яка, у свою чергу, керується мотивованим клопотанням підприємства, зацікавленого в передачі секретних відомостей, та рішенням органу державної влади, який курує коло питань, до якого відносяться відомості, що передаються. Для забезпечення захисту інтересів держави зі стороною, що приймає секретні відомості, укладається договір, що містить необхідні зобов'язання по захисту одержуваної інформації, а також порядок вирішення конфліктних ситуацій та компенсації можливого збитку.

Політика опублікування матеріалів у відкритих джерелах (таких як газети, журнали, виставки, мережа Інтернет, радіо – і телепередачі, конференції, музейні експозиції тощо) повинна забезпечувати запобігання випадкових і організованих витоків конфіденційної інформації при взаємодії підприємства із засобами масової інформації, громадськими та державними органами, науковими, академічними і бізнес-спільнотою. Для того щоб уникнути шкоди інтересам підприємства, така політика повинна містити основні правила і процедури підготовки інформаційних матеріалів до відкритої публікації.

Зокрема, в політиці безпеки слід передбачати створення спеціального експертної ради, відповідальної за розгляд всіх інформаційних матеріалів, які передбачається опублікувати у відкритих джерелах (політика безпеки повинна містити конкретні обмеження на опублікування інформаційних матеріалів без їх розгляду експертною радою). Основним завданням такої ради є підготовка висновків про можливість або неможливість опублікування певних інформаційних матеріалів, а також підготовка конкретних пропозицій щодо вилучення певних відомостей з матеріалів, підготовлених до опублікування. За відсутності єдиної думки у членів експертної комісії рішення про можливість опублікування може бути прийнято керівником підприємства з урахуванням рекомендацій експертів. Для ефективного вирішення завдань члени експертної ради мають детально знати всі існуючі обмеження (зокрема, встановлені законодавством) і володіти ситуацією в тій сфері, в якій функціонує підприємство. При цьому, як правило, сам автор підготовлюваних до опублікування матеріалів не може входити до експертної ради, а редактор або керівник, який відповідає за підготовку матеріалів, не може бути головою експертної ради.

Політика управління паролями (або, в більш загальному вигляді, політика ідентифікації і аутентифікації) може визначати періодичність заміни паролів, дії, які необхідно здійснити при компрометації паролів, основні вимоги до їх якості, процедур їх генерації, розподілу основних обов'язків, пов'язаних з

генерацією паролів, їх зміною і доведенням до користувачів, а також основні заходи відповідальності за порушення встановлених правил і вимог. Політика на цьому рівні також може встановлювати заборону зберігання записаних паролів, заборону повідомляти будь-кому свій пароль (в тому числі керівникам та адміністраторам інформаційних систем) та інші аналогічні обмеження.

Політика встановлення та оновлення версій програмного забезпечення може включати в себе деякі обмеження на самостійне придбання і установку програмного забезпечення окремими підрозділами та користувачами, а також певні вимоги до кваліфікації спеціалістів, які здійснюють їх установку, настройку та підтримку.

Політика придбання інформаційних систем та їх елементів (програмних і апаратних засобів) може включати в себе вимоги до ліцензування та сертифікації використовуваного програмного забезпечення і устаткування, а також певні вимоги до фірм, які здійснюють їх постачання та впровадження.

Політика доступу сторонніх користувачів (організацій) в інформаційні системи підприємства може містити перелік основних ситуацій, коли такий доступ можливий, а також основні критерії та процедури, відповідно до яких здійснюється доступ. Також політика може передбачати розподіл відповідальності співробітників самого підприємства за дії зовнішніх користувачів, які отримують такий доступ.

Політика щодо розробки ПЗ може містити вимоги як до питань безпеки і надійності програмних засобів, самостійно розроблюваних підприємством, так і щодо передачі розробки програмних засобів (модулів інформаційних систем, окремих програмних бібліотек тощо) стороннім спеціалізованим організаціям (аутсорсинг), а також щодо придбання та використання тиражованих програмних бібліотек (модулів), поширюваних компаніями-виробниками. Зокрема, політика може містити вимоги до тестування самостійно розроблюваного ПО, аналізу його вихідних кодів, описувати основні критерії надійності.

Політики використання окремих універсальних інформаційних технологій в масштабі всього підприємства можуть включати в себе:

• політику використання електронної пошти (e - mail);

• політику використання засобів шифрування даних;

• політику захисту від комп'ютерних вірусів і інших шкідливих програм;

• політику використання модемів та інших аналогічних комунікаційних засобів;

• політику використання Інфраструктури публічних ключів;

• політику використання технології Віртуальних приватних мереж ( Virtual Private Network - VPN).

Політика використання електронної пошти може включати в себе як загальні обмеження на її використання певними категоріями співробітників, так і вимоги до управління доступом і збереження конфіденційності повідомлень, а також до адміністрування поштової системи та зберігання електронних повідомлень. Крім того, політика може передбачати:

• заборона на використання електронної пошти в особистих цілях;

• спеціальні вимоги до відправлення та одержання приєднаних файлів, які потенційно можуть містити шкідливі програми;

• заборона на використання електронної пошти тимчасовими співробітниками;

• вимоги шифрування переданих повідомлень;

• спостереження за всіма переданими і одержуваними повідомленнями;

• обмеження на передачу конфіденційної інформації за допомогою електронної пошти та інші положення.

Політика використання комунікаційних засобів може визначати межі використання технологій, що дозволяють підключити комп'ютери та інформаційні системи підприємства до інформаційних систем і комунікаційних каналів за його межами. Зокрема, така політика може вводити певні обмеження на використання модемів для телефонних ліній, пристроїв, що використовують сучасні бездротові технології, такі, як GSM (GPRS ), Wi -Fi, передача даних у мережах стандарту CDMA і т.п.

## 6.2. Визначення політики інформаційної безпеки

При прийнятті рішень адміністратори ІС зіштовхуються з проблемою вибору варіантів рішень з організації ЗІ на основі обліку принципів діяльності організації, співвідношення важливості цілей і наявності ресурсів. Ці рішення включають визначення того, як будуть захищатися технічні й інформаційні ресурси, а також як повинні поводитися службовці в тих чи інших ситуаціях.

*Політика інформаційної безпеки* – набір законів, правил і практичних рекомендацій і практичного досвіду, що визначають управлінські і проектні рішення в області ЗІ. На основі ПІБ будується керування, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поводження ІС у різних ситуаціях.

Відповідно до запропонованого підходу політика (ЗАХОДИ) інформаційної безпеки (003) реалізується відповідною СТРУКТУРОЮ органів (002) на основі нормативно-методичної БАЗИ (001) з використанням програмно-технічних методів і ЗАСОБІВ (004), що визначають архітектуру системи захисту.

Для конкретної ІС політика безпеки повинна бути індивідуальної. Вона залежить від технології обробки інформації, використовуваних програмних і технічних засобів, структури організації т.д.

## 6.3. Принципи політики інформаційної безпеки

Політика безпеки визначається як сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів.

При розробці і проведенні її в життя доцільно керуватися наступними засадами:

неможливість минати захисні засоби;

посилення найслабшої ланки;
неприпустимість переходу у відкритий стан;
мінімізація привілеїв;
поділ обов'язків;
багаторівневий захист;
розмаїтість захисних засобів;
простота і керованість інформаційної системи;
забезпечення загальної підтримки заходів безпеки.

Пояснимо зміст перерахованих принципів.

Щодо міжмережевих екранів принцип неможливості минати захисні засоби означає, що всі інформаційні потоки в мережу, що захищається, і з неї повинні проходити через екран. Не повинно бути "таємних" модемних чи входів тестових ліній, що йдуть в обхід екрана.

Надійність будь-якої оборони визначається найслабшою ланкою. Часто найслабшою ланкою виявляється не чи комп'ютерна програма, а людина, і тоді проблема забезпечення інформаційної безпеки здобуває нетехнічний характер.

Принцип неприпустимості переходу у відкритий стан означає, що при будь-яких обставинах (у тому числі позаштатних), СЗІ або цілком виконує свої функції, або повинна цілком блокувати доступ.

Принцип мінімізації привілеїв наказує виділяти користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання службових обов'язків.

Принцип поділу обов'язків припускає такий розподіл ролей і відповідальності, при якому одна людина не може порушити критично важливий для організації процес. Це особливо важливо, щоб запобігти зловмисні чи некваліфіковані дії системного адміністратора.

Принцип багаторівневого захисту наказує не покладатися на один захисний рубіж, яким би надійним він ні здавався. За засобами фізичного захисту повинні випливати програмно-технічні засоби, за ідентифікацією й аутентифікацією - керування доступом і, як останній рубіж, - протоколювання й аудит. Ешелонована оборона здатна принаймні затримати зловмисника, а наявність такого рубежу, як протоколювання й аудит, істотно утрудняє непомітне виконання злочинних дій.

Принцип розмаїтості захисних засобів рекомендує організовувати різні за своїм характером оборонні рубежі, щоб від потенційного зловмисника було потрібно оволодіння різноманітними і, по можливості, несумісними між собою навичками подолання СЗІ.

Принцип простоти і керованості інформаційної системи в цілому і СЗІ особливо визначає можливість формального чи неформально доказу коректності реалізації механізмів захисту. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.

Принцип загальної підтримки заходів безпеки - носить нетехнічний характер. Рекомендується із самого початку передбачити комплекс заходів,

спрямований на забезпечення лояльності персоналу, на постійне навчання, теоретичне і, головне, практичне.

### 6.4. Види політики інформаційної безпеки

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

Для вивчення властивостей способу керування доступом створюється його формальний опис — математична модель. При цьому модель повинна відображати стан всієї системи, її переходи з одного стану в інший, а також враховувати, які стани і переходи можна вважати безпечними в змісті даного керування. Без цього говорити про які-небудь властивості системи, і тим більше гарантувати їх, щонайменше некоректно.

В даний час найкраще вивчені два види політики безпеки: виборча і повноважна, засновані, відповідно на виборчому і повноважному способах керування доступом.

Крім того, існує набір вимог, що підсилює дію цих політик і призначений для керування інформаційними потоками в системі.

Слід зазначити, що засоби захисту, призначені для реалізації якого-небудь з названих способів керування доступом, тільки надають можливість надійного керування чи доступу до інформаційних потоків. Визначення прав доступу суб'єктів до об'єктів і/чи інформаційним потокам (повноважень суб'єктів і атрибутів об'єктів, присвоєння міток критичності і т.д.) входить у компетенцію адміністрації системи.

***Виборча політика безпеки***

Основою виборчої політики безпеки є виборче керування доступом, що має на увазі, що:

- усі суб'єкти й об'єкти системи повинні бути ідентифіковані;
- права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей виборчого керування доступом застосовується модель системи на основі матриці доступу (МД), іноді неї називають матрицею контролю доступу. Така модель одержала назву матричної.

Матриця доступу являє собою прямокутну матрицю, у якій об'єкту системи відповідає рядок, а суб'єкту стовпець. На перетинанні стовпця і рядка матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Виділяють такі типи доступу суб'єкта до об'єкта, як “доступ на читання”, “доступ на запис”, “доступ на виконання” та ін.

Безліч об'єктів і типів доступу до них суб'єкта може змінюватися відповідно до деяких правил, що існують у даній системі. Визначення і зміна цих правил також є задачею МД.

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеним у відповідній осередку матриці доступу. Звичайно виборче керування доступом реалізує принцип “що не дозволено, те заборонено”, що

припускає явний дозвіл доступу суб'єкта до об'єкта. Матриця доступу — найбільш простий підхід до моделювання систем доступу.

Виборча політика безпеки широко застосовується в комерційному секторі, тому що її реалізація на практиці відповідає вимогам комерційних організацій по розмежуванню доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати.

***Повноважна політика безпеки***

Основу повноважної політики безпеки складає повноважне керування доступом, що має на увазі, що:

- усі суб'єкти й об'єкти системи повинні бути однозначно ідентифіковані;
- кожному об'єкту системи привласнена влучна критичності, що визначає цінність інформації, що міститься в ньому;
- кожному суб'єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

У тому випадку, коли сукупність міток має однакові значення, говорять, що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру і, таким чином, у системі можна реалізувати ієрархічно спадний потік інформації (наприклад, від рядових виконавців до керівництва). Чим важливішим є об'єкт за суб'єкт, тим вищою його мітка критичності. Тому найбільш захищеними виявляються об'єкти з найбільш високими значеннями мітки критичності.

Кожен суб'єкт, крім рівня прозорості, має поточне значення рівня безпеки, що може змінюватися від деякого мінімального значення до значення його рівня прозорості.

Основне призначення повноважної політики безпеки — регулювання доступу суб'єктів системи до об'єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії на нижні, а також блокування можливого проникнення з нижніх рівнів на верхні. При цьому вона функціонує на тлі виборчої політики, додаючи її вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки).

Споконвічно повноважна політика безпеки була розроблена в інтересах МО США для обробки інформації з різними грифами таємності. Її застосування в комерційному секторі стримується наступними основними причинами:

- відсутністю в комерційних організаціях чіткої класифікації збереженої й оброблюваної інформації, аналогічної державної класифікації (грифи таємності зведень);
- високою вартістю реалізації і великих накладних витрат.

*Організаційно-технічні заходи*

Приведемо перелік основних організаційно-технічні заходи щодо ЗІ:

- розробка і твердження функціональних обов'язків посадових осіб служби інформаційної безпеки;
- внесення необхідних змін і доповнень в усі організаційно-розпорядницькі документи (положення про підрозділи, обов'язок посадових осіб, інструкції користувачів системи і т.п.) з питань забезпечення безпеки програмно-інформаційних ресурсів ІС і діям у випадку виникнення кризових ситуацій;

- оформлення юридичних документів (договору, накази і розпоряджень керівництва організації) з питань регламентації відносин з користувачами (клієнтами), що працюють в автоматизованій системі, між учасниками інформаційного обміну і третьою стороною (арбітраж, третейський суд) про правила дозволу, зв'язаних із застосуванням електронного підпису;

- створення науково-технічних і методологічних основ захисту ІС;

- виключення можливості таємного проникнення в приміщення);

- перевірка і сертифікація використовуваних у ІС технічних і програмних засобів на предмет визначення заходів для їхнього захисту від витоку по каналах побічних електромагнітних випромінювань і наведень;

- визначення порядку призначення, зміни, твердження і надання конкретним посадовим особам необхідних повноважень по доступі до ресурсів системи;

- розробка правил керування доступом до ресурсів системи, визначення переліку задач, розв'язуваних структурними підрозділами організації з використанням ІС, а також використовуваних при їхньому рішенні режимів обробки і доступу до даних;

- визначення переліку файлів і баз даних, що містять зведення, що складають комерційну і службову таємницю, а також вимоги до рівнів їхньої захищеності від НСД при передачі, збереженні й обробці в ІС;

- виявлення найбільш ймовірних погроз для даної ІС, виявлення уразливих місць процесу обробки інформації і каналів доступу до неї;

- оцінка можливого збитку, викликаного порушенням безпеки інформації, розробка адекватних вимог по основних напрямках захисту;

- організація надійного пропускного режиму;

- визначення порядку обліку, видачі, використання і збереження знімних магнітних носіїв інформації, що містять еталонні і резервні копії програм і масивів інформації, архівні дані і т.п.;

- організація обліку, збереження, використання і знищення документів і носіїв із закритою інформацією;

- організація і контроль за дотриманням усіма посадовими особами вимог по забезпеченню безпеки обробки інформації;

- визначення переліку необхідних заходів для забезпечення безупинної роботи ІС у критичних ситуаціях, що виникають у результаті НСД, збоїв і відмовлень СВТ, помилок у програмах і діях персоналу, стихійних лих і т.п.

- контроль функціонування і керування використовуваними засобами захисту;

- явний і схований контроль за роботою персоналу системи;

- контроль за реалізацією обраних заходів захисту в процесі проектування, розробки, введення в лад і функціонування ІС;

- періодичний аналіз стану й оцінка ефективності заходів захисту інформації;

- розподіл реквізитів розмежування доступу (паролів, ключів шифрування і т.п.);

- аналіз системних журналів, уживання заходів по виявлених порушеннях правил роботи;

- складання правил розмежування доступу користувачів до інформації;

- періодичне, з залученням сторонніх фахівців, здійснення аналізу стану й оцінки ефективності заходів і застосовуваних засобів захисту. На основі отриманої в результаті такого аналізу інформації вживати необхідних заходів по удосконалюванню системи захисту;

- розгляд і твердження всіх змін в устаткуванні ІС, перевірка їх на задоволення вимогам захисту, документальне відображення змін і т.п.;

- перевірка прийнятих на роботу, навчання правилам роботи з інформацією, ознайомлення з заходами відповідальності за порушення правил захисту, створення умов, при яких персоналу було б невигідно порушувати свої обов'язки.

*Захист даних адміністративними методами*

До таких заходів захисту можна віднести організаційно-технічні й організаційно-правові заходи, здійснювані в процесі створення й експлуатації системи обробки і передачі даних з метою забезпечення захисту інформації.

Наскільки важливі організаційно-режимні заходи в загальному арсеналі засобів захисту, говорить уже хоча б той факт, що жодна ІС не може функціонувати без участі обслуговуючого персоналу. Крім того, організаційно-режимні заходи охоплюють усі структурні елементи системи захисту на всіх етапах їхнього життєвого циклу: будівництво приміщень, проектування системи, монтаж і налагодження устаткування, іспити і перевірка в експлуатації апаратури, оргтехніки, засобів обробки і передачі даних.

З одного боку, ці заходи повинні бути спрямовані на забезпечення правильності функціонування механізмів захисту і виконуватися адміністратором безпеки системи. З іншого боку, керівництво фірми повинне регламентувати правила обробки і захисту інформації, а також установити заходи відповідальності за порушення цих правил.

Нижче перерахований ряд дуже простих дій, що можуть значно підвищити ступінь захисту корпоративної мережі без великих фінансових уливань.

1. Більш ретельний контроль за персоналом, особливо за найбільш низькооплачуваними працівниками, наприклад прибиральниками й охоронцями.

2. Акуратна непомітна перевірка послужного списку найманого працівника, що допоможе уникнути виникнення проблем у майбутньому.

3. Ознайомлення найманого співробітника з документами, що описують політику компанії у сфері інформаційної безпеки, і одержання від нього відповідної розписки.

4. Зміна вмісту всіх екранів для входу в систему таким чином, щоб вони відображали політику компанії в сфері захисту даних.

5. Підвищення рівня фізичного захисту.

6. Блокування всіх дисководів гнучких дисків в організаціях, у яких установлена мережа, – це дозволить мінімізувати ризик комп'ютерних крадіжок і зараження вірусами.

7. Визнання за співробітниками визначених прав при роботі з комп'ютерами, наприклад організація дошок оголошень, дотримання конфіденційності електронної пошти, дозвіл використовувати визначені комп'ютерні ігри.

Співробітники компанії повинні бути союзниками, а не супротивниками адміністратора системи в боротьбі за безпеку даних.

## ТЕМА 7:

## «Організація системи інформаційної безпеки підприємства»

## ПЛАН

7.1. Постановка завдання та порядок його розв'язання
7.2. Багаторівнева модель об'єктів інформаційної безпеки
7.3. Правила побудови системи інформаційної безпеки підприємства
7.4. Принципи захисту інформації
7.5. Методи і засоби забезпечення інформаційної безпеки організації.
7.6. Методика побудови корпоративної системи захисту інформації
7.7. Формування організаційної політики безпеки
7.8. Особливості розробки концепції безпеки
7.9 Страхування інформаційних ризиків

### Література:

1. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997.
2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х т. – М.: Энергоатомиздат, 1994.
3. Хоффман Л.Дж. Современные методы защиты информации. Пер. с англ. – М.: Советское радио, 1980.
4. «Інформаційна безпека. Організаційні заходи по забезпеченню безпеки. Розподіл відповідальності». [Електронний ресурс]. – Джерело доступу: usufit.org.ua/teaching/MSZBP/DownloadHandler.ashx?pg
5. Домарєв В. Основні поняття та визначення політики інформаційної безпеки. [Електронний ресурс]. – Джерело доступу: http://domarev.com.ua/obuch/lek_14_n6.htm
6. Менеджмент в сфере информационной безопасности [Електронний ресурс]. – Джерело доступу: http://www.intuit.ru/department/itmngt/manofis/1/

### 7.1. Постановка завдання та порядок його розв'язання

Вирішення проблеми забезпечення безпеки інформації на сучасному рівні вимагає системного підходу, який передбачає систематизацію певних завдань і порядок їх вирішення. Що захищати? Де захищати? Коли захищати? Від чого захищати? І, нарешті, як захищати? Розглянемо порядок і основні складові, які необхідно враховувати при системному аналізі об'єкта захисту. Будемо розглядати підприємство як об'єкт захисту, що складається з:

- виду діяльності або класу вирішуваних завдань, що спричиняють появу інформації з обмеженим доступом і необхідність її захисту;
- носіїв інформації різної фізичної природи (персонал, технічні пристрої, тверді носії, поля, хімічні середовища тощо);

- обумовлених каналів зв'язку між носіями інформації, що забезпечують функціонування об'єкта захисту;

- протоколів зберігання, обробки та обміну інформацією між носіями;

- функціональних параметрів об'єкта захисту і його елементів, що характеризують режими зберігання, обробки і передачі інформації з обмеженим доступом та їх зміну в часі;

- фізичного простору, в якому розташовуються носії і канали зв'язку (будівлі, споруди, транспорт, територія і т.д.);

- вимог щодо забезпечення безпеки інформації.

Вивчення поведінки інформації в носіях та її руху по обумовлених каналах зв'язку дозволяє отримати модель функціонування об'єкта захисту. Така модель дає можливість відповісти на перші три питання, Що? Де? Коли? і таким чином забезпечити спостереженість об'єкта захисту як об'єкта управління безпекою. З позицій системного аналізу ця відповідь являє собою не що інше, як модель всього об'єкта захисту, адекватність, повнота і точність якої буде, швидше за все, визначатися розумною достатністю. Очевидно, що тільки тепер можна найбільш повно відповісти на запитання «Від чого захищати?», Тобто визначити діючі і передбачувані загрози, виявити найбільш ймовірні канали витоку інформації.

Проведення аудиту системи інформаційної безпеки підприємства дає можливість провести найбільш обґрунтований вибір організаційних і технічних засобів захисту, як на етапі створення об'єкта, так і на етапі його експлуатації і, таким чином, забезпечити властивість керованості об'єкта захисту як об'єкта управління. Загальними характеристиками для організаційних і технічних засобів захисту є вартість захисту, вартість впровадження, вартість експлуатації, час впровадження, ступінь захисту. Отже, модель об'єкта захисту як системи, визначає передбачення загроз, організаційні та технічні засоби і методи захисту, визначають зміст і порядок проведення діяльності щодо забезпечення безпеки корпорації.

Розгляд основних елементів і властивостей об'єкта захисту як системи дозволяє обґрунтовано стверджувати, що підприємство можливо уявити як складну систему з точки зору забезпечення безпеки, так як йому притаманні 4 характерних властивості, які є фундаментальними у визначенні складної системи в термінах теорії множин. Це цілісність і наявність обумовлених зв'язків, певна організація та наявність інтегративних якостей. Системний аналіз дозволяє здійснити дійсно комплексний підхід до забезпечення безпеки, включаючи статичний і динамічний стан об'єкта захисту, забезпечити повноту і безперервність дій щодо забезпечення безпеки, розробити загальний підхід до проектування комплексних систем управління безпекою. Одним з узагальнених параметрів, що характеризують стійкість інформаційної інфраструктури, є показник «живучості», що включає в якості компонентів безпеку, надійність і доступність. Під «живучістю» слід розуміти здатність інфраструктури досягати поставленої мети постійним (безперервним) способом в умовах атак, збоїв і аварій. Метою ж є стійкість і процвітаюча діяльність організації в цілому. Звичайно, досягнення ефекту не дасть керівництву необхідних гарантій того,

що інформаційна інфраструктура, а тому і саме підприємство буде функціонувати належним чином.

Як наслідок, виняткову практичність набуває питання про методи і критерії оцінки безпеки інформаційних систем. Система оцінок повинна носити інтегральний характер, оскільки керівництво підприємства по суті справи цікавить не стільки конкретний рівень безпеки в приватних технологічних питаннях, скільки загальний рівень якості функціонування самого підприємства, що забезпечується, в тому числі, і рівнем безпеки інформаційних систем. З практичної точки зору це питання є найважчим. Наявні підходи до проблеми створення інструментів і методик оцінки інтегрального рівня інформаційної безпеки організації вельми суперечливі. Тим не менш, перерахуємо існуючі підходи:

- використання стандартів і норм аудиту фінансових організацій, включаючи аудит їх інформаційних систем і аудит безпеки цих систем;
- проведення аудиту IT-інфраструктури організації за стандартом безпеки комп'ютерних систем ISO 17799;
- застосування для оцінки захищеності інформаційних систем стандартів ISO 15408 «Відкриті критерії»;
- використання для оцінки захищеності інформаційних систем приватних методик і критеріїв, призначених для оцінки криптографічної стійкості алгоритмів шифрування і захищеності інформації від витоку по технічних каналах.

При цьому відбувається фактична підміна моделі загроз, в центрі якої стоять проблеми боротьби з легальним користувачем системи (він, як вже згадувалося, і є основним джерелом проблем), моделлю відповідних відомств, в центрі яких стоять суб'єкти несанкціонованого доступу. При такому підході фактично одні й ті ж питання в організації піддаються різним перевіркам за різними методиками, за підсумками яких виносяться певні судження про рівень безпеки окремих підсистем. Керівництво як було, так і залишається в деякому невіданні щодо того, наскільки правильно організована робота, чи достатній рівень безпеки, чи не знецінилися вкладення в цю сферу, або, навпаки, чи не занадто багато коштів витрачається на безпеку. Щодо цілей керівництва, яке об'єктивно зацікавлено у забезпеченні сталого та ефективного функціонування організації, то необхідно на всіх рівнях функціонування організації здійснювати прямий вплив на її діяльність в цілому.

З цієї точки зору найважливішою властивістю безпеки у забезпеченні інтересів організації в цілому виявляється можливість забезпечення її прозорості та контрольованості. Це необхідно враховувати при розробці політики безпеки інформаційних систем. Під *прозорістю* тут слід розуміти можливість отримання об'єктивної та цілісної інформації на всіх рівнях організації в обмежені терміни без створення конфліктної ситуації. Під *контролюванням* розуміють можливість отримання в обмежені терміни об'єктивної оцінки результатів рішень, прийнятих на даному рівні організації, і внесення відповідних змін до дії співробітників і підрозділів з метою

отримання бажаного результату. Реалізація цих властивостей дозволяє керівництву організації:

- зосередити свою увагу на найбільш важливих аспектах забезпечення безпеки організації;
- приймати рішення на основі об'єктивної та цілісної інформації;
- контролювати виникаючі ризики;
- домагатися з більшою ефективністю виконання прийнятих рішень;
- відстежувати якість прийнятих рішень та оперативно вносити необхідні корективи;
- значно підвищити передбачуваність результатів прийнятих рішень.

До теперішнього часу в нашій країні ще не склався стандартний підхід до оцінки ефективності роботи підрозділів інформаційної безпеки і на роль факторів, що роблять вплив на рівень інтегральної безпеки організації.

Регулюючі відомства поки не подають ознак того, що вони готові трансформувати свої погляди в бік більш реального обліку проблем і потреб громадянського сектора. Все це, безсумнівно, впливає на вироблення політики безпеки інформаційних систем організації і веде до необхідності врахування наступних факторів:

- визначення цілей захисту;
- визначення об'єкта захисту;
- визначення актуальних загроз, суб'єктів цих загроз, вибору профілів захисту;
- розробки методів визначення якості захисту або вибору вже існуючих систем критеріальних оцінок;
- отримання гарантій захищеності системи.

В умовах ситуації невизначеності досить поширена ситуація, коли організація, замовляючи послуги у сфері безпеки інформаційних систем, погано уявляє собі роль і місце конкретної послуги, так само як і її внесок в інтегральний рівень безпеки. Як наслідок, різко збільшуються витрати на забезпечення безпеки при практичній невизначеності в оцінці досягнутого ефекту. При цьому парадокс полягає в тому, що при подальших вкладеннях невизначеність оцінок практично не знижується, а складність реалізації заходів безпеки зростає. У практичній роботі з організації та підтримання рівня безпеки адекватного потребам організації (захищеності, безпеки) інформаційних ресурсів при розробці політики безпеки в умовах невизначеності та неоднозначності діючої в країні концептуальної, законодавчої та нормативної бази волею-неволею доводиться стикатися з вельми різноплановими факторами, що впливають на формування цієї політики. Слід також зазначити, що будь-який замовник послуг безпеки знаходиться під сильним інтелектуальним тиском постачальників таких послуг, і в першу чергу, постачальників обладнання та програмних засобів безпеки, а ці кошти орієнтовані на найпоширенішу модель загроз - модель НСД (несанкціонованого доступу). У результаті, за відсутності власної, адекватної реаліям, політики безпеки замовник набуває ті послуги, які пропонують постачальники, а не ті,

які необхідні самій організації. Тим часом, рівень багатьох фірм, навіть таких, що володіють усіма необхідними ліцензіями, далекий від досконалості.

### 7.2. Багаторівнева модель об'єктів інформаційної безпеки

Краще зрозуміти комплекс згаданих проблем, вибудувати ефективну політику безпеки організації, а також політику роботи з постачальниками послуг, допомагає багаторівнева модель структуризації об'єктів інформаційної безпеки, суть якої полягає в наступному: аналіз інформаційної інфраструктури організації дозволяє виділити сім рівнів технологій і реалізованих ними процесів, для яких принципово різняться актуальні загрози, агенти цих загроз, методи захисту, критерії оцінки ефективності і, нарешті, термінологія.

Ця модель дещо умовна. Не у всіх випадках наявні всі позначені рівні, однак у великій організації, що володіє власною корпоративною мережею, всі рівні простежуються зовсім виразно. Як правило, пропозиції щодо дуже гарних, ефективних та сертифікованих засобів забезпечення безпеки не виходять за III рівень і захищають від загроз, що виходять від суб'єкта НСД (табл. ).

Таблиця 1

Рівні інформаційної безпеки семирівневої моделі об'єктів інформаційної безпеки

| Номер рівня | Назва рівня |
|---|---|
| VII | Рівень бізнес-процесів |
| VI | Рівень додатків |
| V | Рівень системи управління базами даних |
| IV | Рівень операційних систем |
| III | Рівень мережевих додатків |
| II | Рівень мережі |
| I | Фізичний рівень |

Однак, парадокс ситуації полягає в тому, що найбільш небезпечним суб'єктом загроз в організації є легальний користувач, допущений до її ресурсів (зокрема, це підтверджує статистика по злочинах в банківській сфері.) Значення суб'єкта легального доступу різко зростає від III до VI рівня - саме там, де практично немає спеціальних засобів захисту і вся безпека базується на організації системи управління доступом, аудиту, забезпечення цілісності програм і штатності виконуваних бізнес-процесів. На стійкість забезпечення безпеки налаштувань впливає їх доступність великому числу адміністраторів систем і програмістів. Так як ступенів свободи у фахівців цієї категорії багато, а моніторинг їх діяльності, як правило, дуже слабкий, в цій зоні наявні відсутність «прозорості» і високий ступінь ризику. Іншими словами, на цих рівнях різко зростає роль «людського фактора», найбільш нестабільною і мінливою складовою у всій сукупності проблем, що впливають на безпеку.

Ще важча ситуація на VII рівні. Тут панує так званий «користувач», тобто «Суб'єкт легального доступу». Для нього комп'ютер - не більш ніж допоміжний інструмент на його робочому столі, із засобами НСД він стикається тільки при наборі пароля на вхід і при його заміні, в чужі каталоги не лазить, про проблеми налаштувань маршрутизаторів мережі та мережевої безпеки поняття не має. Крім того, як правило, він має різноманітні засоби комунікацій (факс, телефон, електронну пошту, Internet) і, само собою, може скопіювати дані на відчужений носій. IT-служба постійно піклується про те, щоб надати йому ще більше послуг, більше зручностей. Зовсім інша картина в сфері безпеки.

У компетенцію якої служби потрапляє проблема зловживання легальним доступом? Тут немає готових рішень. На жаль, можна дати рекомендації лише загального характеру. В організації повинна існувати детальна адміністративна політика щодо персоналу. Ця політика повинна детально регламентувати і мінімізувати права доступу співробітників до інформації, мети цього доступу, вимоги за регламентом використання доступної інформації. Адміністративна політика повинна підкріплюватися не менш детальним аудитом дій користувача з довіреної йому інформацією. Таким аудитом повинні бути охоплені не одні користувачі, але всі, хто має легальні права доступу до інформації, налаштувань обладнання, баз даних, операційним системам і т.д. Розбіжність адміністративної політики та аудиту означає наявність «конфлікту інтересів» організації та її співробітника. Необхідно дотримання принципу «прозорості»: співробітник повинен виразно пояснити всі свої дії з інформацією, виявлені системою аудиту. Повинен існувати звід корпоративних морально-етичних вимог, що чітко регламентують правила поведінки співробітника, що дозволяють виявити «конфлікт інтересів» і дають можливість керівництву застосувати, у разі потреби, адміністративні заходи стягнення. З персоналом має проводитися виховна робота, метою якої є вироблення у людей етики корпоративної поведінки та ставлення до ресурсів організації.

На кожному рівні ієрархії фахівці, що працюють з інформаційними ресурсами, використовують свою, притаманну тільки цьому рівню термінологію. З неї і формується понятійний апарат у галузі безпеки. При цьому такий апарат не може бути застосований на сусідньому рівні, а фахівці I і VII рівнів просто не розуміють один одного. Дійсно, чи можна вимагати від спеціаліста, який здійснює реєстрацію документа, навіть в електронній формі, щоб він знав і розумів, у чому виражається, що означає і яким має бути перехідне згасання сигналу при спільному пробігу кабелів зв'язку?

Багаторівнева модель дозволяє врахувати і присутність легального користувача. При цьому з кожним наступним рівнем даний фактор стає все значнішим. Очевидно і те, що говорити про будь-які гарантії безпеки без конкретної прив'язки до конкретного рівня моделі безглуздо. Хотілося б відзначити в цьому зв'язку, що говорити про відповідність захисту можна тільки в тому випадку, якщо необхідний рівень безпеки досягнуть на кожному «поверсі». Ну а рівень безпеки досягається шляхом застосування набору адекватних моделей загроз і властивих розглянутому рівню інструментів захисту. Таким чином, багато чого залежить від наявного інструментарію. До

III рівня справи йдуть зовсім непогано. Запитання технічного захисту від НСД непогано опрацьовані, мають достатньо ефективні сертифіковані засоби забезпечення безпеки. Питання тільки в їх вартості й зручності експлуатації. Далі ситуація серйозно змінюється. На рівнях вище III практично немає спеціальних сертифікованих засобів захисту, безпека цілком базується на програмних настройках систем управління доступом, аудиту, забезпечення цілісності програм і платності бізнес-процесів. Якість роботи адміністраторів систем, які повинні відслідковувати всі зміни адміністративної політики підрозділів, своєчасно вносячи зміни в налаштування системи управління доступом. Практика показує, що з часом ця якість слабшає, а політика управління доступом, надані користувачам права і паролі перестають відповідати адміністративній політиці. Доступність налаштувань, особливо при побудові мереж на персональних комп'ютерах, як правило, мають надлишкові і не потрібні простому користувачеві автономні можливості по їх адмініструванні, доступні великому числу користувачів, адміністраторів систем і програмістів.

Рішенням в даній ситуації є перехід до централізованої обробки і централізованого управління безпекою, розвиток аудиту подій в системі з обов'язковим оперативним розбором інформації з метою забезпечення їх прозорості для служби безпеки, а також посилення адміністративного компонента в управлінні персоналом. Саме це демонструють найбільші IT – корпорації, які домоглися практично повної централізації не тільки обробки, а й адміністрування ресурсів, виключивши з цього процесу власне користувачів і поставивши під контроль і аудит адміністраторів. Це, у свою чергу, вимагає наявності зрозумілої і логічної політики безпеки, розробленої для конкретної організації і з урахуванням ресурсів, які є для неї критичними. Так, в організації, що надає послуги передачі міжбанківських платежів, ресурс буде одним, а в банках, які користуються цією системою – зовсім іншим. Природно, що і політики безпеки в цих організаціях відрізняються, включаючи в першому випадку одну групу рівнів моделі, а в другому – іншу групу. Але в такому випадку вони відрізняються і за видами загроз, і за агентами цих загроз, і за методами захисту, і критеріями оцінки безпеки. При зовнішній схожості і загальної сфері діяльності двох цих організацій, безпека інформаційних систем у них разюче різниться.

### 7.3. Правила побудови системи інформаційної безпеки підприємства

**Система інформаційної безпеки підприємства повинна бути побудована з дотриманням таких правил:**

*Запобігання можливих загроз.* Необхідно своєчасне виявлення можливих загроз безпеки підприємства, аналіз яких дозволить розробити відповідні профілактичні заходи.

*Законність.* Заходи щодо забезпечення безпеки розробляються на основі і в рамках чинних правових актів. Локальні правові акти підприємства не повинні суперечити законам і підзаконним актам. Комплексне використання

сил і засобів. Для забезпечення безпеки використовуються всі наявні в розпорядженні підприємства сили та засоби. Кожен співробітник повинен, в рамках своєї компетенції, брати участь у забезпеченні безпеки підприємства. Організаційною формою комплексного використання сил і засобів є програма (план робіт) забезпечення безпеки підприємства.

*Координація та взаємодія всередині і поза підприємством.* Заходи протидії загрозам здійснюються на основі взаємодії та координації зусиль усіх підрозділів, служб підприємства, а також встановлення необхідних контактів із зовнішніми організаціями, здатними надати необхідне сприяння в забезпеченні безпеки підприємства. Організувати координацію і взаємодію всередині і поза підприємством може служба безпеки (СБ) підприємства (або керівник підприємства, якщо СБ в організації немає).

*Поєднання гласності з секретністю.* Доведення інформації до відома персоналу підприємства та громадськості в допустимих межах заходів безпеки виконує найважливішу роль - запобігання потенційних і реальних загроз.

*Компетентність.* Співробітники повинні вирішувати питання забезпечення безпеки на професійному рівні, а в необхідних випадках спеціалізуватися за основними його напрями управлінням.

*Економічна доцільність.* Вартість фінансових витрат на забезпечення безпеки не повинна перевищувати той оптимальний рівень, при якому втрачається економічний сенс їх застосування.

*Планова основа діяльності.* Діяльність щодо безпеки повинна будуватися на основі комплексної програми забезпечення безпеки підприємства, підпрограм забезпечення безпеки по основних його видах (економічна, науково - технічна, екологічна, технологічна і т. д.) і розроблюваних для їх виконання планів роботи підрозділів підприємства та окремих співробітників.

*Системність.* Цей принцип передбачає врахування всіх факторів, що впливають на безпеку підприємства, включення в діяльність щодо його забезпечення всіх співробітників, використання всіх сил і засобів.

### 7.4. Принципи захисту інформації

Побудову системи захисту доцільно проводити з принципами захисту, які досить універсальні для різних предметних областей (інженерне забезпечення в армії, фізична безпека осіб та територій тощо):

- *Адекватність* (розумна достатність). Сукупна вартість захисту (тимчасові, людські і грошові ресурси) повинна бути нижче вартості ресурсів, що захищаються. Якщо оборот компанії складає 10 тис. доларів на місяць, навряд чи є сенс розгортати систему на мільйон доларів (так, само як і навпаки).

- *Системність*. Важливість цього принципу особливо проявляється при побудові великих систем захисту. Він полягає в тому, що система захисту повинна будуватися не абстрактно (захист від усього), а на основі аналізу загроз, засобів захисту від цих загроз, пошуку оптимального набору коштів та побудови системи.

- *Прозорість для легальних користувачів*. Введення механізмів безпеки (зокрема аутентифікації користувача) неминуче призводить до ускладнення їх дій. Проте, ніякий механізм не повинен вимагати нездійсненних дій (наприклад, щотижня придумувати 10-значний пароль і ніде його не записувати) або затягувати процедуру доступу до інформації.

- *Рівноцінність ланок*. Ланки – це елементи захисту, подолання будь-якого з яких означає подолання всього захисту. Зрозуміло, що не можна слабкість одних ланок компенсувати посиленням інших. У кожному разі, міцність захисту (або її рівня, див. нижче) визначається міцністю найслабшої ланки. І якщо нелояльний співробітник готовий за 100 доларів «скинути на диск» цінну інформацію, то зловмисник навряд чи буде вибудовувати складну хакерську атаку для досягнення тієї ж мети.

- *Безперервність*. Загалом це та ж рівноцінність, тільки в тимчасовій області. Якщо ми вирішуємо, що будемо щось і якось захищати, то треба захищати саме так у будь-який момент часу. Не можна, наприклад, вирішити по п'ятницях робити резервне копіювання інформації, а в останню п'ятницю місяця влаштувати «санітарний день». Закон підлості невблаганний: саме в той момент, коли заходи по захисту інформації будуть ослаблені, відбудеться те, від чого ми захищалися. Тимчасовий провал у захисті, так само, як і слабка ланка, робить її безглуздою.

- *Багаторівневість*. Багаторівневий захист зустрічається повсюди, досить побродити по руїнах середньовічної фортеці. Навіщо захист будується в кілька рівнів, які повинен долати як зловмисник, так і легальний користувач (якому, зрозуміло, це робити легше)? На жаль, завжди існує ймовірність того, що якийсь рівень може бути подоланий або в силу непередбачених випадковостей, або з ненульовою ймовірністю. Проста математика підказує: якщо один рівень гарантує захист у 90 %, то три рівня (ні в якому разі не повторюють один одного) дадуть вам 99,9 %. Це, до речі, резерв економії: шляхом ешелонування недорогих і відносно ненадійних засобів захисту можна малою кров'ю домогтися дуже високого ступеня захисту. Облік цих принципів допоможе уникнути зайвих витрат при побудові системи захисту інформації і в той же час добитися дійсно високого рівня інформаційної безпеки бізнесу.

### 7.5. Методи і засоби забезпечення інформаційної безпеки організації.

Методами забезпечення захисту інформації є наступні:
- перешкода;
- управління доступом;
- маскування;
- регламентація;
- примус;
- спонукання.

*Перешкода* - метод фізичного перегородження шляху зловмиснику до інформації, що захищається (до апаратури, носіїв інформації і т. п.).

*Управління доступом* - метод захисту інформації регулювання використання всіх ресурсів автоматизованої інформаційної системи організації. Управління доступом включає наступні функції захисту:

- ідентифікацію користувачів, персоналу і ресурсів неформаційної системи (привласнення кожному об'єкту персонального ідентифікатора);
- аутентифікацію (встановлення автентичності) об'єкту або суб'єкта по пред'явленому їм ідентифікатору;
- перевірку уповноваження (перевірка відповідності дня тижня, часу доби, запрошуваних ресурсів і процедур встановленому регламенту);
- дозвіл і створення умов роботи в межах встановленого регламенту;
- реєстрацію (протоколювання) звернень до ресурсів, що захищаються;
- реагування (сигналізація, відключення, затримка робіт, відмова в запиті) при спробах несанкціонованих дій.

*Маскування* - метод захисту інформації автоматизованою інформаційною системою шляхом її криптографічного закриття.

*Регламентація* - метод захисту інформації, що створює такі умови автоматизованої обробки, зберігання та передачі інформації, при яких можливість несанкціонованого доступу до неї зводилася б до мінімуму.

*Примус* - такий метод захисту інформації, при якому користувачі та персонал системи змушені дотримуватися правил обробки, передачі і використання інформації, що захищається під загрозою матеріальної, адміністративної чи кримінальної відповідальності.

*Спонукання* - такий метод захисту інформації, який спонукає користувачів і персонал системи не порушувати встановлені правила за рахунок дотримання сформованих моральних і етичних норм.

Зазначені вище методи забезпечення інформаційної безпеки організації реалізуються на практиці застосуванням різних механізмів захисту, для створення яких використовуються такі основні засоби:

- фізичні,
- апаратні,
- програмні,
- апаратно-програмні,
- криптографічні,
- організаційні,
- законодавчі,
- морально-етичні.

**Фізичні засоби захисту** призначені для зовнішньої охорони території об'єктів, захисту компонентів автоматизованої інформаційної системи підприємства і реалізуються у вигляді автономних пристроїв і систем. Поряд з традиційними механічними системами за домінуючої участі людини розробляються і впроваджуються універсальні автоматизовані електронні системи фізичного захисту, призначені для охорони територій, охорони приміщень, організації пропускного режиму, організації спостереження; системи пожежної сигналізації; системи запобігання розкрадання носіїв.

**Апаратні засоби захисту** - це різні електронні, електромеханічні та інші пристрої, безпосередньо вбудовані в блоки автоматизованої інформаційної системи або оформлені у вигляді самостійних пристроїв і сполучаються з цими блоками. Вони призначені для внутрішнього захисту структурних елементів засобів і систем обчислювальної техніки: терміналів, процесорів, периферійного обладнання, ліній зв'язку і т.д.

**Програмні засоби захисту** призначені для виконання логічних і інтелектуальних функцій захисту і включаються або до складу програмного забезпечення автоматизованої інформаційної системи, або до складу коштів, комплексів і систем апаратури контролю. Програмні засоби захисту інформації є найбільш поширеним видом захисту, володіючи такими позитивними властивостями: універсальністю, гнучкістю, простотою реалізації, можливістю зміни і розвитку. Дена обставина робить їх одночасно і самими уразливими елементами захисту інформаційної системи підприємства. У даний час створено велику кількість операційних систем, систем управління базами даних, мережевих пакетів і пакетів прикладних програм, що включають різноманітні засоби захисту інформації.

## 7.6. Методика побудови корпоративної системи захисту інформації

Відповідно до закону «Про інформацію» цілями захисту інформації у тому числі є:

- запобігання витоку, розкрадання, втрати, спотворення, підробки інформації;
- запобігання несанкціонованих дій по знищенню, модифікації, спотворення, копіювання, блокування інформації;
- запобігання інших форм незаконного втручання в інформаційні ресурси та інформаційні системи.

Головна мета будь-якої системи інформаційної безпеки полягає у забезпеченні сталого функціонування об'єкта: запобіганні загроз його безпеки, захисту законних інтересів власника інформації від протиправних посягань, у тому числі кримінально-караних діянь у даній сфері відносин, передбачених Кримінальним кодексом України, забезпеченні нормальної виробничої діяльності всіх підрозділів об'єкта. Інше завдання зводиться до підвищення якості надаваних послуг і гарантій безпеки майнових прав та інтересів клієнтів.

Для виконання зазначених цілей необхідно:

- віднести інформацію до категорії обмеженого доступу (службової або комерційної таємниці);
- прогнозувати і вчасно виявляти загрози безпеки інформаційних ресурсів, причини та умови, що сприяють нанесенню фінансового, матеріального і морального збитку, порушення його нормального функціонування і розвитку;
- створити умови функціонування з найменшою імовірністю реалізації загроз безпеці інформаційних ресурсів і нанесення різних видів збитків;
- створити механізм та умови оперативного реагування на загрози інформаційної безпеки і прояву негативних тенденцій у функціонуванні,

ефективне припинення зазіхань на ресурси на основі правових, організаційних і технічних заходів і засобів забезпечення безпеки;

- створити умови для максимально можливого відшкодування та локалізації збитку, що наноситься неправомірними діями фізичних і юридичних осіб, і тим самим послабити можливий негативний вплив наслідків порушення інформаційної безпеки. При виконанні робіт можна використовувати наступну модель побудови корпоративної системи захисту інформації (рис. 1), засновану на адаптації Загальних Критеріїв (ISO 15408) і проведенні аналізу ризику (ISO 17799). Ця модель відповідає спеціальним нормативним документам щодо забезпечення інформаційної безпеки, прийнятим в Україні, міжнародному стандарту ISO / IEC 15408 «Інформаційна технологія методи захисту критерії оцінки інформаційної безпеки», стандартом ISO / IEC 17799 «Управління інформаційною безпекою» і враховує тенденції розвитку вітчизняної нормативної бази з питань захисту інформації.

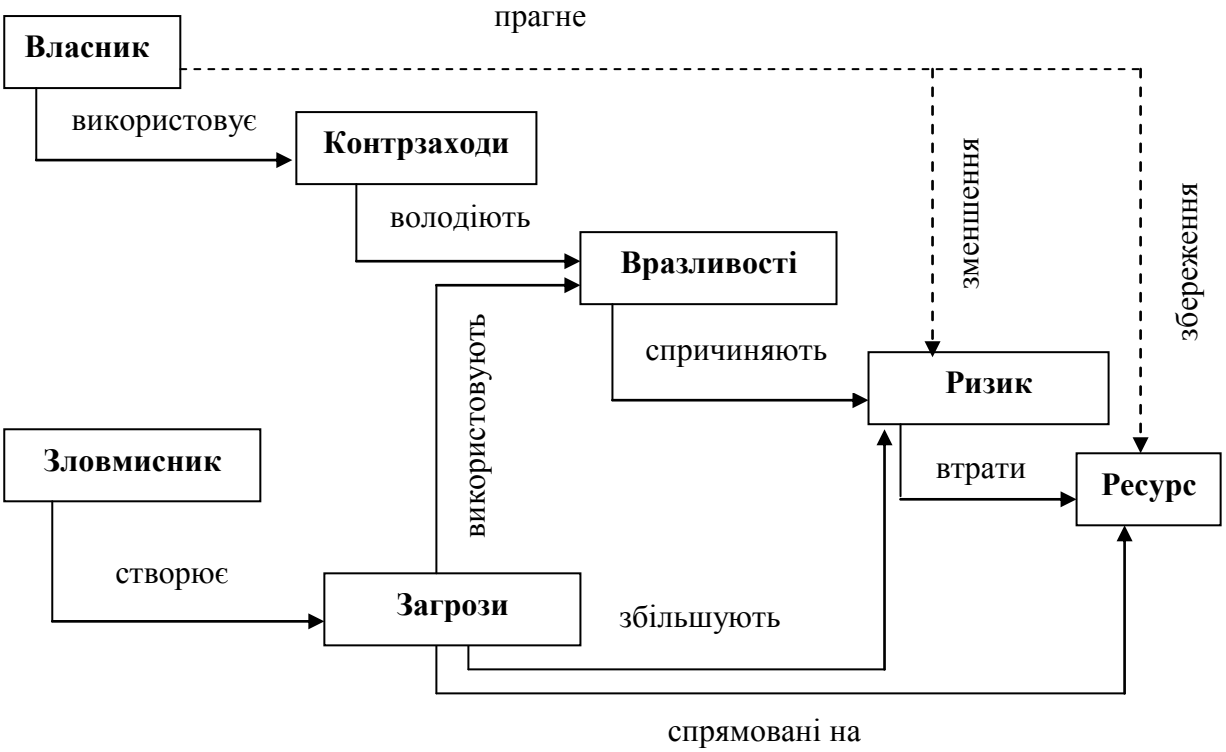


Рис. 1. Модель побудови корпоративної системи захисту інформації

Представлена модель захисту інформації – це сукупність об'єктивних зовнішніх і внутрішніх факторів і їх вплив на стан інформаційної безпеки на об'єкті та на збереження матеріальних або інформаційних ресурсів.

Розглядаються наступні об'єктивні фактори:

- загрози інформаційній безпеці, що характеризуються ймовірністю виникнення і ймовірністю реалізації;

- уразливості інформаційної системи або системи контрзаходів (системи інформаційної безпеки), що впливають на ймовірність реалізації загрози;

- ризик - фактор, що відображає можливий збиток організації в результаті реалізації загрози інформаційної безпеки: витоку інформації та її

неправомірного використання (ризик в кінцевому підсумку відображає ймовірні фінансові втрати прямі або непрямі).

Для побудови збалансованої системи інформаційної безпеки передбачається спочатку провести аналіз ризиків в області інформаційної безпеки. Потім визначити оптимальний рівень ризику для організації на основі заданого критерію. Систему інформаційної безпеки (контрзаходи) належить побудувати таким чином, щоб досягти заданого рівня ризику. Розглянута методика проведення аналітичних робіт дозволяє:

- повністю проаналізувати і документально оформити вимоги, пов'язані із забезпеченням інформаційної безпеки;
- уникнути витрат на зайві заходи безпеки, можливих при суб'єктивній оцінці ризиків;
- надати допомогу в плануванні і здійсненні захисту на всіх стадіях життєвого циклу інформаційних систем;
- забезпечити проведення робіт у стислі терміни;
- представити обгрунтування для вибору заходів протидії;
- оцінити ефективність контрзаходів;
- порівняти різні варіанти контрзаходів.

У ході робіт мають бути встановлені кордони дослідження. Для цього необхідно виділити ресурси інформаційної системи, для яких надалі будуть отримані оцінки ризиків. При цьому належить розділити представлені ресурси і зовнішні елементи, з якими здійснюється взаємодія. Ресурсами можуть бути засоби обчислювальної техніки, програмне забезпечення, дані, окремі документи і окремі масиви документів, документи і масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, інших інформаційних системах). Прикладами зовнішніх елементів є мережі зв'язку є зовнішні сервіси. При побудові моделі необхідно враховувати взаємозв'язки між ресурсами. Наприклад, вихід з ладу будь-якого обладнання може призвести до втрати даних або виходу з ладу іншого критично важливого елементу системи. Подібні взаємозв'язки визначають основу побудови моделі організації з точки зору інформаційної безпеки.

Ця модель, відповідно до запропонованої методики, будуватиметься таким чином: для виділених ресурсів визначається їх цінність, як з точки зору асоційованих з ними можливих фінансових втрат, так і з точки зору шкоди репутації організації, дезорганізації її діяльності, нематеріальної шкоди від розголошення конфіденційної інформації. Потім описуються взаємозв'язки ресурсів, визначаються загрози безпеки і оцінюються ймовірності їх реалізації.

На основі побудованої моделі можна обґрунтовано вибрати систему контрзаходів, що знижують ризики до допустимих рівнів і володіють найбільшою цінової ефективністю. Частиною системи контрзаходів будуть рекомендації з проведення регулярних перевірок ефективності системи захисту. Забезпечення підвищених вимог до інформаційної безпеки передбачає відповідні заходи на всіх етапах життєвого циклу інформаційних технологій. Планування цих заходів проводиться по завершенні етапу аналізу ризиків та вибору контрзаходів. Обов'язковою складовою частиною цих планів є

періодична перевірка відповідності існуючого режиму інформаційної безпеки політиці безпеки, сертифікація інформаційних систем (технологій) на відповідність вимогам певного стандарту безпеки. По завершенні робіт, можна буде визначити міру гарантії безпеки інформаційного середовища, засновану на оцінці, з якою можна довіряти інформаційному середовищі об'єкта.

Даний підхід передбачає, що велика гарантія випливає з застосування великих зусиль при проведенні оцінки безпеки. Адекватність оцінки заснована на залученні в процес оцінки більшого числа елементів інформаційного середовища об'єкта, глибині, що досягається за рахунок використання при проектуванні системи забезпечення безпеки більшого числа проектів та описів деталей виконання, строгості, яка полягає у застосуванні більшої кількості інструментів пошуку і методів, спрямованих на виявлення менш очевидних вразливостей або на зменшення ймовірності їх наявності.

### 7.7. Формування організаційної політики безпеки

Перш ніж пропонувати будь-які рішення у системі інформаційної безпеки, необхідно розробити політику безпеки. Організаційна політика безпеки визначає порядок надання та використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки. Система інформаційної безпеки виявиться ефективною, якщо вона буде надійно підтримувати виконання правил політики безпеки, і навпаки. Етапи побудови організаційної політики безпеки – це внесення в опис об'єкта автоматизації структури цінності та проведення аналізу ризику, та визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають даний ступінь цінності.

Організаційна політика безпеки оформляється у вигляді окремого документа. Перш за все, необхідно скласти деталізований опис спільної мети побудови системи безпеки об'єкта, яке виражається через сукупність факторів або критеріїв, уточнюючих мету. Сукупність факторів служить базисом для визначення вимог до системи (вибір альтернатив). Фактори безпеки, у свою чергу, можуть розподілятися на правові, технологічні, технічні та організаційні. Вимоги гарантії досягнення захисту виражаються через оцінки функцій безпеки системи інформаційної безпеки об'єкта. Оцінка сили функцій безпеки виконується на рівні окремого механізму захисту, а її результати дозволяють визначити відносну здатність відповідної функції безпеки протистояти ідентифікованим загрозам. Виходячи з відомого потенціалу нападу, сила функції захисту визначається, наприклад, категоріями «базова», «середня», «висока».

Потенціал нападу визначається шляхом експертизи можливостей, ресурсів і мотивів спонукання нападника. Перелік вимог до системи інформаційної безпеки, ескізний проект, план захисту (далі - технічна документація), містить набір вимог безпеки інформаційного середовища об'єкта, які можуть посилатися на відповідний профіль.

**У загальному вигляді розробка технічної документації включає:**

- уточнення функцій захисту;

- вибір архітектурних принципів побудови системи інформаційної безпеки;

- розробку логічної структури системи інформаційної безпеки (чіткий опис інтерфейсів);

- уточнення вимог функцій забезпечення гарантоспроможності системи інформаційної безпеки;

- розробку методики і програми випробувань відповідно до сформульованих вимог.

На етапі оцінки проводиться оцінка заходів гарантування безпеки інформаційного середовища. Ступінь гарантії ґрунтується на оцінці, з якою після виконання рекомендованих заходів можна довіряти інформаційному середовищі об'єкта. Базові положення даної методики припускають, що ступінь гарантії випливає з ефективності зусиль при проведенні оцінки безпеки. Збільшення зусиль оцінки передбачає:

- значне число елементів інформаційного середовища об'єкта, що беруть участь в процесі оцінювання;

- розширення типів проектів та описів деталей виконання при проектуванні системи забезпечення безпеки;

- строгість, яка полягає у застосуванні більшої кількості інструментів пошуку і методів, спрямованих на виявлення менш очевидних вразливостей або на зменшення ймовірності їх наявності.

### 7.8. Особливості розробки концепції безпеки

Для більш глибокого розуміння проблеми наведемо декілька факторів, що дозволяють оцінити особливості розробки, якість і повноту вже розроблених концепцій безпеки, пропонованих керівникам підприємств. При формуванні та реалізації повноцінної концепції безпеки керівник підприємства (або начальник служби безпеки) повинен провести аналіз штатної структури фірми, визначити пріоритетність своїх співробітників залежно від їх цінності для підприємства: кваліфікації, взаємозамінності, ступеня поінформованості про діяльність організації, особистого внеску в загальну справу, перспективності, доступу до фінансів, матеріальних і інтелектуальних цінностей. Без цього неможливо захистити співробітників від реальних загроз. Аналогічно слід вчинити з матеріальними цінностями, нерухомістю і транспортними засобами. При визначенні пріоритетів захисту необхідно мати на увазі, що найбільше потребують захисту ті об'єкти і матеріальні цінності, без яких підприємство не зможе працювати або взагалі припинить своє існування. Для одних це може бути комп'ютер з базою даних, для інших - офісне приміщення, для третіх - транспортні засоби. У ході розробки заходів захисту інформації розробники у концепції спільно з керівником підприємства повинні визначити:

- яка інформація підлягає обов'язковому захисту відповідно до чинного законодавства;

- яка інформація є комерційною таємницею і має право на захист;

- хто і за яких обставин має право доступу до перерахованих видів інформації.

При аналізі слід враховувати інформацію, що зберігається як на паперових носіях, так і в електронному вигляді. До об'єктів захисту необхідно віднести і канали прийому-передачі інформації, вразливі для технічних засобів перехоплення. Не слід забувати при цьому, що персонал організації може бути не тільки носієм, а й джерелом витоку інформації. Тобто в організаціях, що мають конфіденційну інформацію, список об'єктів захисту буде досить великим. У подібних випадках рекомендується ранжувати список інформаційних об'єктів захисту так само, як і матеріальних: за ступенем можливого заподіяння шкоди діяльності організації у разі впливу на неї різних видів загроз.

У концепції повинні бути передбачені способи захисту від реальних загроз, в тому числі:

- організаційні (адміністративні, економічні, юридичні);
- технічні (встановлення охоронно-пожежної сигналізації, використання систем контролю і управління доступом, при трансформаційних змінах технічних засобів захисту інформації, впровадження інтегрованих систем безпеки);
- фізичні (робота сторожів і контролерів, охоронців та інкасаторів, службових собак);
- оперативні (використання оперативних методів роботи, оперативно-технічних засобів, наприклад « поліграфа » для вхідного контролю та періодичної перевірки лояльності персоналу).

Концепція обов'язково повинна містити об'єктивну оцінку рентабельності системи безпеки в умовах реально прогнозованих загроз. Керівник підприємства, приймаючи рішення про прийняття та реалізацію концепції, повинен точно знати, за що він платить гроші, тобто що конкретно дає йому той чи інший елемент системи безпеки і який збиток він понесе за відсутності цього елемента в системі захисту в ситуації реальної загрози.

Таким чином, розумну верхню межу асигнувань на реалізацію концепції керівник повинен оцінити сам шляхом зіставлення збитків від реалізації конкретної загрози і витрат на організацію захисту від цієї загрози (за аналогією з системою страхування – зіставлення страхового внеску і збитку при настанні страхового випадку). При цьому необхідно мати на увазі, що захист - це запобігання загроз і нещасть, а страхування – компенсація збитків від наслідки нещасть, що відбулися і реалізації загроз.

Найбільш раціональним з точки зору економії коштів і підвищення відповідальності виконавця за результати своєї роботи є варіант, коли розробка концепції безпеки доручається організації, здатній не тільки ставити комплексні оперативно-технічні завдання щодо забезпечення безпеки, а й успішно їх вирішувати, здаючи службі безпеки підприємства в експлуатацію «під ключ» повний комплекс технічних засобів і заходів безпеки, який сформований в залежності від обраного переліку об'єктів захисту і набору найбільш ймовірних загроз, здатних заподіяти підприємству максимальний

збиток. Критерієм якості концепції безпеки, розробленої спеціалізованим виконавцем, є можливість її використання не як жорсткої одноваріантної конструкції, а як саморозвиваючу систему, здатну адаптуватися до нових загрозам, оптимізувати витрати, підвищувати ефективність діяльності підприємства. Однак не слід забувати, що жодна, система не здатна забезпечити необхідний рівень безпеки без належної підготовки служби безпеки і персоналу організації, без проведення навчання, тренувань, ігор і навчань.

### 7.9. Страхування інформаційних ризиків

Діяльність будь-якої організації так чи інакша схильна до загроз і, відповідно, пов'язана з ризиками їх настання. Розвиток і поширення інформаційних технологій окрім розширення можливостей і підвищення ефективності роботи тягне за собою посилення залежності від інформаційно-телекомунікаційних систем і, як наслідок, змінює структуру підприємницького ризику. Зокрема, зростає стратегічний ризик у зв'язку з можливістю помилитися щодо вибору того чи іншого інформаційно-технологічного напрямку.

Збільшується операційний ризик у зв'язку з можливими збоями в інформаційних системах при виконанні ділових та управлінських операцій. Зростають також правовий, репутаційний та системний ризики.

*Правовий ризик* зростає у зв'язку з відставанням нормативної бази від розвитку інформаційних технологій.

*Репутаційний ризик* зростає у зв'язку з поширенням інформації про збої та проблеми, пов'язані з використовуваними новими інформаційними технологіями, навіть якщо вони відбуваються не в даній організації, а при використанні подібних систем десь в іншому місці.

*Системний ризик* належить до сфери діяльності (галузі) в цілому і є приводом для занепокоєння організацій, відповідальних за її стан. Зазначене посилення залежності результатів роботи організацій від роботи інформаційних систем вимагає відповідного забезпечення інформаційної безпеки.

Забезпечення безпеки підприємницької та управлінські діяльності має на меті зниження ризиків, з якими пов'язане її ведення, до якогось прийнятного рівня. Результати роботи визначаються не наявністю ризиків, а тим, наскільки успішно керівництво підприємств і організацій оцінює їх і вживає заходів щодо їх зниження. Які заходи можуть бути прийняті для компенсації зростання ризиків у зв'язку з розвитком інформаційних технологій? Звичайною рекомендацією є забезпечення адекватного рівня безпеки у сфері інформаційних технологій (інформаційної безпеки). Однак, тут виникає питання: що вважати адекватним? Абсолютної безпеки не існує, крім того, заходи і засоби безпеки вимагають витрат і постійної модернізації. Як зіставити конкретні витрати з можливими (зовсім не обов'язково) втратами? Вживання заходів безпеки можна доповнити іншою мірою компенсації ризиків страхуванням інформаційних ресурсів. Ця послуга поки ще повільно, але все-таки пробиває собі дорогу в Україні. Її розвиток стримується через

недосконаліть методик оцінювання вартості інформаційних ресурсів і ризиків. Однією з причин цього є те, що статистика пригод неповна і недостовірна. За наявними оцінками, велика частина інцидентів, пов'язаних з порушеннями інформаційної безпеки, не віддається розголосу. Інша причина полягає у відсутності єдиної системи оцінки стану захищеності інформаційної системи організації. Не зовсім зрозуміло, яким вимогам повинна задовольняти система забезпечення інформаційної безпеки з урахуванням її вартості і ризиків втрат. Наслідком цього є висока вартість даної страхової послуги, яка випливає з експертної оцінки «із запасом».

Вихід представляється в більш тісній ув'язці умов страхування з оцінкою стану захищеності інформаційної системи організації. Якщо знайти такі умови, які були б вигідні всім учасникам процесу, то підприємства та організації отримають гарантований захист від втрат на умовах, які залежать від прийнятих заходів забезпечення безпеки. Витрати підприємства будуть складатися з вартості заходів інформаційної безпеки та оплати страхування, причому підвищення заходів безпеки знижує за інших рівних умов вартість страховки. Страхові ж компанії розширять клієнтуру за рахунок зниження страхових внесків для тих клієнтів, які відповідають заданим вимогам безпеки. Послуга страхування інформаційних ризиків подешевшає і стане доступною не тільки для великих, але й середніх і дрібних підприємств. Комерційна вигода для страхових компаній буде полягати в тому, що вони підвищать прибутковість свого бізнесу за рахунок зниження числа страхових випадків у тих клієнтів, які відповідають заданим вимогам безпеки: більш захищений клієнт платить менший внесок, але і ймовірність того, що йому доведеться виплачувати страховку, менше, ніж для менш захищеного. Зазначене вище потенційне розширення клієнтури також є позитивним чинником для страхувальників. Для широкого використання страхування інформаційних ризиків необхідно виробити стандартизовані вимоги до інформаційної безпеки, що дозволяють оцінювати її стан в конкретній організації з якоюсь загальною шкалою, буде потрібно оцінити здійсниміть умов, при яких дана взаємодія буде економічно вигідно всім учасникам, тобто знайти відповідне співвідношення умов страхування та заходів захисту. Для досягнення цього потрібні відповідні форми співпраці між страховими компаніями, організаціями - клієнтами та постачальниками послуг інформаційної безпеки.

У цілому розглянута вище методика дозволяє оцінити або переоцінити рівень поточного стану захищеності інформаційних активів підприємства, а також виробити рекомендації щодо забезпечення (підвищення) інформаційної безпеки. У тому числі знизити потенційні втрати шляхом підвищення стійкості функціонування корпоративної мережі, розробити концепцію і політику безпеки.

## ТЕМА 8:

## «Організаційні заходи захисту інформації суб'єктів господарювання»

## ПЛАН

8.1. Комерційна таємниця
8.2. Конфіденційна інформація
8.3. Організаційні заходи захисту інформації на підприємстві

### Література:

1. Браіловський М.М., Хорошко В.О., Чирков Д.В., Шелест М.Е. Захист економічної інформації. Навчальний посібник / За редакцією професора В.О. Хорошка: – К.: НАУ, 2002. – 78 с.

2. Кавун С. В. Інформаційна безпека. Навчальний посібник. Ч. 2 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 196 с.

3. Игнатьев В.А. Информационная безопасность современного коммерческого предприятия: Монография. –Старый Оскол: ООО «ТНТ», 2005. – 448 с.

### 8.1. Комерційна таємниця

З погляду законодавства **комерційна таємниця (КТ)** - це відомості, зв'язані з виробництвом, технологічною інформацією, керуванням, фінансами й іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) якої може завдати шкоди інтересам підприємства (Господарський кодекс України).

Основним документом, що визначає перелік зведень, які відносяться до КТ на підприємстві, виступає відповідний Наказ керівника «Про комерційну таємницю», зміст якого не повинен суперечити положенням діючого законодавства.

Підставою для прийняття такого Наказу служить частина 2 статті 30 вищезгаданого Закону: «Склад і обсяг зведень, що представляють КТ, порядок їх захисту визначаються керівником підприємства. Відомості, що не можуть складати КТ, визначаються Кабінетом міністрів України».

*Відповідно до Господарського кодексу України КТ не складають:*

- установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю і її окремими видами;
- інформація з усіх установлених форм державної звітності;
- дані, необхідні для перевірки нарахування і сплати податків і інших обов'язкових платежів;
- відомості про чисельність і склад працюючих, їх заробітню плату в цілому і по професіях і посадах, а також про наявність вільних робочих місць;
- документи про сплату податків і обов'язкових платежів;

- інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізації продукції, що наносить шкоду здоров'ю, а також про інші порушення законодавства України і розмірах нанесених при цьому збитків;

- документи про платоспроможність;

- відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, союзах, об'єднаннях і інших організаціях, що займаються підприємницькою діяльністю;

- відомості, що підлягають оголошенню, відповідно до діючого законодавства.

Приведений перелік на перший погляд «лякає» своїм «розмахом», тим більше, що розсекречення перерахованої вище інформації може реально зашкодити інтересам багатьох фірм. Насамперед, це зв'язано з можливістю заволодіння даною інформацією конкурентами, здатними на несумлінну боротьбу на ринку.

Щоб не допустити виникнення подібної ситуації, підприємці повинні враховувати, що:

1. Підприємства зобов'язані надавати перераховані в Постанові № 611 відомості тільки контролюючим органам державної виконавчої влади і правоохоронним органам, іншим юридичним особам і тільки відповідно до чинного законодавства. Порядок надання інформації даним органам регламентується Законами України «Про інформацію», «Про прокуратуру», «Про Службу безпеки України», «Про державну податкову службу», «Про державну контрольно-ревізійну службу в Україні», іншими нормативними актами.

2. Відповідно до Закону України «Про інформацію» громадяни, юридичні особи, що володіють інформацією професійного, ділового, виробничого, банківського, комерційного й іншого характеру, отриманої на власні засоби, або такою, котра є предметом їх професійного, ділового, виробничого, банківського, комерційного й іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи приналежність її до категорії конфіденційної, і встановлюють для неї систему (способи) захисту. Для цього, крім Наказу про комерційну таємницю, підприємства можуть затверджувати посадові інструкції з вказівкою порядку і системи обміну інформацією між співробітниками підприємства і зовнішніх користувачів, встановлювати деталізований графік документообігу з призначенням осіб, відповідальних за витік інформації, вносити спеціальні розділи в трудові угоди і контракти і т.д.

*Перелік типових відомостей, що складають комерційну таємницю.*

У приведеному нижче переліку відомості, що складають комерційну таємницю, згруповані по тематичному принципі. Пропонований поділ на групи носить рекомендаційний характер і може бути змінене в залежності від специфіки відомостей, що складають комерційну таємницю конкретного підприємства (організації).

Відомості, включені в даний перелік, є комерційною таємницею тільки з урахуванням особливостей конкретного підприємства.

1.Відомості про фінансову діяльність:

- прибуток, кредити, товарообіг;
- фінансові звіти і прогнози;
- комерційні задуми;
- фонд заробітної плати;
- вартість основних і оборотних фондів;
- кредитні умови платежу;
- банківські рахунки;
- планові,звітні калькуляції.

2. Інформація про ринок:

- ціни, знижки, умови договорів, специфікація продукції;
- обсяг, історія, тенденції виробництва і прогноз для конкретного продукту;
- ринкова політика і плани;
- маркетинг і стратегія цін;
- відносини зі споживачами і репутація;
- чисельність і розміщення торгових агентів;
- канали і методи збуту;
- політика збуту;
- програма реклами.

3. Відомості про виробництво і продукцію:

- відомості про технічний рівень, техніко-економічні характеристики розроблювальних виробів;
- відомості про плановані терміни створення розроблювальних виробів;
- відомості про плановані терміни створення розроблювальних виробів;
- відомості про застосовувані і перспективні технології, технологічні процеси, прийоми і устаткування;
- відомості про модифікацію і модернізацію раніше відомих технологій, процесів, устаткування;
- виробничі потужності;
- стан основних і оборотних фондів;
- організації виробництва;
- розміщення і розмір виробничих приміщень і складів;
- перспективні плани розвитку виробництва;
- технічні специфікації існуючої і перспективної продукції;
- схеми і креслення окремих вузлів, готових виробів, нових розробок;
- відомості про стан програмного і комп'ютерного забезпечення;
- оцінка якості й ефективності;
- номенклатура виробів;
- спосіб упакування;
- доставка.

4. Відомості про наукові розробки:

- нові технологічні методи, технологічні і фізичні принципи, плановані до використання в продукції підприємства;

- програми НДР;

- нові алгоритми;

- оригінальні програми.

5. Відомості про систему матеріально-технічного забезпечення:

- відомості про склад торгових клієнтів, представників і посередників;

- потреби в сировині, матеріалах, що комплектують вузли і деталі, джерела задоволення цих потреб;

- транспортні й енергетичні потреби.

6. Відомості про персонал підприємства:

- чисельність персоналу підприємства;

- визначення облич, що приймають рішення, і їхня філософія.

7. Відомості про принципи керування підприємством:

- відомості про застосовувані і перспективні методи керування виробництвом;

- відомості про факти ведення переговорів, предметах і цілях нарад і засідань органів керування;

- відомості про плани підприємства по розширенню виробництва;

- умови продажу і злиття фірм.

8. Інші відомості:

- важливі елементи систем безпеки, кодів і процедур доступу до інформаційних мереж і центрів;

- принципи організації захисту комерційної таємниці.

Приведена класифікація носить рекомендаційний характер і може мінятися в залежності від виду чи роботи специфіки підприємства.

Організація може мати інформацію, що складає комерційну таємницю, чотирьох рівнів важливості:

*1. Життєво важлива* - незамінна інформація, наявність якої необхідно для функціонування підприємства. Витік цієї інформації ставить під загрозу самофункціонування організації (підприємства).

*2. Важлива* - інформація, процес ліквідації наслідків витоку якої складний чи зв'язаний з великими витратами.

*3. Корисна* - інформація, витік якої завдає матеріальної шкоди підприємству, однак вона може ефективно функціонувати й у випадку витоку цієї інформації.

*4. Несуттєва інформація*- витік якої не наносить матеріального збитку підприємству і не впливає на його функціонування.

Інформація, що відноситься до перших трьох рівнів, є комерційною таємницею. Для забезпечення збереження зведень, що складають комерційну таємницю, необхідно наказом по підприємстві ввести наступні нові грифи інформації зі ступеня важливості:

- для життєво важливої - КОМЕРЦІЙНА ТАЄМНИЦЯ 3 (КТ 3);

- для важливої - КОМЕРЦІЙНА ТАЄМНИЦЯ 2 (КТ 2);

- для корисної - КОМЕРЦІЙНА ТАЄМНИЦЯ 1(КТ 1).

## 8.2. Конфіденційна інформація

**Конфіденційна інформація (КІ)** - це відомості, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням відповідно до передбачениих ними умовами (ст. 30 Закону України «Про інформацію»).

Як ми бачимо з визначення, підприємства, крім захисту КТ, також мають право і на захист КІ. І якщо склад першої регламентується Постановою Кабінету міністрів, то перелік зведень, що відносяться до другого, обмежується тільки Законом «Про інформацію», у відповідності, з яким не може бути КІ:

- інформація комерційного і банківського характеру;
- інформація, правовий режим якої установлений Верховною Радою України;
- інформація, приховання якої створює загрозу життю і здоров'ю людей.

З усього вищесказаного можна зробити висновок: частина інформації, що відповідно до діючих нормативами не може бути визнана КТ, у той же час може затверджуватися на підприємстві як КІ, режим використання якої встановлюється підприємством самостійно на підставі окремого Наказу керівника «Про конфіденційну інформацію».

Така інформація захищена:

1) Конституцією України: «Не допускається збір, збереження, використання і поширення КІ про особу без її згоди, за винятком випадків, встановлених Законом, і тільки в інтересах національної безпеки, економічного добробуту і прав людини» (ч. 2, ст. 32);

2) Господарським кодексом України: «Учасники товариства зобов'язані:...- не розголошувати КТ і КІ щодо діяльності підприємства»;

3) Законом України «Про обмеження монополізму і недопущення недобросовісної конкуренції в підприємницькій діяльності»:

«Недобросовісною конкуренцією визнається - одержання, використання, розголошення КТ, а також КІ з метою заподіяння шкоди ділової репутації чи майну іншого підприємця» (ст. 7);

4) Законом України «Про державну податкову службу в Україні»: «Службові особи державних податкових інспекцій зобов'язані зберігати комерційну і службову таємниці» (ст. 13);

5) Кодексом України про адміністративні правопорушення: «...Одержання, використання, розголошення КТ, а також КІ з метою заподіяння шкоди ділової репутації чи майну іншого підприємця спричиняє накладення штрафу від 10 до 20 мінімальних розмірів заробітної плати» (ст. 164-3);

6) Законом України «Про захист від недобросовісної конкуренції» установлено, що вважається розголошенням КТ «Розголошенням КТ є ознайомлення іншої особи без згоди особи, уповноваженої на це, із відомостями, що, відповідно до чинного законодавства, складають КТ, особою, якій ці відомості були довірені у встановленому порядку чи стали відомими в зв'язку з виконанням службових обов'язків, якщо це нанесло чи могло завдати шкоди суб'єкту, що хазяює, (підприємцю)» (ст. 16).

7) Кримінальним кодексом України: «Незаконний збір з метою використання зведень, що складають КТ, якщо це принесло великий матеріальний збиток суб'єкту підприємницької діяльності, - карається позбавленням волі на термін до трьох років чи штрафом від 300 до 500 мінімальних розмірів заробітної плати» (ст. 231);

«Навмисне розголошення КТ - карає позбавленням волі на термін до 2-х років...» (ст. 232);

Усього більш 30 законів та нормативних документів України містять положення, зв'язані в тій чи іншій мірі з захистом КТ і КІ.

У процесі організації захисту КТ також необхідно пам'ятати і про те, що відповідно до Закону України «Про аудиторську діяльність» відкриття бухгалтерської звітності, що складає КТ, для проведення аудиту відбувається тільки користувачами бухгалтерської звітності (ч. 3, ст.8). Цими користувачами можуть бути тільки уповноважені на підставі законів України представники органів державної влади, юридичні і фізичні особи, зацікавлені в наслідках господарської діяльності суб’єктів, у тому числі: власники, засновники, орендарі, інвестори й інші особи, що на підставі законів мають право на одержання інформації з бухгалтерської звітності. При цьому дане положення не поширюється на іншу інформацію.

## 8.3. Організаційні заходи захисту інформації на підприємстві

**Система захисту інформації** - раціональна сукупність напрямків, методів, засобів і заходів, що знижують уразливість інформації та перешкоджають несанкціонованому доступу до інформації, її розголошенні або витоку.

Структура системи захисту охоплює не тільки електронні інформаційні системи, а весь управлінський комплекс фірми. При формуванні системи безпеки необхідно чітко усвідомити, які завдання перед нею стоять (рис. 1).


Рис. 1 Завдання системи безпеки інформації

Для вирішення цих завдань використовується комплекс заходів, до числа яких входить система організаційних заходів (рис. 2).


Рис. 2. Заходи щодо забезпечення захисту інформації

Основна характеристика системи: комплексність, тобто наявність у ній обов'язкових елементів, що охоплюють всі напрямки захисту інформації.

Співвідношення елементів та їх утримання забезпечують індивідуальність побудови системи захисту інформації і гарантують неповторність системи, труднощі її подолання.

**Елементами системи є:** правовий, організаційний, інженерно-технічний, програмно-апаратний і криптографічний елементи.

Організаційний елемент системи захисту інформації містить заходи управлінського, обмежувального та технологічного характеру, що визначають основи і зміст системи захисту, які спонукають персонал дотримуватися правил захисту конфіденційної інформації фірми. Елемент включає в себе регламентацію:

1) Формування та організації діяльності служби безпеки та служби конфіденційної документації, забезпечення діяльності цих служб нормативно-методичними документами з організації і технології захисту інформації.

2) Складання і регулярного оновлення складу захисту інформації фірми, складання та ведення переліку паперових, машино читальних та електронних документів.

3) Дозвільної системи розмежування доступу персоналу до інформації, що захищається.

4) Методів відбору персоналу для роботи з інформацією що захищається, методики навчання і інструктування співробітників.

5) Напрямів і методів виховної роботи з персоналом, контролю дотримання співробітниками порядку захисту інформації.

6) Технології захисту, обробки та зберігання паперових, машино читальних та електронних документів, поза машинної технології захисту електронних документів.

7) Порядку захисту цінної інформації фірми від випадкових або навмисних несанкціонованих дій персоналу.

8) Ведення всіх видів аналітичної роботи.

9) Порядку захисту інформації при проведенні нарад, засідань, переговорів, прийомі відвідувачів, роботі з представниками ЗМІ.

10) Обладнання та атестації приміщень і робочих зон, виділених для роботи з конфіденційною інформацією.

11) пропускного режиму на території, в будівлі, приміщеннях, ідентифікації транспорту і персоналу фірми.

12) Системи охорони території.

13) Дій персоналу в екстремальних ситуаціях.

14) Організаційних питань придбання, встановлення та експлуатації технічних засобів захисту інформації та охорони.

15) Роботи з управління системою захисту інформації.

16) Критеріїв і порядку проведення оціночних заходів щодо встановлення ступеня ефективності системи захисту інформації.

Система організаційних заходів щодо захисту інформації являють собою комплекс заходів, що включають чотири основні компоненти:

- вивчення обстановки на об'єкті;
- розробку програми захисту;
- діяльність з проведення зазначеної програми в життя;
- контроль за її дієвістю та виконанням установлених правил.

До числа розглянутих підсистем організаційного плану по захисту інформації можна віднести наступні заходи:

- ознайомлення з співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил захисту інформації та ін.;
- організація надійної охорони приміщень і території проходження лінії зв'язку;
- організація, зберігання і використання документів та носіїв конфіденційної інформації, включаючи порядок обліку, видачі, виконання і повернення;
- створення штатних організаційних структур по захисту цінної інформації або призначення відповідального за захист інформації на конкретних етапах обробки і передачі;
- створення особливого порядку взаємовідносин зі сторонніми організаціями та партнерами;
- організація секретного і КТ-діловодства.

На всіх стадіях інформаційного процесу провідна роль належить людині - носію, користувачеві інформації і знання. Від того, як будуть враховані в інформаційних процесах інтереси, психологічні установки, властивості особистості, залежить ефективність використання інформації. Такий

компонент, як розмежування доступу до інформації, задається одним з важливих елементів системи комплексного захисту інформації. В основі її побудови лежить положення про те, що кожен з членів трудового колективу повинен володіти тільки тими відомостями, які необхідні йому в силу виконуваних обов'язків. У цьому випадку тільки керівник має доступ до всіх матеріалів, незалежно від їх важливості.

Якісна розробка та суворе дотримання зазначених правил - досить дієва міра, спрямована на те, щоб привести до мінімуму ризик втрати найбільш важливої інформації і визначити обсяг викрадених відомостей.

Розробка правил передбачає знайти відповідь на питання:

- кому і в якому випадку може бути дано дозвіл на допуск інформації;
- хто з керівників має право давати дозвіл на доступ і до яких відомостей.

При деталізації зазначених правил передбачається виокремлення таких основних позицій:

- права, обов'язки та відповідальність співробітників і керівників по доступу та види дозволів на доступ до конкретної інформації, зберігання, обробки і передачі по мережі;
- порядок доступу до відомостей, що становлять таємницю представників замовника;
- порядок доступу до цих відомостей представників державних структур;
- розсилка носіїв інформації в інші точки і обмін ними між підрозділами організацій.

Виходячи з усього вищесказаного, приходимо до висновку, що необхідне розмежування прав доступу різних осіб до інформації на різних етапах її обробки і передачі. Елемент організаційного захисту є стержнем, основною частиною розглянутої комплексної системи. Заходи щодо організаційної захисту інформації становлять 50-60 % у структурі більшості систем захисту інформації. Це пов'язано з тим, що важливою складовою частиною організації захисту інформації є підбір, розстановка і навчання персоналу, який буде реалізовувати на практиці систему захисту інформації. Організаційні заходи захисту відображаються в нормативно-методичних документах служби безпеки, служби конфіденційної документації установи або фірми.

## ТЕМА 9:

## «Організація роботи відділу (департаменту) інформаційної безпеки організації»

## ПЛАН

9.1. Департамент інформаційної безпеки: завдання, функції, особливості функціонування

9.2. Організаційна структура і персонал департаменту інформаційної безпеки

9.3. Робота з персоналом підприємства

### Література:

1. Інформаційна безпека. Організаційні заходи по забезпеченню безпеки. Розподіл відповідальності. [Електронний ресурс]. – Джерело доступу: usufit.org.ua/teaching/MSZBP/DownloadHandler.ashx?pg

2. Менеджмент в сфере информационной безопасности [Електронний ресурс]. – Джерело доступу: http://www.intuit.ru/department/itmngt/manofis/1/

3. Кавун С.В. Информационная безопасность в бизнесе. Научное издание. – Харьков: Изд. ХНЭУ, 2007. – 408 с.

### 9.1. Департамент інформаційної безпеки: завдання, функції, особливості функціонування

Департамент інформаційної безпеки (далі - департамент) підприємства являє собою самостійний структурний підрозділ підприємства, безпосередньо виконує ключові функції захисту інформаційних ресурсів.

Його основними *завданнями*, як правило, є:

• організація та координація робіт із забезпечення комплексного захисту інформації на підприємстві;

• контроль за виконанням встановлених вимог та оцінка ефективності роботи підрозділів і персоналу підприємства щодо забезпечення інформаційної безпеки;

• виконання окремих адміністративних і технічних функцій щодо забезпечення інформаційної безпеки, у т.ч.:

• формування, підтримка та документальне забезпечення політики інформаційної безпеки на всіх рівнях;

• впровадження різних засобів захисту інформації;

• адміністрування окремих інформаційних систем.

*Склад завдань департаменту* і його внутрішня організаційна структура в кожному конкретному випадку визначається такими особливостями функціонування підприємства, як:

• значимість інформаційних ресурсів у роботі підприємства і характер існуючих загроз;

• ставлення керівництва і власників підприємства до питань інформаційної безпеки та їх управлінська кваліфікація;

• функціональність і характер використовуваних інформаційних систем, їх роль у бізнес - процесах;

• організація роботи та структура IT -служби;

• фінансовий стан підприємства.

Таким чином, рішення про склад і структуру департаменту в кожному випадку має бути індивідуальним і враховувати всі основні умови.

Функції, пов'язані з формуванням, підтримкою і документальним забезпеченням політики інформаційної безпеки підприємства, можуть включати в себе:

• консультування керівників і власників підприємства з питань розробки та вдосконалення політики інформаційної безпеки;

• самостійна розробка політики безпеки, її узгодження і подання її керівництву підприємства для затвердження, а також внесення необхідних змін у міру зміни умов роботи підприємства;

• самостійна розробка політик безпеки, які стосуються окремих питань захисту інформації (правил застосування телекомунікаційних технологій, вимог, обов'язкових для всіх використовуваних на підприємстві персональних комп'ютерів тощо);

• формування вимог і регламенту процедур перегляду політики безпеки, окремих правил, типових форм та інших документів;

• аналіз окремих договорів і угод зі сторонніми організаціями (постачальниками, покупцями, партнерами з проведення НДДКР тощо) на предмет відповідності вимогам політики інформаційної безпеки;

• аналіз і узагальнення передового досвіду і сучасних теорій у сфері управління інформаційною безпекою з метою їх практичного застосування на підприємстві;

• залучення сторонніх фахівців, дослідників, консультантів (консалтингових компаній) для розробки та вдосконалення політики безпеки підприємства та впровадження розвинених методів управління в цій сфері;

• управління навчанням персоналу компанії (контроль за повнотою і правильністю матеріалів навчальних програм, пов'язаних з інформаційною безпекою, забезпечення своєчасності проходження навчання тощо);

• консультування фахівців та керівників підрозділів підприємства з питань відповідності розроблюваних внутрішніх документів окремих підрозділів вимогам політики безпеки підприємства;

• контроль відповідності внутрішніх організаційних документів підприємства (правил внутрішнього розпорядку, посадових інструкцій, інструкцій з використання інформаційних систем, типових форм договорів тощо) вимогам політики інформаційної безпеки, а також узгодження таких документів при їх затвердженні.

*Функції, пов'язані з впровадженням засобів захисту інформації можуть включати в себе:*

• аналіз сучасних програмних і апаратних засобів захисту інформації та пов'язаних з ними методик захисту, а також ринку доступних засобів захисту інформації, застосовуваних для різних цілей, і підготовка обгрунтованих пропозицій щодо придбання певних продуктів у певних постачальників;

• аналіз закуповуваних інформаційних систем (операційних систем, прикладних програм, телекомунікаційного обладнання, обчислювальної техніки тощо) на предмет їхньої потенційної надійності та наявності вразливостей;

• залучення сторонніх експертів і консультантів для аналізу закуповуваних і використовуваних засобів захисту інформації з точки зору їх надійності, а також з точки зору доцільності їх застосування (впровадження);

• формулювання вимог (пов'язаних із забезпеченням інформаційної безпеки) до самостійно розробляються програмним продуктам або програмному забезпеченню, створюваному на замовлення сторонніми розробниками;

• участь у проектуванні нових інформаційних систем, а також тестуванні знову розроблених і впроваджуваних програмних продуктів;

• розробку техніко - економічного обгрунтування для проектів впровадження засобів захисту інформації, а також залучення для цих цілей сторонніх аналітиків і консультантів, що спеціалізуються на питаннях аналізу засобів захисту інформації;

• підготовку обгрунтованих рішень про вибір між самостійною розробкою засобів захисту інформації (наприклад, програмних модулів, що здійснюють шифрування даних) і передачею їх розробки стороннім компаніям.

*Функції, пов'язані з адмініструванням інформаційних систем і систем захисту інформації можуть включати в себе:*

• виконання деяких функцій з адміністрування окремих інформаційних систем (баз даних, систем колективної роботи з документами, поштових систем тощо), а також адміністрування та конфігурування систем захисту інформації (міжмережевих екранів, систем виявлення вторгнень і т.п.);

• визначення необхідних типових налаштувань та конфігурації робочих станцій (персональних комп'ютерів), що мають відношення до інформаційних систем підприємства (зокрема, підключених до його локальної мережі);

• залучення сторонніх організацій для здійснення поточного адміністрування інформаційних систем і систем захисту інформації, а також для консультаційної та технічної підтримки при виникненні інцидентів, пов'язаних з інформаційною безпекою (зокрема, при здійсненні нападів на інформаційні системи підприємства);

• установку (в тому числі і спільно з фахівцями IT -підрозділу) програмних і апаратних засобів захисту інформації на робочі місця користувачів і в інші елементи інформаційних систем;

• консультування користувачів з виникаючих питань, пов'язаним з інформаційною безпекою, і оперативне вирішення виникаючих у них проблем;

• реагування на різні інциденти, пов'язані з порушенням інформаційної безпеки;

• прийняття активних зустрічних заходів при виявленні вторгнень в інформаційну систему (інформування правоохоронних органів, самостійний пошук нападників і т.п.);

• генерування паролів користувачів інформаційних систем та забезпечення їх збереження;

• участь у відновленні працездатності інформаційних систем після збоїв і порушень в роботі.

*Функції, пов'язані з контролем виконання вимог політики інформаційної безпеки та проведенням аудитів можуть включати в себе:*

• збір та аналіз відомостей про порушення різних вимог політики безпеки, що надходять з різних джерел (у тому числі і від адміністраторів інформаційних систем) та визначення пріоритетних напрямків контрольної роботи;

• перевірку організаційної документації окремих підрозділів підприємства на предмет відповідності вимогам політики інформаційної безпеки (у тому числі і своєчасності внесення всіх необхідних змін в чинні внутрішні організаційні документи);

• перевірку стану (правильності ведення) поточної господарської та кадрової документації окремих підрозділів підприємства, пов'язаної із забезпеченням інформаційної безпеки (правильності і своєчасності заповнення журналів, своєчасність оформлення зобов'язань про нерозголошення відомостей співробітниками тощо);

• проведення комплексних аудитів інформаційної безпеки на підприємстві;

• організацію контрольних перевірок захищеності окремих елементів інформаційних систем (серверів, сегментів мережі тощо);

• залучення сторонніх організацій для проведення аудитів інформаційної безпеки на підприємстві, перевірок надійності інформаційних систем.

Крім перерахованих функцій, безпосередньо пов'язаних із захистом інформаційних ресурсів, також велике значення має виконання функцій, пов'язаних з охороною майна підприємства і вирішенням завдань, які пов'язані з забезпеченням безпеки підприємства у більш широкому сенсі. Зокрема, *для забезпечення інформаційної безпеки має значення виконання таких функцій, як:*

• охорона території та майна підприємства, а також охорона персоналу;

• забезпечення дотримання пропускного режиму;

• спостереження за територією і приміщеннями (у тому числі за допомогою відеокамер);

• контроль за ввезенням на територію підприємства і вивезенням готової продукції, матеріалів, документів та іншого майна;

• організація внутрішніх службових перевірок та розслідувань, а також взаємодії з правоохоронними органами;

• контроль за дотриманням тимчасового режиму роботи, а також за дотриманням правил внутрішнього розпорядку.

## 9.2. Організаційна структура і персонал департаменту інформаційної безпеки

На практиці департамент є підрозділом, або безпосередньо підпорядковується першій особі підприємства, або входять як структурна одиниця в службу безпеки підприємства. Співробітники департаменту знаходяться в адміністративному та функціональному підпорядкуванні у керівника департаменту (рис. 1), який несе відповідальність за забезпечення інформаційної безпеки на підприємстві. Висновок департаментів інформаційної безпеки зі структури IT-служб на підприємствах є однією з важливих сучасних тенденцій в управлінні бізнесом, інформаційними технологіями та інформаційною безпекою, тому що, на думку деяких фахівців, у цих підрозділів є деякі частково взаємопротилежні інтереси і тому деякі завдання не можуть бути ефективно вирішені в рамках одного структурного підрозділу.

У складі департаменту для підвищення ефективності роботи можуть бути виділені самостійні групи (відділи), що спеціалізуються на виконанні певних функцій (рис. 1) :

- відділ (група, бюро) нормативної (організаційної) документації;
- відділ (група, бюро) адміністрування інформаційних систем;
- відділ (група, бюро) аудиту інформаційної безпеки;
- відділ (група, бюро) впровадження інформаційних систем і систем захисту інформації.

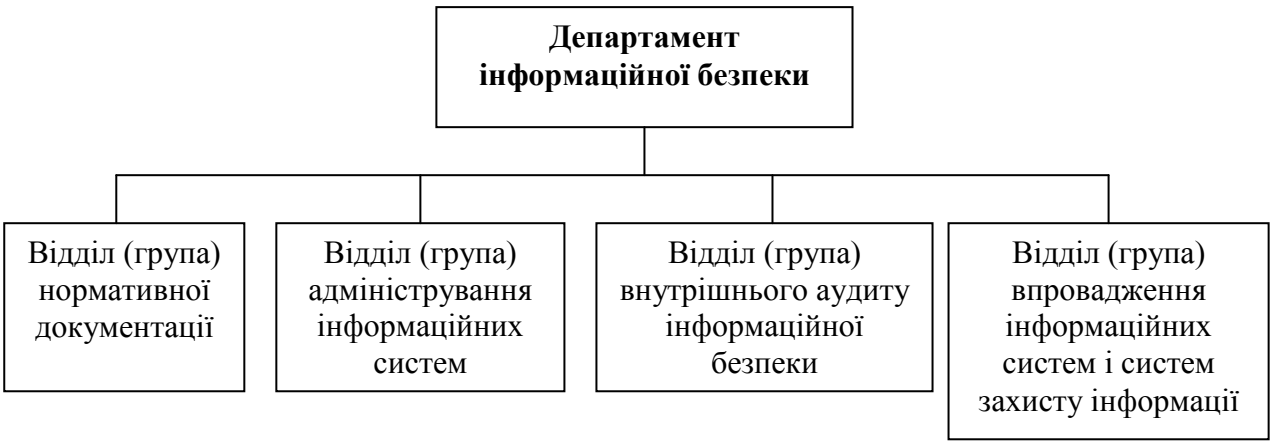


Рис. 1. Приклад організаційної схеми департаменту інформаційної безпеки підприємства

Відділ нормативної документації вирішує завдання, пов'язані з формуванням, підтримкою і документальним забезпеченням політики інформаційної безпеки підприємства, і повинен включати в себе фахівців з менеджменту та бізнес-аналізу, що пройшли додаткову підготовку у сфері управління інформаційною безпекою. Також до складу такого відділу можуть входити юристи. Аналогічний кадровий склад може бути і у Відділу внутрішнього аудиту інформаційної безпеки. При цьому до кваліфікації

співробітників Відділу нормативної документації, як правило, повинні пред'являтися набагато вищі професійні вимоги.

Відділ адміністрування інформаційних систем, а також Відділ впровадження інформаційних систем і систем захисту інформації, як правило, повинні включати в себе фахівців з інформаційних технологій та засобів захисту інформації, які мають значний досвід впровадження та експлуатації корпоративних інформаційних систем.

### 9.3. Робота з персоналом підприємства

Практична реалізація всіх положень сформованої політики інформаційної безпеки вимагає від підприємства тривалих практичних зусиль. Одним з основних і найбільш складних напрямків роботи є робота з персоналом, цілі якої:

• відбір і попередня перевірка персоналу, прийнятого на роботу (на службу);

• навчання співробітників;

• досягнення взаєморозуміння керівників і співробітників в питаннях забезпечення інформаційної безпеки;

• психологічна підготовка з метою протистояння методам т.зв. "соціальної інженерії".

В одній зі своїх книг відомий фахівець з проблем інформаційної безпеки Брюс Шнайер зауважив, що в загальній системі заходів щодо захисту інформації "математичний апарат є бездоганним, комп'ютери ж уразливі, мережі взагалі паршиві, а люди просто огидні. Я вивчив безліч питань, пов'язаних із забезпеченням безпеки комп'ютерів і мереж, і можу стверджувати, що не існує рішення проблеми людського фактора". Це висловлювання найбільш яскраво і наочно демонструє важливість цілеспрямованих заходів щодо добору, розстановки та роботи з кадрами підприємства з тією метою, щоб у роботі інформаційних систем не виникло " вузьких місць" і т.зв. людський фактор не став найбільш вагомим джерелом загроз для інформаційної безпеки. Основною причиною, визначальною значущість людського фактора в загальній системі захисту інформації, є те, що при всій розвиненості сучасних засобів автоматизації інформаційні системи як і раніше представляють собою людино-машинні комплекси та їх (систем) функціонування багато в чому залежить від роботи окремих людей. Саме з цієї причини неадекватне поводження службовців підприємства з компонентами інформаційної системи може завдати серйозної шкоди інформаційної безпеки навіть за наявності детально опрацьованих політик безпеки і високоефективних програмних і апаратних засобів захисту інформації.

Початкова стадія роботи - підбір і розстановка кадрів - може мати кілька аспектів. У першу чергу, основним критерієм для призначення на певні посади, пов'язані з роботою з відомостями, що становлять державну таємницю, є отримання відповідної форми допуску (ця процедура описана в попередньому підрозділі). Відповідно до вимог чинних нормативно-правових актів Перелік

посад, при призначенні на які необхідно оформляти спеціальний допуск, встановлюється керівником підприємства і може періодично переглядатися (для відомостей, що становлять державну таємницю, - не рідше одного разу на 5 років). Ця вимога пов'язана, з одного боку, з тим, що керівник підприємства несе відповідальність за забезпечення режиму секретності, а з іншого - з тим, що для виконання функціональних обов'язків співробітникам підприємства необхідно працювати з певними відомостями і, відповідно, мати певний рівень допуску.

Також при підборі і розстановці кадрів можуть застосовуватися і менш формалізовані методи. Це можуть бути різні методики психологічної оцінки, що включають в себе:

• аналіз мотиваційних аспектів особистості;

• оцінку психологічної стійкості особистості;

• оцінку рівня пізнавальних здібностей особистості (успішність придбання нових знань і навичок і здатність до їх практичного застосування);

• оцінку активності особистості в досягненні поставленої мети, уміння об'єктивно оцінювати ситуацію і людей, вміння виробляти оптимальну стратегію поведінки.

Такого роду аналіз може бути необхідний як щодо фахівців і керівників, які працюють з інформацією, що підлягає захисту, у зв'язку з виконанням своїх посадових обов'язків за основним профілем роботи підприємства, так і спеціалістів та керівників, чиїм основним завданням є забезпечення інформаційної безпеки підприємства (аудиторів ІБ, проектувальників і адміністраторів інформаційних систем і систем захисту інформації тощо).

Крім ретельного підбору, однією з важливих основ роботи з персоналом є його навчання способам забезпечення інформаційної безпеки і безпечній роботі з інформаційними системами. Навчання і наступний контроль отриманих (наявних) знань може бути як первинним, так і повторним. У загальному випадку співробітник підприємства не може бути допущений до виконання своїх посадових обов'язків і роботі з інформаційними системами доти, поки він не пройде навчання з питань інформаційної безпеки та не буде:

• детально ознайомлений з усіма діючими на підприємстві вимогами і загальними правилами;

• повністю навчений методам і прийомам забезпечення інформаційної безпеки, необхідним для виконання його посадових обов'язків;

• ознайомлений з усіма можливими заходами відповідальності (дисциплінарної, адміністративної, кримінальної), які можуть бути до нього застосовані в разі порушення вимог, а також у випадку нанесення шкоди з його вини.

На завершення всієї попередньої роботи співробітник повинен дати всі необхідні зобов'язання про нерозголошення конфіденційних відомостей, а також письмово засвідчити, що він повністю ознайомлений з основними положеннями політики безпеки. У процесі роботи підприємство також може проводити періодичний контроль знань і навичок, пов'язаних із забезпеченням інформаційної безпеки з тією метою, щоб засвідчити компетентність

працівників у цій сфері. Також одним з інструментів навчання може бути періодичне ознайомлення персоналу з реальними прикладами, що недавно відбулися, а також з інцидентами, пов'язаними з інформаційною безпекою. Крім того, додаткове навчання персоналу підприємства може проводитися у випадках:

• впровадження нових автоматизованих інформаційних систем;

• зміни безнес - процесів підприємства;

• зміни вимог політик безпеки (наприклад, у зв'язку зі зміною вимог законодавства).

Необхідність додаткового навчання при впровадженні нових інформаційних систем і, зокрема, інтегрованих систем управління підприємством, як правило, може бути обумовлена появою нових функціональних можливостей програмного забезпечення і зміною процедур обробки інформації. Також доступ до інтегрованих інформаційних систем потенційно може дати доступ до раніше недоступної інформації та надати раніше були відсутні можливості впливати на різні інформаційні потоки. У зв'язку з цим може виникнути потреба в тому, щоб співробітники дали додаткові зобов'язання про дотримання заходів інформаційної безпеки. Аналогічні організаційні заходи щодо забезпечення захисту інформації можуть бути необхідні і при зміні бізнес-процесів підприємства, коли змінюється його структура, розподіл функцій між підрозділами і обов'язків співробітників, і відповідно, вносяться зміни в організаційні схеми, штатні розписи і посадові інструкції персоналу. Зміни вимог політики безпеки можуть бути пов'язані з появою нових загроз, зміною законодавчих вимог, розширенням ринків, зміною ставлення керівництва і власників підприємства до питань інформаційної безпеки та іншими факторами, – всі ці уточнення і зміни також повинні своєчасно і в повному обсязі доводитися до персоналу.

У процесі навчання певну значимість може мати роз'яснення раціональних причин, за якими підприємство застосовує саме таку політику безпеки. Це може служити як для кращого розуміння та засвоєння положень політики безпеки, так і для певної розрядки психологічної напруженості, неминуче виникає при прийнятті обмежувальних заходів та покладанні додаткових обов'язків, необхідність яких не завжди очевидна і зрозуміла як рядовим співробітникам, так і фахівцям.

Окремим напрямом навчання та підвищення кваліфікації може бути розвиток у персоналу компанії навичок протидії методам т.зв. соціальної інженерії (даний підхід також іноді називають "соціотехніки"). Використання для незаконного проникнення в інформаційні системи методів соціальної інженерії пов'язано з т.зв. "людським фактором", який являє собою сукупність певних психологічних схильностей та особливостей мислення і поведінки, які властиві практично всім людям. До числа таких схильностей та особливостей можна віднести:

• нездатність адекватно оцінити небезпеку в деяких ситуаціях;

• специфічне ставлення до рідко відбувається подій (притуплення уваги);

• надмірна довіра засобам автоматизації;

• схильність маніпулюванню, заснована, наприклад, на бажанні допомогти людям (у тому числі і незнайомим) або на зайвому довірі людям, одягненим у спеціальну уніформу, і т.п.

Саме з використанням деяких психологічних особливостей такого роду здійснюються багато найбільш успішних (для нападників) проникнень в корпоративні інформаційні системи. Прикладами таких проникнень є ситуації, коли зловмисник:

• здійснює телефонний дзвінок, представляється адміністратором і, пославшись на певні обставини (такі як збій в системі), просить повідомити йому пароль;

• приходить в офіс у спеціальній уніформі (наприклад, у формі співробітника компанії, що займається обслуговуванням і ремонтом комп'ютерів) і просить надати йому доступ до інформаційної системи;

• надсилає повідомлення електронною поштою від імені адміністратора інформаційної системи або керівництва підприємства і просить повідомити пароль або вчинити певні дії.

Велику значимість у системі заходів з подолання впливу людського фактору має повсякденна робота з персоналом. Крім навчання персоналу та застосування дисциплінарних заходів впливу, одним з основних завдань такої роботи є постійне нагадування всім співробітникам про необхідність дотримання правил інформаційної безпеки. Конкретні способи, за допомогою яких такі нагадування можуть бути зроблені, будуть залежати від уподобань керівників підприємства, сформованої корпоративної культури, специфіки бізнес-процесів та інших обставин. Характерними способами того, як підприємство може постійно нагадувати своїм співробітникам про необхідність дотримуватися обережності, є:

• розміщення і періодична зміна (оновлення дизайну і змісту) нагадувань про необхідність дотримуватися вимог політики інформаційної безпеки на предметах, які постійно перебувають у полі зору співробітників протягом робочого дня: настінних і настільних календарях, кавових гуртках, обкладинках блокнотів, настільних експонатах, ручках, олівцях та інших канцелярському приладді;

• періодична розсилка відповідних брошур, бюлетенів та буклетів, а також повідомлень електронною поштою;

• використання скрінсейвер, містять відповідні нагадування;

• використання голосової пошти і гучного зв'язку для періодичної передачі повідомлень про необхідність дотримання правил інформаційної безпеки тощо.

Таким чином, комплекс всіх організаційних заходів по роботі з персоналом підприємства, що включає в себе систему навчання персоналу, систему залучення порушників до відповідальності, і постійне підтримання атмосфери відповідального ставлення до питань безпеки, повинен у певній мірі зменшити негативний вплив людського фактора на захищеність інформаційних систем і стан інформаційної безпеки.

## ТЕМА 10:

## «Заходи реагування на інциденти»

## ПЛАН

10.1. Фактори виникнення надзвичайних ситуацій (інцидентів), структура процедур реагування на надзвичайні ситуації

10.2. Виявлення атак і розпізнавання вторгнень

10.3. Локалізація та усунення наслідків

10.4. Оцінка та аналіз процесу нападу і його обставин

### Література:

1. «Інформаційна безпека. Організаційні заходи по забезпеченню безпеки. Розподіл відповідальності». [Електронний ресурс]. – Джерело доступу: usufit.org.ua/teaching/MSZBP/DownloadHandler.ashx?pg

2. Менеджмент в сфере информационной безопасности [Електронний ресурс]. – Джерело доступу: http://www.intuit.ru/department/itmngt/manofis/1/

3. Кавун С. В. Информационная безопасность в бизнесе. Научное издание. – Харьков: Изд. ХНЭУ, 2007. – 408 с.

### 10.1. Фактори виникнення надзвичайних ситуацій (інцидентів), структура процедур реагування на надзвичайні ситуації

Реагування на виникаючі надзвичайні ситуації (інциденти), пов'язані з порушенням інформаційної безпеки, є таким же важливим напрямком роботи, як і побудова системи захисту та запобігання порушень. Під *інцидентом*, як правило, розуміється будь-яке відхилення від нормального процесу використання інформаційних ресурсів та функціонування інформаційних систем, що спричинило збитки для певних інформаційних активів підприємства або безпосередньо створює загрозу нанесення такої шкоди.

Надзвичайна ситуація (інцидент), пов'язана з порушенням інформаційної безпеки, може бути обумовлена:

• руйнівним впливом на весь майновий комплекс підприємства при виникненні стихійних факторів (повінь, пожежа, землетрус тощо) або цілеспрямованому нападу (підрив, підпал, руйнування будинків і приміщень тощо);

• негативним впливом виключно на інформаційні ресурси підприємства (як правило, здійснюваним віддалено, з використанням телекомунікаційних каналів).

У загальному випадку організаційні процедури (регламенти) реагування на надзвичайні ситуації повинні включати в себе:

• регламенти альтернативних процесів обробки інформації (у тому числі, можливо, і без використання засобів автоматизації) на період виходу з ладу основних інформаційних ресурсів;

• визначення груп персоналу, відповідальних за виконання тих чи інших функцій у разі виникнення надзвичайної ситуації, а також визначення процедур взаємодії між групами та окремих груп з керівництвом підприємства;

• технічну та організаційну документацію, необхідну для відновлення інформаційних систем і даних після надзвичайної ситуації;

• порядок зберігання архівних (резервних) копій даних і програмних додатків обробки даних в місцях, захищених від механічних впливів, крадіжок, повеней, пожеж тощо (в т.ч., можливо, в місцях, територіально віддалених від основних місць зберігання та обробки інформації);

• угоди з постачальниками програмних і апаратних засобів, що входять в інформаційну інфраструктуру підприємства, про термінову поставку компонентів, що вийшли з ладу і потребують заміни в разі надзвичайної ситуації.

### 10.2. Виявлення атак і розпізнавання вторгнень

Процес реагування на інциденти включає в себе чотири основних етапи:

1. виявлення нападу;
2. локалізація нападу;
3. ідентифікація нападників;
4. оцінка і подальший аналіз процесу нападу і його обставин.

Виявлення атак і розпізнавання вторгнень, як правило, є інженерно-технічним завданням, розв'язуваним за допомогою спеціальних програмних та іноді апаратних засобів. Зокрема, виявлення може здійснюватися на основі аналізу мережевого трафіку і журналів (лог-файлів), в яких фіксуються різні дії. Виявлення може здійснюватися на основі т.зв. сигнатур-формалізованих наборів ознак певних вірусів, типів атак і т.п. Також, очевидно, джерелом інформації про порушення є повідомлення користувачів про відхилення в роботі інформаційних систем і поява явних негативних наслідків які виникли під час порушень.

Для забезпечення своєчасного виявлення порушень підприємство повинно організувати постійну (при необхідності - цілодобову) роботу фахівців, що відповідають за дозвіл інцидентів. Для цього може бути вибраний один з можливих підходів:

• організація власної чергової служби, що складається з компетентних фахівців, несучих позмінне чергування і оснащених засобами мобільного зв'язку;

• залучення сторонньої організації, що спеціалізується на наданні подібних послуг.

При цьому співробітники підприємства повинні знати номери телефонів та інші способи зв'язку, за допомогою яких вони могли б оперативно повідомляти черговим фахівцям про всі події. Важливість організації якомога більш оперативного інформування фахівців з безпеки і, відповідно, якомога більш оперативного реагування обумовлена тим, що виявлення нападу і початок

протидії в той час, як саме напад ще триває, в більшості випадків може бути набагато більш ефективним, ніж реагування після закінчення нападу.

Виявлення порушень може бути здійснено не тільки по явним ознаками, таким як повідомлення користувачів про припинення функціонування окремих елементів інформаційних систем, одночасне використання одного облікового запису на декількох робочих станціях або явне виявлення вірусів в даних, переданих по локальній мережі, але і за деякими непрямими ознаками (аномальним явищам), які в окремих випадках можуть свідчити (а можуть і не свідчити) про порушення. Прикладами таких непрямих свідчень можуть бути:

• використання інформаційних систем і певних облікових записів у нехарактерний час (рано вранці, пізно ввечері і т.п.);

• різке нехарактерне підвищення навантаження на інформаційні системи або їх окремі елементи (сегменти мережі, сховища даних тощо);

• зміна характеру поведінки користувачів (наприклад, послідовності певних дій при використанні інформаційної системи);

• та інші.

Для більш ефективного аналізу таких непрямих ознак і інтерпретації різних фактів фахівцям з реагування на інциденти може знадобитися аналіз функціональності інформаційних систем і взаємодія аналітиків департаменту інформаційної безпеки з користувачами (вивчення особливостей їх роботи). Також для автоматизації такого аналізу можуть бути використані спеціальні програмні засоби, які автоматично здійснюють статистичний аналіз мережевого трафіку та інших елементів інформаційної інфраструктури та сигналізують при виявленні аномальної активності, для того щоб адміністратори могли провести подальший якісний аналіз виявлених відхилень і при необхідності зробити активні дії у відповідь. У цілому, розробка і вдосконалення таких засобів аналізу в складі комплексних систем виявлення вторгнень є одним з перспективних напрямків розвитку засобів захисту інформації.

Таким чином, основним завданням на початковому етапі реагування є визначення характеру порушень і достовірне встановлення того, що виявлені аномальні події, дії і характеристики є дійсно порушеннями, а, наприклад, не проявом особливостей роботи програмного забезпечення.

Одним з найважливіших організаційних аспектів реагування на інциденти (і, зокрема, на окремі сигнали про деякі пригоди) є та обставина, що може відбуватися більш -менш часте надходження хибних сигналів (помилкових або спеціально спровокованих) про деякі пригоди, і реакція персоналу департаменту інформаційної безпеки з часом може поступово слабшати (так само як, наприклад, може притупитися увага при частих помилкових спрацьовуваннях охоронної сигналізації). Зокрема, за оцінкою деяких фахівців, в середньому в 90 % випадків, коли користувачі повідомляють про те, що, на їх думку, комп'ютер заражений вірусом, вони помиляються. У зв'язку з цим при організації реагування на інциденти необхідно приділити особливу увагу психологічній підготовці персоналу, що відповідає за реагування, а також по можливості аналізувати причини появи таких помилкових сигналів і запобігати їх надалі.

Також значущим питанням організації роботи з користувачами в ситуаціях реагування на інциденти є те, що взаємодія між користувачами і групами реагування, а також різних груп реагування між собою по можливості необхідно здійснювати за спеціальними захищеними каналами зв'язку.

### 10.3. Локалізація та усунення наслідків

Локалізація та усунення наслідків є основним етапом, в рамках якого, власне, здійснюється реагування на інцидент. На цьому етапі відбувається:

• визначення конкретних параметрів порушення (нападу), його характеру (конкретних сегментів мережі, серверів, груп робочих станцій, додатків, порушених нападом);

• попередній аналіз дій порушника і сценарію нападу що стався (що відбувається), алгоритму роботи при появі вірусу тощо;

• блокування дій порушника (якщо порушення є тривалим);

• блокування (повне або часткове) роботи інформаційної системи (сервера, бази даних, сегмента мережі тощо) з метою недопущення подальших руйнівних дій, поширення шкідливих програм або витоку конфіденційної інформації.

Припинення нападу і відновлення нормальної роботи інформаційних систем може зажадати скоординованих дій не тільки самих співробітників департаменту інформаційної безпеки, але й:

• фахівців IT-підрозділів, що відповідають за яких умов атакували інформаційні сервіси;

• користувачів атакованих інформаційних систем;

• підприємств-партнерів, що мають відношення до атакованих інформаційних ресурсів;

• розробників і постачальників атакованих інформаційних систем;

• постачальників телекомунікаційних послуг, через які здійснюється атака;

• сторонніх консультантів, що спеціалізуються на відповідних проблемах інформаційної безпеки.

Одним з найбільш важливих обставин роботи на даному етапі є те, якими повноваженнями володіє спеціаліст (черговий), що відповідає за реагування на інциденти. Зокрема, необхідно заздалегідь передбачити можливість оперативного самостійного відключення тих чи інших інформаційних сервісів фахівцями з реагування на інциденти (самостійно, або через відповідний IT - підрозділ). Особливо важливою є здатність відповідальних фахівців оперативно оцінити ситуацію, провести її аналіз (у більшості практичних ситуацій це необхідно буде робити за неповними даними про нападаючу сторону) і прийняти рішення про призупинення роботи тих чи інших інформаційних сервісів, до виявлення і усунення загроз і / або введення в дію додаткових коштів протидії вторгненням. При прийнятті такого рішення необхідно враховувати (як правило, на основі експертних оцінок) як можливий збиток, який може бути викликаний виявленим порушенням, так і можливий збиток від зупинки інформаційних сервісів, зупинка (зупинення) може бути здійснена з метою запобігання збитку від дій нападаючої сторони. Характерним прикладом

такої ситуації є напад на систему електронної торгівлі, коли нападаюча сторона може завдати серйозної шкоди (викрасти конфіденційну інформацію учасників торгових угод, самостійно вчинити незаконні угоди від імені учасників торгової системи і т.п.), а зупинка сервісу з метою запобігання такої шкоди може призвести до втрат, пов'язаних з упущеною вигодою від недосконалих угод та шкодою для ділової репутації. Іншим прикладом такої ситуації є реагування на розподілені атаки типу "відмова в обслуговуванні" (Distributed Deny of Service, DDoS), часто здійснювані на сервери в мережі Інтернет, коли може бути необхідно на деякий час повністю відключити сервер як на шкоду користувачам, так і в збиток власникам інформаційних ресурсів, розташованих на сервері.

Основою для прийняття рішень може бути заздалегідь сформований перелік (довідник) можливих основних інцидентів і ознак порушень (проникнень), в якому може бути наведено оцінку ризиків сумарних втрат і рекомендовані дії для кожного типу порушень (в тому числі і перелік ситуацій, коли необхідно здійснити відключення сервісів щоб уникнути витоку або порушення цілісності інформації, що є найбільш критичною для всієї діяльності підприємства).

Ідентифікація нападника (або джерела розповсюдження шкідливих програм) є важливим кроком у процесі реагування, наступним безпосередньо за локалізацією нападу. У разі якщо напад здійснювався з локальної мережі підприємства, при належному дотриманні внутрішніх режимних правил ця задача може виявитися відносно легкою. У разі якщо напад було скоєно ззовні, задача ідентифікації нападників принципово ускладнюється і в деяких ситуаціях проблема стає практично нерозв'язною.

Як правило, для виявлення джерела нападу необхідно:

• детально вивчити всі технічні аспекти нападу;

• провести якісний аналіз процесу нападу (в контексті функціонування атакується система захисту інформації);

• організувати взаємодію зі сторонніми організаціями, які можуть сприяти в ідентифікації нападника.

Однією з найбільш важливих завдань аналізу процесу нападу є встановлення тієї інформації, яка була відома нападаючим до початку нападу і якою вони скористалися для здійснення цього нападу. Зокрема, в процесі такого аналізу з певним ступенем впевненості можна встановити, що до початку нападу зловмисникам були відомі:

• інформація про структуру і склад атакуючої інформаційної системи (використовувані програмні та апаратні засоби, їх архітектура і використовувані настройки);

• відомості про режим роботи організації та функціонування окремих елементів інформаційної системи.

Відомості про регламент деяких бізнес-процесів підприємства;

• конкретні ідентифікаційні дані (імена користувачів, паролі), необхідні для проникнення в інформаційну систему і/або правила (алгоритми) їх генерації.

Узагальнення всіх цих відомостей може допомогти встановити, які контакти були у нападників (а яких не було), і, зіставляючи факти, а також користуючись методом виключення, постаратися обмежити коло осіб, які потенційно могли бути причетні до організації даного інциденту.

У свою чергу, проведення такого аналізу буде можливо тільки в тому випадку, якщо всі інформаційні системи та системи захисту інформації налаштовані належним чином (зокрема, в них ведуться всі необхідні системні журнали) та системні дані не були пошкоджені в процесі нападу.

Другим важливим напрямком організаційної та аналітичної роботи при встановленні (ідентифікації) нападників, які вчинили напад ззовні, є взаємодія з адміністраторами систем (телекомунікаційних мереж, комп'ютерів, що використовувалися в якості проксі - серверів, і т.п.), з використанням яких було здійснено напад. Підходи до такої взаємодії в кожному конкретному випадку, швидше за все, будуть індивідуальними і можуть залежати від політики розкриття інформації адміністрації тієї мережі або вузла, через який здійснювалася атака. Також можуть бути зроблені дії для того, щоб у судовому порядку або із залученням правоохоронних органів зобов'язати адміністрації таких мереж і вузлів надати необхідну інформацію, пов'язану з подією нападу.

Процес ідентифікації повинен проводитися з урахуванням того, що згодом необхідно буде використовувати інформацію про нападників як доказ у кримінальному процесі. Зокрема, при знятті (копіюванні) необхідних лог-файлів з атакованих комп'ютерів представниками правоохоронних органів, провідними слідство у даній справі, повинні бути дотримані всі процесуальні формальності, передбачені кримінально-процесуальним законодавством. Однією з особливостей процедури вилучення доказів у потерпілої сторони в цьому випадку є те, що поняті, присутні при вилученні, повинні по можливості мати хоча б загальне уявлення про сенс виробленої процедури. Також на цьому етапі при необхідності може бути проведена техніко-криміналістична експертиза комп'ютерних систем.

### 10.4. Оцінка та аналіз процесу нападу і його обставин

Одним із заключних кроків процесу реагування на інцидент є оцінка та аналіз процесу нападу і його обставин. Цей аналіз необхідно проводити в контексті цілей і завдань функціонування всього підприємства, з урахуванням результатів роботи з ідентифікації осіб, які вчинили напад. Основні завдання аналітичної роботи на даному етапі:

• аналіз цілей і мотивів нападників;

• аналіз фундаментальних (організаційних і технічних) причин, які зробили напад можливим і успішним (якщо воно було успішним);

• аналіз наслідків (у тому числі і довгострокових) нападу для всієї діяльності підприємства;

• аналіз і оцінка роботи персоналу та взаємовідносин з підприємствами - партнерами (у тому числі і з постачальниками інформаційних систем і засобів захисту інформації).

Результатом аналізу повинні бути висновки, які можуть послужити основою для організаційної роботи в різних напрямках:

• коригування і уточнення політики інформаційної безпеки підприємства;

• проведення додаткової роботи з персоналом підприємства (покарання, заохочення, додаткове навчання і т.п.);

• проведення додаткової роботи з персоналом департаменту інформаційної безпеки підприємства, а також персоналом IT- служб;

• перегляд взаємовідносин з контрагентами підприємства (покупцями, постачальниками, партнерами по НДДКР і т.п.), що мають доступ до його інформації, що захищається або інформаційних систем;

• залучення сторонніх консультантів з інформаційної безпеки та фахівців по засобах захисту інформації;

• ініціювання технічного переоснащення окремих ділянок інформаційної інфраструктури підприємства.

Таким чином, аналіз і всебічна оцінка інцидентів є відправною точкою для реалізації комплексу заходів щодо вдосконалення системи забезпечення інформаційної безпеки на підприємстві. Всі ці заходи повинні в майбутньому знизити ймовірність аналогічних інцидентів, а також зменшити вірогідність нанесення істотного збитку у разі їх повторення.

Важливою складовою аналізу нападу також є оцінка збитку від події порушення інформаційної безпеки. Збиток може бути оцінений одночасно з декількох точок зору і залежить від характеру виникненя позаштатної ситуації. Найбільш простим для кількісної економічної оцінки є прямий збиток: витрати на відновлення втраченої інформації (можуть бути розраховані на основі трудомісткості робіт з відновлення інформації і даних про середню вартість робочого часу відповідних фахівців), витрати на заміну скомпрометованих паролів, кодів і ключів, вартість пошкодженого обладнання, штрафні санкції за розголошення конфіденційної інформації (якщо такі санкції, наприклад, були передбачені договорами з підрядниками, постачальниками або замовниками) і т.п. Також в оцінці потребується упущена вигода, яка може бути пов'язана як з безпосереднім припиненням (зупиненням, уповільненням) поточних операцій підприємства, так і з довгостроковим (перспективним) негативним впливом виниклої позаштатної ситуації - втратою довіри до підприємства, що приводить до відтоку замовників, формуванням негативного іміджу підприємства і т.п. Окремо також може бути оцінено падіння ринкової вартості підприємства - його акцій (якщо мова йде про підприємство, акції якого котируються на біржовому ринку).

Найбільш складним для оцінки є моральний збиток і наслідки від розголошення інформації особистого характеру (наприклад, відомостей, що становлять лікарську таємницю). Конкретні суми морального збитку, як правило, можуть бути встановлені за результатами судових розглядів з окремими особами, яким такий збиток був нанесений, або процедур досудового врегулювання конфліктів (на основі вимог постраждалих осіб).

Заключним етапом процесу реагування також є усунення негативних наслідків нападу - локалізація збитку, заподіяного порушенням. Ця робота може включати в себе:

• зміну скомпрометованих паролів окремих користувачів;

• перестановку пошкоджених операційних систем, а також пошкодженого програмного забезпечення;

• відновлення порушеної конфігурації (налаштувань) програмного забезпечення та операційних систем;

• відновлення пошкодженої інформації (баз даних, файлів), як з раніше створених резервних копій, так і іншими способами.

У процесі відновлення працездатності інформаційних систем на деякий час можуть бути задіяні резервні (альтернативні) апаратні і програмні платформи.

Крім того, необхідним завершальним кроком може бути додаткова інформаційна робота, яка може в себе включати:

• розсилку користувачам інформації про інциденти що відбулися (у вигляді спеціальних листів та бюлетенів);

• передачу деяких відомостей про напад в засоби масової інформації;

• передачу відомостей про напад великим групам реагування на інциденти, пов'язані з інформаційною безпекою (таким як, наприклад, CERT / CC), а також у науково-дослідні центри, які займаються проблемами захисту інформації;

• додаткову інформаційну роботу з постачальниками інформаційних систем і підрядниками, які здійснювали їх поставку, впровадження та налагодження.

З точки зору розподілу обов'язків з виконання окремих функцій у рамках процесу реагування на інциденти, одним з ефективних і досить широко використовуваних підходів до організації реагування на інциденти є побудова централізованої системи реагування на інциденти, коли одна група реагування обслуговує декілька підрозділів чи підприємств. Зокрема, такий підхід реалізований у Міністерстві оборони США (він був описаний в одній з попередніх лекцій), де кілька централізованих груп реагування на інциденти обслуговують безліч військових підрозділів. Централізовані групи реагування можуть створюватися для обслуговування різних підприємств і організацій. Це можуть бути компанії, що входять у великий холдинг, організації, що входять в одну дослідницьку мережу, університети і дослідницькі організації однієї країни, клієнти постачальника певних продуктів або послуг і т.д. Для об'єднання зусиль різних груп реагування був створений спеціальний Форум груп реагування на інциденти та забезпечення безпеки (Forum of Incident Response and Security Teams, FIRST), на Інтернет сайті якого (http://www.first.org/) можна знайти повний список його учасників.

## ТЕМА 11:

## «Аудит системи інформаційної безпеки підприємства»

## ПЛАН

11.1. Поняття, види та цілі аудиту інформаційної безпеки підприємства
11.2. Процедура проведення аудиту інформаційної безпеки підприємства

### Література:

1. «Інформаційна безпека. Організаційні заходи по забезпеченню безпеки. Розподіл відповідальності». [Електронний ресурс]. – Джерело доступу: usufit.org.ua/teaching/MSZBP/DownloadHandler.ashx?pg
2. Менеджмент в сфере информационной безопасности [Електронний ресурс]. – Джерело доступу: http://www.intuit.ru/department/itmngt/manofis/1/
3. Кавун С. В. Информационная безопасность в бизнесе. Научное издание. – Харьков: Изд. ХНЭУ, 2007. – 408 с.

### 11.1. Поняття, види та цілі аудиту інформаційної безпеки підприємства

Аудит стану інформаційної безпеки на підприємстві являє собою експертне обстеження основних аспектів інформаційної безпеки, їх перевірку на відповідність певним вимогам. У деяких випадках під аудитом інформаційної безпеки мається на увазі перевірка захищеності окремих елементів інформаційної інфраструктури підприємства (сегментів його мережі, окремих серверів, баз даних, Інтернет-сайтів тощо) і надійності засобів захисту інформації (міжмережевих екранів, систем виявлення вторгнень). Однак, ми надалі виходимо з того, що аудит інформаційної безпеки є комплексним (по можливості, вичерпним) дослідженням всіх аспектів інформаційної безпеки (як технічних, так і організаційних) в контексті всієї господарської діяльності підприємства з урахуванням діючої політики інформаційної безпеки, об'єктивних потреб підприємства і вимог, що пред'являються третіми особами (державою, контрагентами тощо).

Розрізняють два основних види аудиту: внутрішній (проводиться виключно силами співробітників підприємства) і зовнішній (здійснюється сторонніми організаціями).

Цілями аудиту можуть бути:

• встановлення ступеня захищеності інформаційних ресурсів підприємства, виявлення недоліків та визначення напрямків подальшого розвитку системи захисту інформації;

• перевірка керівництвом підприємства та іншими зацікавленими особами досягнення поставлених цілей у сфері інформаційної безпеки, виконання вимог політики безпеки;

• контроль ефективності вкладень в придбання засобів захисту інформації та реалізацію заходів щодо забезпечення інформаційної безпеки;

• сертифікація на відповідність загальновизнаним нормам і вимогам у сфері інформаційної безпеки (зокрема, на відповідність національним та міжнародним стандартам).

Одним із стратегічних завдань, що вирішуються при проведенні аудиту інформаційної безпеки та отриманні відповідного сертифіката, є демонстрація надійності підприємства, його здатності виступати в якості сталого партнера, здатного забезпечити комплексний захист інформаційних ресурсів, що може бути особливо важливим при здійсненні операцій, що передбачають обмін конфіденційною інформацією, що має велику вартість (фінансовими відомостями, конструкторсько-технологічною документацією, результатами НДДКР і т.п.).

У тому випадку, якщо аудит є внутрішнім, групу аудиторів необхідно сформувати з числа таких фахівців, які самі не є розробниками і адміністраторами використовуваних інформаційних систем і засобів захисту інформації та не мали відношення до їх впровадження на даному підприємстві.

Як правило, підприємство може вдаватися до допомоги зовнішніх аудиторів з метою:

• підвищення об'єктивності, незалежності та професійного рівня перевірки;

• отримання висновків про стан інформаційної безпеки та відповідно міжнародним стандартам від незалежних аудиторів.

Компанії, що спеціалізуються на проведенні аудитів, можуть здійснювати перевірки стану інформаційної безпеки на відповідність таким загальновизнаним стандартам і вимогам, як:

• ISO 15408: Common Criteria for Information Technology Security Evaluation (Загальні критерії оцінки безпеки інформаційних технологій);

• ISO 17799 (BS 7799): Code of Practice for Information Security Management (Практичні правила управління інформаційною безпекою);

• BSI \ IT: Baseline Protection Manual (Керівництво базового рівня щодо захисту інформаційних технологій Агентства інформаційної безпеки Німеччини);

• COBIT: Control Objectives for Information and related Technology (Основні цілі для інформаційних та пов'язаних з ними технологій);

• Вимогам Керівних документів ФСТЕК РФ, ФСБ чи інших державних органів

• та інших документів (таких як SAC, COSO, SAS 55/ 78).

При цьому організація, що здійснює зовнішній аудит, повинна відповідати певним вимогам:

• мати право (ліцензію) на видачу висновків про відповідність певним вимогам (наприклад, акредитацію UKAS - United Kingdom Accreditation Service);

• співробітники повинні мати право доступу до інформації, що становить державну і військову таємницю (якщо така інформація є на підприємстві, що перевіряється);

• володіти необхідними програмними та апаратними засобами для вичерпної перевірки наявних у підприємства програмного і апаратного забезпечення.

## 11.2. Процедура проведення аудиту інформаційної безпеки підприємства

Основними етапами проведення аудиту є:

• ініціювання проведення аудиту;

• безпосередньо здійснення збору інформації та проведення обстеження аудиторами;

• аналіз зібраних даних і вироблення рекомендацій;

• підготовка аудиторського звіту та атестаційного висновку.

Аудит повинен бути ініційований керівництвом підприємства з досить чітко сформульованою метою на певному етапі розвитку інформаційної системи або системи забезпечення інформаційної безпеки підприємства (наприклад, після завершення одного з етапів впровадження). У разі якщо аудит не є комплексним, на початковому етапі необхідно визначити його безпосередні кордони:

• перелік обстежуваних інформаційних ресурсів та інформаційних систем (підсистем);

• перелік будівель, приміщень і територій, в межах яких буде проводитися аудит;

• основні загрози, засоби захисту від яких необхідно піддати аудиту;

• елементи системи забезпечення інформаційної безпеки, які необхідно включити в процес перевірки (організаційне, правове, програмно - технічне, апаратне забезпечення);

Основна стадія - проведення аудиторського обстеження та збір інформації, як правило, має включати в себе:

• аналіз наявної політики інформаційної безпеки та іншої організаційної документації;

• проведення нарад, опитувань, довірчих бесід і інтерв'ю з співробітниками підприємства;

• перевірку стану фізичної безпеки інформаційної інфраструктури підприємства;

• технічне обстеження інформаційних систем - програмних і апаратних засобів (інструментальна перевірка захищеності).

Перш ніж приступити власне до аудиту інформаційної безпеки, аудиторам (зокрема, якщо проводиться зовнішній аудит) необхідно ознайомитися зі структурою підприємства, його функціями, завданнями та основними бізнес-процесами, а також з наявними інформаційними системами (їх складом, функціональністю, процедурами використання та роллю на підприємстві). На початковому етапі аудитори приймають рішення про те, наскільки глибоко і детально будуть досліджені окремі елементи інформаційної системи та системи захисту інформації. Також необхідно заздалегідь скоординувати з

користувачами інформаційних систем процедури перевірки та тестування, що вимагають обмеження доступу користувачів (такі процедури по можливості повинні проводитися в неробочий час або в періоди найменшого завантаження інформаційної системи).

Якісний аналіз діючої на підприємстві політики безпеки є базою для проведення аудиту. Одне з перших завдань комплексного аудиту – свстановлення того, якою мірою діюча політика відповідає об'єктивним потребам даного підприємства в безпеці, чи можуть дії в рамках даної політики забезпечити необхідний рівень захищеності інформації та засобів її обробки, зберігання та передачі. Це, у свою чергу, може вимагати проведення додаткової оцінки значущості основних інформаційних активів підприємства, їх вразливості, а також існуючих ризиків і загроз. Аналіз політики також може включати оцінку таких її характеристик, як:

• повнота і глибина охоплення всіх питань, а також відповідність змісту політик нижнього рівня цілям і завданням, встановленим в політиках верхнього рівня;

• зрозумілість тексту політики для людей, які не є технічними фахівцями, а також чіткість формулювань і неможливість їх подвійного тлумачення;

• актуальність всіх положень і вимог політики, своєчасність обліку всіх змін, що відбуваються в інформаційних системах і бізнес - процесах.

Після перевірки основних положень політики безпеки в процесі аудиту можуть бути вивчені (впорядковані) діючі класифікації інформаційних ресурсів за ступенем критичності та конфіденційності, а також інші документи, що мають відношення до забезпечення інформаційної безпеки:

• організаційні документи підрозділів підприємства (положення про відділи, посадові інструкції);

• інструкції (положення, методики), що стосуються окремих бізнес - процесів підприємства;

• кадрова документація, зобов'язання про нерозголошення відомостей, дані співробітників, свідоцтва про проходження навчання, професійної сертифікації, атестації та ознайомлення з діючими правилами;

• технічна документація і призначені для користувача інструкції для різних використовуваних програмних і апаратних засобів (як розроблених самим підприємством, так і придбаних у сторонніх постачальників): міжмережевих екранів, маршрутизаторів, операційних систем, антивірусних засобів, систем управління підприємством і т.п.

Основна робота аудиторів у процесі збору інформації полягає у вивченні фактично застосованих заходів щодо забезпечення захисту інформаційних активів підприємства, таких як:

• організація процесу навчання користувачів прийомам і правилам безпечного використання інформаційних систем;

• організація роботи адміністраторів інформаційних і телекомунікаційних систем і систем захисту інформації (правильність використання програмних і апаратних засобів адміністрування, своєчасність створення і видалення облікових записів користувачів, а також налаштування їх прав в інформаційних

системах, своєчасність заміни паролів і забезпечення їх відповідності вимогам безпеки, здійснення резервного копіювання даних, ведення протоколів усіх вироблених у процесі адміністрування операцій, вжиття заходів при виявленні несправностей і т.п.);

• організація процесів підвищення кваліфікації адміністраторів інформаційних систем і систем захисту інформації;

• забезпечення відповідності необхідних (у відповідності з політикою безпеки і посадовими обов'язками) прав користувачів інформаційних систем і фактично наявних;

• організація призначення та використання спеціальних прав в інформаційних системах підприємства;

• організація робіт і координація дій при виявленні порушень інформаційної безпеки та відновленні роботи інформаційних систем після збоїв і нападів (практичне виконання "аварійного плану");

• заходи, що вживаються для антивірусного захисту (належне використання антивірусних програм, облік всіх випадків зараження, організація роботи з усунення наслідків заражень);

• забезпечення безпеки придбаних програмних і апаратних засобів (наявність сертифікатів та гарантійних зобов'язань, підтримка з боку постачальника при усуненні виявлених недоліків тощо);

• забезпечення безпеки самостійно розроблюваного програмного забезпечення (наявність необхідних вимог у проектній документації інформаційних систем, якість програмної реалізації механізмів захисту тощо);

• організація робіт з встановлення та оновлення програмного забезпечення, а також контролю за цілісністю встановленого ПЗ;

• заходи, що вживаються щодо забезпечення обліку і зберігання носіїв інформації (дисків, дискет, магнітних стрічок і т.п.), а також з їх безпечного знищення після закінчення використання;

• ефективність організації взаємодії співробітників підприємства – користувачів інформаційних систем – із службою інформаційної безпеки (зокрема, з питань реагування на інциденти та усунення їх наслідків).

Одним з важливих напрямків аудиторської перевірки є контроль того, наскільки своєчасно і повно положення та вимоги політики безпеки та інших організаційних документів доводяться до персоналу підприємства. У тому числі, необхідно оцінити, наскільки систематично і цілеспрямовано здійснюється навчання персоналу (як при занятті посад, так і в процесі роботи), і, відповідно, дати оцінку тому, якою мірою персонал розуміє всі пропоновані до нього вимоги, усвідомлює свої обов'язки, пов'язані із забезпеченням безпеки, а також можливу відповідальність, яка може настати при порушенні встановлених вимог.

У процес проведення інтерв'ю, нарад і бесід з персоналом необхідно включити якомога більше співробітників підприємства, які мають хоча б якесь відношення до інформаційних систем та процедур обробки інформації: адміністраторів і розробників інформаційних систем, операторів та інших користувачів, допоміжний персонал. При безпосередній роботі з персоналом

аудиторам необхідно з'ясувати особливості протікання окремих бізнес-процесів, ролі окремих співробітників в цих процесах і їх потенційні можливості впливати на інформаційну безпеку. Також необхідно оцінити, якою мірою співробітники фактично виконують свої обов'язки щодо забезпечення інформаційної безпеки.

Одним з важливих завдань аудиту може бути встановлення того, наскільки підприємство здатне протидіяти внутрішнім загрозам в особі співробітників, цілеспрямовано діючих, щоб завдати той чи інший збиток підприємству і мають для цього різні можливості. Зокрема, для цього можуть бути досліджені:

• процедури відбору та прийняття нових працівників на роботу, а також їх попередньої перевірки;

• процедури контролю за діяльністю співробітників (відстеження їх дій);

• процедури реєстрації користувачів і призначення їм прав в інформаційних системах;

• розподіл функцій між різними співробітниками і мінімізація їх привілеїв, а також можливу наявність надлишкових прав у деяких користувачів та адміністраторів.

Перевірка стану фізичної безпеки інформаційної інфраструктури, як правило, включає в себе:

• перевірку того, щоб найбільш важливі об'єкти інформаційної інфраструктури та системи захисту інформації розташовувалися в зонах (частинах будинків, приміщеннях), що мають пропускний режим, а також обладнаних камерами відеоспостереження та іншими засобами контролю (електронними замками, засобами біометричної ідентифікації і т.п.);

• перевірку наявності та працездатності технічних засобів, що забезпечують стійку роботу комп'ютерного та телекомунікаційного обладнання: джерел безперебійного енергопостачання, кондиціонерів (там, де це необхідно) тощо;

• перевірку наявності та працездатності засобів пожежної сигналізації та пожежогасіння;

• перевірку розподілу відповідальності за фізичний (технічний) стан об'єктів інформаційної інфраструктури підприємства.

Інструментальна перевірка захищеності є в основному технічною задачею і здійснюється з використанням спеціалізованого програмного забезпечення, яке підключається до інформаційної системи підприємства і автоматично виробляє збір різних відомостей: версій встановлених операційних систем і програмного забезпечення, даних про використаня мережевих протоколів, номерів відкритих портів, даних про версії встановлених оновлень і т.п. До інших напрямків інструментального та технічного контролю також відносяться такі роботи, як:

• безпосереднє вивчення роботи окремих серверів, робочих станцій і мережевого устаткування відповідними технічними фахівцями, які можуть перевірити різні аспекти їх функціонування (процедури завантаження, виконувані процеси, вміст конфігураційних файлів);

• збір і подальший аналіз даних про те, як виконуються процедури резервного копіювання, а також інші необхідні технічні процедури, передбачені регламентом;

• перевірка якості програмного забезпечення, самостійно розробленого підприємством (у тому числі і шляхом аналізу вихідних кодів і проектної документації до нього), виявлення помилок, які можуть стати причиною збоїв, несанкціонованих проникнень, руйнування і витоку інформації та інших інцидентів;

• вивчення роботи мережі (мережевого трафіку, завантаження різних сегментів мережі тощо);

• проведення з метою тестування пробних, контрольованих "порушень" інформаційної безпеки (по можливості без нанесення реальної шкоди і у позаробочий час), таких як атаки типу "відмова в обслуговуванні" (DoS) або проникнення в певні бази даних і на певні сервери, а також використання різних відомих вразливостей з метою з'ясування конкретних параметрів безпеки, стабільності та надійності перевіреної інформаційної системи.

Також у процесі аудиту може бути перевірено ведення журналів (лог-файлів) інформаційних систем і застосування інших інструментів збору та аналізу інформації, необхідних для забезпечення поточного контролю за дотриманням вимог інформаційної безпеки та своєчасного реагування на інциденти (засобів виявлення вторгнень, аналізаторів роботи локальних мереж тощо).

Інформація, накопичена в лог-файлах за час використання інформаційних систем, є одним з важливих об'єктів аналізу в процесі аудиту. На основі цих даних можуть бути зроблені оцінки і висновки щодо дотримання встановлених правил використання інформаційних систем, ефективності використовуваних засобів захисту інформації, поведінки користувачів, а також про потенційно можливі проблеми.

Аналіз всієї інформації, отриманої в процесі ознайомлення з документацією, контролю фактичного виконання всіх встановлених вимог, отримання відомостей від співробітників, вивчення роботи апаратних засобів і програмного забезпечення, перевірки фізичної захищеності та проведення інструментальних перевірок повинен бути проведений з урахуванням виявлених ризиків та потреб підприємства в інформаційній безпеці. Зокрема, такий аналіз передбачає виявлення конкретних особливостей програмних і апаратних засобів, бізнес-процедур, організаційних правил і розподілів функціональних обов'язків і повноважень, які можуть негативно вплинути на забезпечення інформаційної безпеки, а також опис причинно-наслідкових взаємозв'язків між виявленими особливостями функціонування підприємства і збільшенням ризиків порушення інформаційної безпеки. Всі досліджені обставини, виявлені недоліки та особливості повинні бути узагальнені, і таким чином має бути сформовано загальне уявлення про стан інформаційної безпеки на підприємстві, відображені основні переваги і недоліки діючої системи захисту інформаційних ресурсів, а також позначені основні пріоритети і напрямки її подальшого розвитку та вдосконалення.

Результати аналізу можуть бути представлені як у вигляді узагальнених коротких формулювань, що характеризують захищеність інформації підприємства (адресованих керівництву та власникам підприємства), так і у вигляді переліку конкретних зауважень і пропозицій, що відносяться до окремих ділянок роботи (адресованих керівнику департаменту інформаційної безпеки, керівнику служби безпеки, функціональним директорам і керівникам структурних підрозділів підприємства).

Остаточним результатом аналізу та узагальнення даних, отриманих у процесі аудиту, є звіт (висновок), який може включати в себе:

• оцінку стану (рівня) захищеності інформаційних ресурсів та інформаційних систем;

• висновки про практичні виконання вимог, передбачених політикою інформаційної безпеки підприємства та іншими вимогами та документами;

• висновок про ступінь відповідності фактичного рівня інформаційної безпеки вимогам певних стандартів і нормативних документів;

• пропозиції щодо вдосконалення політики інформаційної безпеки та реалізації додаткових практичних заходів у цій сфері (як організаційних, так і технічних), а також про ті заходи, які необхідно реалізувати для проходження сертифікації на відповідність певному стандарту (якщо за результатами проведеного аудиту зроблено висновок про те, що поточний рівень захищеності інформаційних ресурсів підприємства не відповідає таким вимогам);

• висновок про ступінь відповідності політики безпеки підприємства та всього комплексу заходів щодо захисту інформації вимогам чинного законодавства та відомчих нормативних актів;

• оцінки економічної ефективності вкладень у ті чи інші засоби захисту інформації, а також організаційні заходи (віддачі від них);

• кількісна (грошова) оцінка можливих втрат від тих чи інших порушень, які можуть відбутися при існуючому рівні забезпечення інформаційної безпеки, а також розрахунок необхідних вкладень, які необхідно здійснити для досягнення певного рівня захищеності.

Також за результатами аудиту можуть бути сформульовані додаткові рекомендації, що стосуються:

• перегляду окремих бізнес-процесів і процедур;

• вдосконалення роботи з персоналом підприємства;

• впровадження та використання сучасних технічних (програмних і апаратних) засобів обробки і захисту інформації;

• організації роботи щодо захисту інформації;

• вибору пріоритетів у процесі усунення існуючих недоліків.

## КОНТРОЛЬНІ ЗАПИТАННЯ

### Тема 1.
### Поняття та основи управління інформаційною безпекою організації

1. Що таке інформаційна безпека?
2. Що включає в себе поняття "безпечна діяльність" будь-якого підприємства?
3. Що таке автоматизована система(АС) та захист інформації в АС?
4. Розкрийте суть поняття "інформація".
5. Що таке повідомлення і які його види ви знаєте?
6. Яким процесам піддається інформація в КС? Коротко опишіть кожен з них
7. Класифікація видів інформації.
8. На які категорії можна розділити інформацію за рівнем важливості? Опишіть їх.
9. Які існують особливості інформації як об’єкта власності?
10. Що таке інформаційна продукція та інформаційні послуги?
11. Значення інформаційної безпеки на підприємстві.
12.Опишіть які ви знаєте напрямки щодо забезпечення інформаційної безпеки на рівні підприємства?

### Тема 2.
### Інформаційні потоки в організації

1. Дайте визначення організації та охарактеризуйте здійснення інформаційної діяльності у системі організаційного управління.
2. Інформаційний потік його характеристика та види?
3. Чим визначається корисність інформації та які вимоги до її якості?
4. Як класифікується інформація за фізичною формою подання?
5. Назвіть найбільш важливі види джерел інформації на підприємстві.
6. Види інформаційних потоків та їх характеристика.
7. Заходи з удосконалення процесів обміну інформаією.
8. Суть життєвого циклу інформаційного ресурсу.
9. Бар’єри шляху інформаційних процесів у організації та їх характеристика.
10. Підсистеми структури інформаційних процесів на підприємстві.
11. Розкрити зміст функцій менеджменту та циклу інформаційного ресурсу – визначення цілей.
12. Розкрити зміст функцій менеджменту та циклу інформаційного ресурсу – збирання, створення, зберігання, пошук, передача повідомлень і даних.
13. Розкрити зміст функцій менеджменту та циклу інформаційного ресурсу – використання інформаційних ресурсів.
14.Перерахуйте типові завдання функції організація підсистеми комунікації.
15. Перерахуйте типові завдання функції контроль підсистеми документно-інформаційні ресурси.

## Тема 3.
## Загрози інформаційній безпеці та необхідність захисту інформації на підприємстві

1. Що таке безпека підприємницької діяльності?
2. Базисом на якому будується безпека бізнесу є комплекс ресурсів, якими володіє будь-який бізнес. Назвіть ці ресурси?
3. Навіщо захищати інформацію?
4. Що може створювати небезпеку для бізнесменів зацікавлених у дотриманні комерційної таємниці?
5. Опишіть інформацію, яка представляє інтерес при зборі і аналізі відомостей?
6. Безпека включає забезпечення необхідного рівня захищеності по ряду напрямків. Яких саме?
7. З яких етапів складається процес аналізу ризику?
8. За якими параметрами класифікують потенційних порушників?
9. З яких процесів складається робота з накопичення статистики?
10. Які ви знаєте внутрішні загрози безпеки обєкта захисту?
11. Які ви знаєте зовнішні загрози безпеки обєкта захисту?
12. Опишіть пасивні та активні загрози.
13. Які існують основні шляхи витоку інформації і несанкціонованого доступу до автоматизованих інформаційних систем?

## Тема 4.
## Канали витоку інформації на підприємстві

1. Які ви знаєте групи можливих каналів витоку інформації на підприємстві?
2. Як класифікують канали несанкціонованого доступу до інформації?
3. Опишіть як відбувається витік акустичної інформації через мікрофони?
4. Опишіть як відбувається витік акустичної інформації через диктофони та магнітофони?
5. Опишіть як відбувається витік акустичної інформації через радіомікрофони?
6. Яких типів бувають мікрофони?
7. За якими ознаками класифікують радіозакладки?
8. Які завдання виконують скануючі приймачі?
9. Опишіть витік інформації за рахунок таємного відеоспостереження?
10. Опишіть витік інформації за рахунок дистанційного відеоспостереження?
11. Опишіть витік інформації за рахунок ПЕМВН (побічні електромагнітні аипромінювання і наведення).
12. Опишіть витік інформації за рахунок використання засобів звязку.

## Тема 5.
## Стандарти інформаційної безпеки

1. Що таке "загроза", "джерело загрози" і "вразливість"?
2. Що таке доступ?

3. З яких стадій складається життєвий цикл КС?
4. Вирішенню яких проблем у сфері ІБ сприяють стандарти безпеки?
5. Опишіть відомі вам стандарти безпеки.
6. Що таке атрибути доступу?
7. Які ви знаєте критерії конфіденційності?
8. Що таке критерії цілісності? Їх види.
9. Що таке критерії доступності? Їх види.
10. Що таке критерії спостереженості? Їх види.
11. Що таке критерії гарантій? Їх види.

## Тема 6.
## Політика інформаційної безпеки організації

1.Основне завдання забезпечення внутрішньооб'єктивного режиму?
2.Що встановлюється у рамках пропускного режиму?
3.Що лежить в основі засобів контролю доступу?
4.Що передбачає фізичний захист об'єктів?
5.Що пов'язано з фізичним захистом об'єктів?
6.Назвіть основні заходи організації режиму секретності?
7. Політики використання окремих універсальних інформаційних технологій включають в себе? Що саме?
8.Що може передбачати політика використання електронної пошти?
9.Що таке політика інформаційної безпеки?
10.Назвіть принципи політики інформаційної безпеки?
11.Які види політичної інформаційної безпеки вам відомі?
12.Що собою являє виборча політика безпеки?
13.Призначення повноважної політики безпеки?
14.Назвіть основні організаційно-технічні заходи щодо ЗІ ?
15. Які дії можуть значно підвищити ступінь захисту корпоративної мережі без великих фінансових уливань?

## Тема 7.
## Організація системи інформаційної безпеки підприємства

1. Як відбувається постановка завдання?
2. Як здійснюється порядок розв'язання завдання?
3. Поняття та особливості багаторівневої моделі об'єктів інформаційної безпеки.
4. Які є правила побудови системи інформаційної безпеки підприємства?
5. Перелічити та пояснити принципи захисту інформації
6. Методи забезпечення інформаційної безпеки організації?
7. Засоби забезпечення інформаційної безпеки організації?
8. У чому полягає методика побудови корпоративної системи захисту інформації?
9. Як відбувається формування організаційної політики безпеки?

10. Особливості розробки концепції безпеки?
11. У чому полягає страхування інформаційних ризиків?

## Тема 8.
## Організаційні заходи захисту інформації суб'єктів господарювання

1. Поняття комерційної таємниці?
2. Що може становити комерційну таємницю на підприємстві?
3. Специфіка захисту комерційної таємниці?
4. Поняття конфіденційної інформації?
5. Основи та особливості організаційних заходів захисту інформації на підприємстві?

## Тема 9.
## Організація роботи відділу (департаменту) інформаційної безпеки організації

1.Що являє собою департамент інформаційної безпеки?
2.Які основні завдання департаменту вам відомі?
3.Якими особливостями визначається склад завдань департаменту та його внутрішня структура?
4.Що включають в себе функції,пов'язані з впровадженням засобів захисту інформації?
5.Які функції мають значення для забезпечення інформаційної безпеки?
6.На практиці департамент є?
7.Що включають в себе функції,пов'язані з адмініструванням інформаційних систем і систем захисту інформації?
8.Назвіть організаційну структуру департаменту інформаційної безпеки?
9.Основні цілі роботи з персоналом підприємства?Назвати?
10.Що собою являє початкова стадія роботи?
11.методи психологічної оцінки при підборі і розстановці кадрів?
12.У яких випадках може проводитися додаткове навчання персоналу підприємства?

## Тема 10.
## Заходи реагування на інциденти

1.Що таке інцидент?
2.Чим може бути обумовлена надзвичайна ситуація (інцидент)?
3.Що включають в себе інциденти?
4.Які чотири етапи включає в себе інцидент?
5.Яке основне завдання на початковому етапі реагування?
6.Який один найважливіший організаційний аспект реагування на інцидент?
7.Що відбувається на етапі локалізації та усуненні наслідків?
8.Що необхідно для виявлення джерела нападу?

9.Які основні завдання оцінки та аналізу процесу нападу?
10.Заключним етапом процесу реагування є?Доповнити ?
11.Що включає в себе додаткова інформаційна робота?
12.Що було створено для об'єднання зусиль різних груп реагування ?

## Тема 11.
## Аудит системи інформаційної безпеки підприємства

1.Що являє собою аудит стану інформаційної безпеки на підприємстві?
2.Які основні види аудиту вам відомі?
3.Назвіть цілі аудиту?
4.Які існують завдання аудиту? Перелічити?
5.Що є базою для проведення аудиту?
6.У чому полягає основна робота аудиторів у процесі збору інформації?
7.Які є основні етапи проведення аудиту?
8.Що являє собою основна стадія аудиту?
9.Який існує важливий напрям аудиторської перевірки?
10.Що включає в себе перевірка стану фізичної безпеки інформаційної інфраструктури?
11.Що є остаточним результатом аналізу та узагальнення даних?
12.Якими стандартами і вимогами користуються компанії,що спеціалізуються на проведенні аудитів?

# ТЕСТИ

## ТЕМА 1

**1. Об’єктами захисту з урахуванням їх пріоритетів є:**
А) підприємство, особа, цінні папери;
Б) особа, інформація, матеріальні цінності;
В) організація, економічні операції, підприємство;
Г) підприємство, особа, економічні операції

**2. Вид інформації, витік якої може привести до банкрутства підприємства:**
А) матеріальна інформація;
Б) економічна інформація;
В) комерційна інформація;
Г) усі відповіді вірні

**3. Автоматизована система – це:**
А) стан інформації, у якому забезпечуються збереження визначених політикою безпеки властивостей інформації;
Б) організаційно-технічна система, що об’єднує обчислювальну систему, фізичне середовище, персонал і оброблювальну інформацію;
В) діяльність, яка спрямована на забезпечення безпеки інформації;
Г) стан інформації, що об’єднує обчислювальну систему, фізичне середовище, персонал і оброблювальну інформацію

**4. Інформація – це :**
А) результат відображення та обробки в людській свідомості різноманіття навколишнього світу відомостей про предмети,що оточують людину,явищ природи,діяльність інших людей;
Б) сукупність організаційних та інженерних заходів,програмно – апаратних засобів,які забезпечують захист в автоматизованих системах;
В) фізична величина, що передає безперервне повідомлення;
Г) діяльність, яка спрямована на забезпечення безпеки оброблюваної в економічній сфері

**5. Повідомлення – це:**
А) інформація, що втілена і зафіксована в певній матеріальній формі;
Б) набір словосполучень, який має певний зміст;
В) набір тексту, який занесено в комп’ютерну систему;
Г) інформація,яка внесена в комп’ютерну систему

**6. Інформація поряд з матеріальними об’єктами захищається законом:**
А) так, завжди;
Б) ні, це не можливо;
В) так, але не завжди;

Г) вірна відповідь відсутня

**7. Набір букв (символів) дискретного повідомлення утворює:**
А) словосполучення;
Б) текст;
В) алфавіт;
Г) всі відповіді вірні

**8. Збереження або передача інформації без матеріального носія можлива?**
А) так;
Б) ні;
В) так, але не завжди;
Г) вірна відповідь відсутня

**9. Несуттєва інформація – це:**
А) інформація, що може бути замінена чи відновлена;
Б) інформація, яку важко відновити;
В) інформація, без якої система продовжує існувати;
Г) всі відповіді вірні

**10. Ревелантність інформації – це:**
А) показник, що характеризує відповідність її потребам задачі, яка розв'язується;
Б) показник сприйняття та використання інформації в процесі розв'язання відповідної задачі;
В) показник, що характеризує міру достатності інформації;
Г) показник, який показує ступінь економічного зростання

**11. Таємність інформації – це:**
А) захист інформації від негативних впливів на неї;
Б) статус інформації, який фіксується залежно від її важливості та певного рівня її захищеності;
В) інформація, яка розголошується тільки працівникам організації;
Г) усі відповіді вірні

**12. Фактична сфера безпеки інформації – це:**
А) захист інформації;
Б) захист прав власності на інформацію;
В) захист об'єму інформації;
Г) правильної відповіді немає

**13. Право власності включає такі види правомірності власника:**
А) право збереження, право копіювання, право використання;
Б) право передачі, право розпорядження, право розміщення;
В) право розпорядження, право володіння, право користування;

Г) право збереження, право копіювання, право розміщення

**14. Повідомлення можуть бути:**
А) безперервними(аналоговими);
Б) дискретними(цифровими);
В) текстовими;
Г) вірні відповіді а і б

**15. При дискретній формі представлення інформації окремим її елементам можуть бути присвоєнні:**
А) числові значення;
Б) буквені значення;
В) текстові значення;
Г) аналогові значення

**16. Процеси, яким піддається інформація в комп'ютерних системах:**
А) введення;
Б) збереження;
В) обробка;
Г) виведення;
Д) всі відповіді вірні

## ТЕМА 2

**1. Організація –**
А) це структура, стан якої визначається виключно зовнішньою взаємодією з оточуючим середовищем;
Б) це динамічна структура, яка охоплює елементи внутнішного та зовнішнього середовища;
В) це динамічна структура, стан якої визначається як зовнішньою взаємодію з оточуючим середовищем так і внутрішньою взаємодією між її елементами;
Г) вірна відповідь відсутня

**2. До моделей «електронних офісів» належать:**
А) інформаційна, комунікаційна, соціотехнічна моделі;
Б) інформаційна, технічна, колективна моделі;
В) комунікаційна, соціотехнічна, організаційна моделі;
Г) вірна відповідь відсутня

**3. Комунікаційна модель «електронних офісів»–**
А) описує процес і результат проектування автоматизованих систем;
Б) обґрунтовує інформацію управління як комплексну систему;
В) включає організацію апарату управління разом з персоналом, організаційними зв'язками, методами роботи;
Г) вірні відповіді б, в

**4. Інформаційний потік поділяється на :**
А) прямий, непрямий;
Б) соціальний, комунікаційний, інформаційний;
В) горизонтальний, прямий;
Г) горизонтальний, вертикальний

**5. Вимоги до якості інформації:**
А) конфіденційність, доступність і зрозумілість, достовірність, порівнюваність, відповідність і своєчасність;
Б) достовірність, відповідність, зрозумілість, своєчасність, стабільність;
В) конфіденційність, порівнюваність, вірність, укомплектованість;
Г) зрозумілість, реальність, стабільність, лінійність

**6. За процедурою перетворення інформація класифікується на:**
А) основна, опрацьована, аналітична;
Б) ймовірна, соціальна, моделююча, аналітична, обчислювана;
В) універсальна, спеціалізована;
Г) вірна відповідь відсутня

**7. Залежно від суб'єкта інформацію розрізняють:**
А) публічна, таємна, невідома;
Б) аналітична, прогнозна, довідкова, ознайомча, рекомендаційна;
В) зовнішня, внутрішня;
Г) достовірна, правильна, сучасна, легалізована

**8. Вертикальний інформаційний потік пов'язує:**
А) процес і результат проектування автоматизованих систем;
Б) органи управління,які знаходяться на одному рівні;
В) підприємства та соціальні служби;
Г) органи управління різних рівнів

**9. Порівнюваність інформації забезпечує:**
А) надання користувачам лише тієї інформації яка не завдасть шкоди організації з боку конкурентів;
Б) здатність впливати на прийняття рішення користувачем;
В) можливість порівняння показників, що потребує застосування набору визначень, одиниць вимірювання, методики опрацювання даних;
Г) гарантію об'єктивності та правдивості надання даних

**10. До видів інформаційних потоків належать:**
А) вертикальний обмін інформацією;
Б) формальний обмін інформацією;
В) горизонтальний обмін інформацією;
Г) міжгалузевий обмін інформацією

**11. Подання інформації в середині системи – це:**
А) найбільш складний етап обробки, коли вхідна інформація перетворюється в інформаційну структуру і зручну для користувача;
Б) є початковим етапом внутрішньої інформаційної обробки;
В) обмін між організацією та зовнішнім середовищем;
Г) нисхідні потоки інформації, якими повідомляють підлеглим про поточні завдання

**12. Викривлення повідомлень буває:**
А) ненавмисні викривлення;
Б) навмисні викривлення;
В) специфічні зміни у структурі користувачів інформації;
Г) вірні відповіді а, б

**13. Підсистеми структури інформаційних процесів:**
А) первинне інформаційне середовище;
Б) вхідний інформаційний фільтр;
В) аналіз реакції користувача;
Г) всі відповіді вірні;
Д) вірні відповіді а і в

**14. Горизонтальний обмін інформацією:**
А) наради керівників суміжних підрозділів;
Б) обговорення виробничих питань під час неформальних зустрічей;
В) обмін інформацією між організацією і зовнішнім середовищем;
Г) обмін інформацією між керівниками та підлеглими

**15. На вході інформації забезпечується:**
А) блокування несанкціонованого виходу інформації з системи;
Б) захист від несанкціонованого доступу до внутрішньої інформації системи;
В) вірна відповідь відсутня;
Г) всі відповіді вірні

**16. До життєвого циклу інформаційного ресурсу належать:**
А) визначення цілей і інформації, необхідної для їх дослідження;
Б) використання інформації;
В) вірні відповіді а, б;
Г) вірна відповідь відсутня

**17. Етап життєвого циклу інформаційного ресурсу «визначення цілей» включає такі функції:**
А) планування;
Б) організація;
В) контроль;

Г) всі відповіді вірні;
Д) вірні відповіді а і в

**18. Зміст функції менеджменту планування на етапі визначення цілей у структурі життєвого циклу інформаційного ресурсу включає:**
А) аналіз інформаційних потреб організації; розробка планів інформаційної роботи;
Б) проведення нарад, семінарів, виставок ; контроль ефективності використання інформаційних матеріалів;
В) організація комп'ютерної переробки інформації; впровадження, ведення і розвиток системи документації;
Г) аналіз перспектив розвитку галузі; створення умов для зберігання нормативної інформації

**19. До етапів життєвого циклу інформаційного ресурсу належить :**
А) визначення цілей; збирання і створення, зберігання, пошук, передача повідомлення і даних; використання інформаційних ресурсів;
Б) аналіз інформаційних потреб організації; контроль ефективності використання інформаційних ресурсів;
В) вивчення потреб працівників підприємства в інформації; пошук зовнішньої інформації, яка відповідає потребам організації;
Г) вірна відповідь відсутня

**20. Типовим завданням планування інформаційної діяльністю, як функція менеджменту є :**
А) організація ділових контрактів підприємства із зовнішнім середовищем;
Б) контроль структури зовнішніх і внутрішніх інформаційних потоків;
В) планування розвитку організації з урахуванням впровадження нових інформаційних **технологій;**
Г) інформаційно-аналітичний моніторинг документного потоку мережі Інтернет

**21. Типовим завданням організації інформаційної діяльності, як функції менеджменту є:**
А) організація процесів управління інформаційною діяльністю;
Б) здійснення соціально-психологічного регулювання в трудових колективах;
В) організація ділових контрактів підприємства із зовнішнім середовищем;
Г) вірні відповіді а, б

**22. Типовим завданням контролю інформаційної діяльності, як функції менеджменту є:**
А) контроль використання інформаційно-ресурсного потенціалу підприємства;
Б) контроль форм і методів подання інформації користувачам віртуального середовища;
В) контроль структури зовнішніх і внутрішніх інформаційних потоків;
Г) всі відповіді вірні;

Д) вірні відповіді б і в

**23. Уміння здійснювати контроль якості і достовірності інформації, що циркулює всередині організації і тієї що находить із зовнішніх джерел – це:**
А) функція організація підсистеми комунікації;
Б) функція планування підсистеми управління інформаційною діяльністю;
В) функція контроль підсистеми комунікації;
Г) всі відповіді вірні

## ТЕМА 3

**1. Базисом, на якому будується безпека бізнесу є:**
А) комплекс методів;
Б) комплекс ресурсів, якими володіє будь який бізнес;
В) комплекс прийомів та принципів;
Г) вірна відповідь відсутня

**2. Програми, патенти, технології, ліцензії, інформаційні системи – це:**
А) математичний ресурс;
Б) підприємницький ресурс;
В) інтелектуальний ресурс;
Г) інформаційна безпека

**3. Найважливішу роль у захисті бізнесу відіграє :**
А) безпека інноваційної діяльності;
Б) інформаційна безпека;
В) матеріальні ресурси;
Г) вірна відповідь відсутня

**4. До відомостей особистого характеру належать :**
А) статутні документи фірм
Б) інформація керівника та членів його сім'ї;
В) кредитні договори з банками;
Г) умови фінансової діяльності

**5. Конфіденційна інформація компанії – це:**
А) інтелектуальні ресурси;
Б) інформаційні ресурси;
В) фізичні ресурси;
Г) програмні ресурси

**6. Сервери, робочі станції, мережеве та телекомунікаційне обладнання належать до:**
А) програмних ресурсів;
Б) інтелектуальних ресурсів;

В) фізичних ресурсів;
Г) вірна відповідь відсутня

**7. Загрози інформаційній безпеці класифікуються на :**
А) основні та другорядні;
Б) навмисні та ненавмисні;
В) внутрішні та зовнішні;
Г) вірна відповідь відсутня

**8. До внутрішніх загроз безпеки об'єкта захисту належать :**
А) зрада персоналу;
Б) впливи конкурентів;
В) стихійні лиха;
Г) дії постачальників послуг із забезпечення безпеки

**9. До зовнішніх загроз безпеки об'єкта захисту належать :**
А) зрада персоналу;
Б) негативні впливи недобросовісних конкурентів;
В) дії персоналу;
Г) відсутність належної кваліфікації керівника

**10. Загрози, зумовлені несанкціонованими діями обслуговуючого персоналу та несанкціонованим доступом до інформації сторонніх осіб – це :**
А) ненавмисні загрози;
Б) навмисні загрози;
В) пасивні загрози;
Г) активні загрози

**11. До фізичних способів впливу загроз на об'єкта інформаційної безпеки належать:**
А) впровадження комп'ютерних вірусів;
Б) знищення або руйнування засобів обробки інформації та зв'язку;
В) вплив на персонально-ключові системи;
Г) вплив на парольно-ключові системи

**12. Невиконання вимог законодавства та затримки в прийнятті необхідних нормативно-правових положень в інформаційній сфері належить до:**
А) радіоелектронних способів впливу загроз;
Б) фізичних способів впливу загроз;
В) організаційно-правових способів впливу загроз;
Г) інформаційних способів впливу загроз

## ТЕМА 4

**1. Типи заставних пристроїв :**
А) що працюють постійно;
Б) з вбудованими таймерами, що включаються в певний час;
В) керовані дистанційно;
Г) що працюють в режимі очікування;
Д) всі відповіді вірні;
Е) вірні відповіді в і г

**2. Групи каналів витоку інформації на підприємстві:**
А) канали, пов'язані з доступом до елементів системи і зміною структури її компонентів;
Б) канали, пов'язані з доступом до елементів системи обробки даних, але не потребують зміни компонент системи;
В) канали розкладання носіїв інформації;
Г) вірні відповіді а і б;
Д) всі відповіді вірні

**3. Класифікація каналів несанкціонованого доступу до інформації, за якими можна здійснити її розкрадання, зміну або знищення :**
А) доступ через людину;
Б) доступ через навколишнє середовище;
В) доступ через програму;
Г) доступ через апаратуру;
Д) вірні відповіді а, в, г;
Е) вірні відповідь б, в, г

**4. Робоча частота радіо закладок:**
А) від 20 МГц до 2,0 ГГц;
Б) від 35 МГц до 2,5 МГц;
В) від 40 МГц до 1,5 ГГц;
Г) від 45 МГц до 2,0 ГГц

**5. Типи мікрофонів :**
А) вбудовані;
Б) виносні;
В) акустичні;
Г) вібраційні;
**Д) вірні відповіді в, г**

**6. Типи некоректного використання ЕОМ:**
А) доступ до ЕОМ осіб,які не мають на це права;
Б) зчитування інформації з ЕОМ;

В) оцінка ефективності використання технічних засобів захисту інформації;
Д) вірні відповіді а, б

**7. З дисплеїв можна зняти інформацію за допомогою:**
А) спеціальної апаратури на відстані до 500 - 1500 м;
Б) принтерів до 100 – 150 м;
В) вірні відповіді а, б;
Г) вірна відповідь відсутня

**8. З дисплеїв можна зняти інформацію на відстані:**
А) 450 – 1600 м;
Б) 500 - 1500 м;
В) 50 – 150 м;
Г) 700 – 1900 м

**9. З принтерів можна зняти інформацію на відстані:**
А) 500 – 1000 м;
Б) 100 – 150 м;
В) 300 – 500 м;
Г) вірна відповідь відсутня

**10. До класифікаційних ознак радіозакладки відносять:**
А) довготривалість роботи;
Б) дистанції передачі;
В) діапазон використовуваних частот;
Г) всі відповіді вірні;
Д) вірна відповідь відсутня

## ТЕМА 5

**1. Доступ – це :**
А) категорія, що описує процес виконання операцій суб’єктів над об’єктами;
Б) поняття, що знеособлює причину виведення системи із захищеного стану через дії джерела загрози;
В) звернення активного об’єкта до пасивного;
Г) вірна відповідь відсутня

**2. Теорія комп’ютерної безпеки вирішує такі класи взаємопов’язаних завдань:**
А) експлуатація захищеної системи і проектування КС і ПБ;
Б) керування безпекою і формулювання та вивчення ПБ;
В) гарантування заданої ПБ і моделювання ПБ;
Г) всі відповіді вірні

**3. Стандарти безпеки ефективно сприяють вирішенню наступних проблем у сфері ІБ :**
А) реалізація ПБ і механізмів її гарантування;
Б) забезпечення об'єктивності оцінок захищеності ІС і технологій;
В) створення технологій кваліфікаційного аналізу і синтезу захищених ІС;
Г) вірні відповіді б, в;
Д) вірні відповіді а, б

**4. _____ - дозволяє виявити й виключити присутність у системі потоків інформації,яка не може контролюватися іншими засобами захисту**
А) довірча конфіденційність;
Б) повторне використання об'єктів;
В) аналіз прихованих каналів;
Г) конфіденційність при обміні;
Д) адміністративна конфіденційність

**5. Критерії _____ - регламентують роботу засобів, що дозволяють встановити відповідальність користувачів за події в системі**
А) доступності;
Б) спостереженості;
В) цілісності;
Г) конфіденційності;
Д) вірна відповідь відсутня

**6. Спостереженість забезпечується наступними засобами:**
А) використання ресурсів;
Б) цілісність при обміні;
В) ідентифікація та автентифікація;
Д) всі відповіді вірні;
Г) вірна відповідь відсутня

**7. Вимоги до_____ забезпечують гарантії повної керованості розробником, процесами розробки й супроводу оцінюваної КС**
А) архітектури;
Б) документації;
В) середовища розробки;
Г) вірна відповідь відсутня

**8. _____ - дозволяє виявити потенційно небезпечні дії користувачів**
А) реєстрація;
Б) ідентифікація;
В) автентифікація;
Г) само тестування

**9. Опис профілю складається з таких частин :**

А) літературно- числового ідентифікатора;
Б) знака рівості;
В) переліку рівнів послуг у фігурних дужках;
Г) всі відповіді вірні

**10. Життєвий цикл КС складається з таких стадій:**
А) розробка технологій перевірки захищеності систем і проектування КС;
Б) проектування КС і ПС та моделювання ПБ;
В) всі відповіді вірні;
Г) вірна відповідь відсутня

**11. Європейські критерії,безпеки ІТ позначаються:**
А) ITSEC;
Б) TCSEC;
В) FCTITS;
Г) CSSCCSE

**12. До функціональних критеріїв відносять :**
А) документація;
Б) критерії доступності;
В) архітектура системи;
Г) середовище функціонування

## ТЕМА 6

**1. Основою внутрішньооб'єктного режиму є пропускний режим, у рамках якого встановлюються:**
А) документи, що дають право проходу на територію підприємства;
Б) категорії перепусток, що використовуються на підприємстві;
В) вірні відповіді а і б;
Г) вірна відповідь відсутня

**2. Для відомостей, що становлять державну таємницю, встановлюються такі ступені секретності:**
А) "особливо важливо";
Б) "цілком таємно";
В) "таємно ";
Г) усі відповіді вірні

**3. Політика використання окремих універсальних інформаційних технологій в масштабі всього підприємства включає в себе:**
А) політику використання електронної пошти (e - mail);
Б) політика придбання інформаційних систем та їх елементів;
В) політика доступу сторонніх користувачів;

Г) політика управління паролями

**4. Політика використання електронної пошти включати в себе:**
А) загальні обмеження на її використання певними категоріями співробітників;
Б) вимоги до управління доступом і збереження конфіденційності повідомлень;
В) усі відповіді правильні;
Г) вірна відповідь відсутня

**5. Політика інформаційної безпеки – це:**
А) сукупність правових і морально-етичних норм, правил, адміністративних, організаційних і технічних заходів, програмних і криптографічних засобів, направлених на захист інформаційної інфраструктури від випадкового і навмисного втручання в процес її функціонування;
Б) набір законів, правил і практичних рекомендацій і практичного досвіду, що визначають управлінські і проектні рішення в області ЗІ;
В) стан захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди;
Г) стан захищеності, при якому спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам

**6. Заходи при розробці і проведенні інформаційної політики передбачають:**
А) неможливість минати захисні засоби;
Б) посилення самої слабкої ланки;
В) посилення самої сильної ланки;
Г) вірні відповіді а і б

**7. Принцип неприпустимості переходу у відкритий стан означає що:**
А) при будь-яких обставинах (у тому числі позаштатних) СЗІ або цілком виконує свої функції, або повинна цілком блокувати доступ;
Б) що всі інформаційні потоки в мережу, що захищається, і з неї повинні проходити через екран;
В) що всі інформаційні потоки в мережу, що захищається, і з неї повинні проходити через систему контролю доступу;
Г) вірна відповідь відсутня

**8. Вибіркове керування доступом передбачає, що:**
А) усі суб'єкти й об'єкти системи повинні бути ідентифіковані;
Б) кожному суб'єкту системи притаманний рівень прозорості, що визначає максимальне значення ступеня критичності об'єктів, до яких суб'єкт має доступ;

В) усі відповіді вірні;
Г) вірна відповідь відсутня

**9. Повноважне керування доступом має на увазі:**
А) усі суб'єкти й об'єкти системи повинні бути однозначно ідентифіковані
Б) кожному об'єкту системи притаманна точка критичності, що визначає цінність інформації, що міститься в ньому;
В) кожному суб'єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ;
Г) вірні відповіді а і б;
Д) вірна відповідь відсутня

**10. Основне призначення повноважної політики безпеки:**
А) реалізує принцип "що не дозволено, те заборонено", що припускає явний дозвіл доступу суб'єкта до об'єкта;
Б) регулює доступ суб'єктів системи до об'єктів з різним рівнем критичності і запобігає витоку інформації з верхніх рівнів посадової ієрархії на нижні, а також блокує можливе проникнення з нижніх рівнів на верхні;
В) регулює доступ суб'єктів системи до об'єктів з різним рівнем критичності;
Г) вірні відповіді б і в

**11. Організаційно-технічні заходи щодо ЗІ:**
А) створення науково-технічних і методологічних основ захисту ІС;
Б) забезпечення загальної підтримки заходів безпеки;
В) оцінка можливого збитку, викликаного порушенням безпеки інформації, розробка адекватних вимог по основних напрямках захисту;
Г) вірні відповіді а і в;
Д) вірні відповіді а і б

**12. Політика опублікування матеріалів у відкритих джерелах повинна:**
А) забезпечувати запобігання випадкових і організованих витоків конфіденційної інформації при взаємодії підприємства із засобами масової інформації, громадськими та **державними органами, науковим, академічним і бізнес-спільнотою;**
Б) забезпечувати захист законних прав щодо безпеки інформації організації, окремих її структурних підрозділів, персоналу в процесі інформаційної діяльності та взаємодії між собою, а також у взаємовідносинах з зовнішніми вітчизняними і закордонними організаціями;
В) забезпечити загальну підтримку заходів безпеки;
Г) вірна відповідь відсутня

**13. Політика придбання інформаційних систем та їх елементів включає:**
А) вимоги до питань безпеки і надійності програмних засобів, самостійно розроблюваних підприємством та вимоги щодо передачі розробки програмних засобів;

Б) вимоги до ліцензування та сертифікації використовуваного програмного забезпечення і устаткування, а також певні вимоги до фірм, які здійснюють їх постачання та впровадження;
В) вимоги до постачальників програмного забезпечення;
Г) вірна відповідь відсутня

**14. Для інформаційної системи політика безпеки повинна бути:**
А) загальною
Б) індивідуальною
В) вибірковою
Г) альтернативною

**15. Матриця доступу являє собою:**
А) прямокутну матрицю, у якій об'єкту системи відповідає рядок, а суб'єкту стовпець;
Б) прямокутну матрицю, у якій об'єкту системи відповідає стовпець, а суб'єкту рядок;
В) таблицю із комплексом значень;
Г) таблицю із однаковою кількістю стовпців та рядків, що відповідають об’єктам та суб’єктам системи

## ТЕМА 7

**1. Модель функціонування об’єкта захисту – це…**
А) Вивчення поведінки інформації в носіях та її руху по обумовлених каналах зв’язку;
Б) Вид діяльності або клас вирішуваних завдань;
В) Протокол зберігання обробки та обміну інформацією між носіями;
Г) Вірні відповіді а, в

**2. Підприємство, як об’єкт захисту складається з:**
А) Виду діяльності або класу вирішуваних завдань;
Б) Носіїв інформації різної фізичної природи;
В) Вимог щодо забезпечення безпеки інформації;
Г) Всі відповіді вірні

**3. Фактори, які впливають на вироблення політики безпеки інформаційних систем організації:**
А) Визначення цілей захисту;
Б) Визначення об’єкта захисту;
В) Отримання гарантій захищеності системи;
Г) Всі відповіді вірні;
Д) Вірні відповіді а, в

**4. Кількість рівнів, що містить багаторівнева модель об'єктів інформаційної безпеки:**
А) 10;
Б) 7;
В) 4;
Г) 2;

**5. Правило побудови системи інформаційної безпеки підприємства «запобігання можливих загроз» означає:**
А) Своєчасне виявлення можливих загроз безпеки підприємства, аналіз яких дозволить робити відповідні профілактичні заходи;
Б) Заходи, що розробляються на основі чинних правових актів;
В) Використання всіх наявних в розпорядження підприємства сил та засобів;
Г) Врахування усіх факторів, що впливають на безпеку підприємства.

**6. Правило побудови системи інформаційної безпеки підприємства «законність» означає:**
А) Своєчасне виявлення можливих загроз безпеки підприємства;
Б) Заходи, що розробляються, повинні базуватися на основі чинних правових актів;
В) Використання всіх наявних в розпорядження підприємства сил та засобів;
Г) Вірна відповідь відсутня.

**7. Правило побудови системи інформаційної безпеки підприємства «комплексне використання сил і засобів» означає:**
А) Врахування усіх факторів, що впливають на безпеку підприємства;
Б) Використання всіх наявних в розпорядження підприємства сил та засобів;
В) Заходи, що розробляються на основі чинних правових актів;
Г) Вірна відповідь відсутня.

**8. Правило побудови системи інформаційної безпеки підприємства «поєднання гласності із секретністю» означає:**
А) Доведення інформації до відома персоналу підприємства та громадськості в допустимих межах заходів безпеки;
Б) Використання всіх наявних в розпорядження підприємства сил та засобів;
В) Виявлення загроз підприємства;
Г) Вірна відповідь відсутня.

**9. Правило побудови системи інформаційної безпеки підприємства «компетентність» означає:**
А) Запобігання потенційних і реальних загроз;
Б) Співробітники повинні вирішувати питання забезпечення безпеки на професійному рівні;
В) Врахування усіх факторів, що впливають на безпеку підприємства;
Г) Вірна відповідь відсутня.

**10. Правило побудови системи інформаційної безпеки підприємства «економічна доцільність» означає:**
А) Запобігання потенційних і реальних загроз;
Б) Вартість фінансових витрат на забезпечення безпеки не повиння перевищувати оптимальний рівень;
В) Доведення інформації до відома персоналу;
Г) Вірна відповідь відсутня.

**11. Правило побудови системи інформаційної безпеки підприємства «планова основа діяльності» означає:**
А) Врахування усіх факторів, що впливають на безпеку підприємства;
Б) Діяльність щодо безпеки повинна будуватися на основі комплексної програми забезпечення безпеки підприємства;
В) Здійснення заходів ІБ на основі стратегічного плану;
Г) Вірна відповідь відсутня.

**12. Правило побудови системи інформаційної безпеки підприємства «системність» означає:**
А) Запобігання загроз;
Б) Врахування усіх факторів, що впливають на безпеку підприємства, включення в діяльність щодо його забезпечення всіх співробітників, використання всіх сил та засобів;
В) Здійснення заходів безпеки виходячи із системи управління підприємством;
Г) Всі відповіді вірні.

**13. Адекватність, системність, прозорість, рівноцінність ланок, безперервність, багаторівневість – це … ?**
А) Принципи захисту інформації;
Б) Правила побудови системи інформаційної безпеки;
В) Методи забезпечення інформаційної безпеки;
Г) Засоби захисту інформаційної безпеки.

**14. Відповідно до ЗУ «Про інформацію», цілями захисту інформації є :**
А) Запобігання витоку, розкрадання, втрати, спотворення, підробки інформації;
Б) Запобігання несанкціонованих дій по знищенню, модифікації, спотворення, копіювання, блокування інформації;
В) Запобігання інших форм незаконного втручання в інформаційні ресурси та інформаційні системи;
Г) Створення служби захисту інформації;
Д) Вірні відповіді А, Б, В;
Е) Вірні відповіді А, Б, Г.

**15. Ризик – це …**
А) Загроза інформації;

Б) Фактор, що відображає можливий збиток організації в результаті реалізації загрози ІБ;
В) Метод фізичного перешкоджання шляху зловмиснику;
Г) Вірна відповідь відсутня.

**16. Технічні способи захисту від загроз передбачають:**
А) Використання оперативних методів роботи;
Б) Встановлення охоронно-пожежної сигналізації, використання систем контролю і управління доступом;
В) Роботу сторожів і контролерів;
Г) Вірна відповідь відсутня.

**17. Оперативні способи захисту від загроз передбачають:**
А) Використання системи контрою і управління доступом;
Б) Використання оперативних методів роботи, оперативно-технічних засобів для вхідного контролю та періодичної перевірки лояльності персоналу;
В) Впровадження інтегрованих систем безпеки;
Г) Вірна відповідь відсутня.

**18. Перешкода – це …**
А) Метод фізичного перешкоджання шляху зловмиснику до захищеної інформації;
Б) Метод захисту інформації шляхом її криптографічного закриття;
В) Метод захисту інформації, який спонукає користувачів і персонал системи не порушувати встановлені правила за рахунок дотримання сформованих моральних і етичних норм;
Г) Вірна відповідь відсутня.

**19. Управління доступом – це …**
А) Метод фізичного перешкоджання шляху зловмиснику до захищеної інформації;
Б) Метод захисту інформації регулюванням використання всіх ресурсів автоматизованої інформаційної системи організації;
В) Метод захисту інформації, який спонукає користувачів і персонал системи не порушувати встановлені правила за рахунок дотримання сформованих моральних і етичних норм;
Г) Вірна відповідь відсутня.

**20. Регламентація – це …**
А) Метод фізичного перешкоджання шляху зловмиснику до захищеної інформації;
Б) Метод захисту інформації, що створює такі умови автоматизованої обробки, зберігання та передачі інформації, при яких можливість несанкціонованого доступу до неї зводилася б до мінімуму;

В) Метод захисту інформації регулюванням використання всіх ресурсів автоматизованої інформаційної системи організації;
Г) Всі відповіді вірні.

**21. Примус – це …**
А) Метод фізичного перешкоджання шляху зловмиснику до захищеної інформації;
Б) Принцип організації системи захисту ІБ;
В) Метод захисту інформації, при якому користувачі та персонал системи змушені дотримуватися правил обробки, передачі і використання інформації, що захищається під загрозою матеріальної, адміністративної чи кримінальної відповідальності;
Г) Всі відповіді вірні.

**22. Спонукання – це …**
А) Метод захисту інформації, який спонукає користувачів і персонал системи не порушувати встановлені правила за рахунок дотримання сформованих моральних і етичних норм.
Б) Метод фізичного перешкоджання шляху зловмиснику до захищеної інформації;
В) Метод захисту інформації, при якому користувачі системи змушені дотримуватися правил обробки, передачі інформації;
Г) Вірна відповідь відсутня.

**23. Апаратні засоби захисту – це …**
А) Різні електромеханічні та інші пристрої призначені для внутрішнього захисту структурних елементів засобів і систем обчислювальної техніки : терміналів, процесорів, периферійного обладнання, ліній зв'язку і т.д.;
Б) Засоби захисту, що призначені для зовнішньої охорони території об’єктів;
В) Засоби захисту, призначені для виконання логічних і інтелектуальних функцій захисту;
Г) Вірна відповідь відсутня.

## ТЕМА 8

**1. Відомості, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням відповідно до передбаченими ними умовами – це …**
А) Комерційна таємниця;
Б) Конфіденційна інформація;
В) Інформація конфіденційного характеру;
Г) Комерційна інформація.

**2. «Навмисне розголошення комерційної таємниці карається позбавленням волі на термін …» (ст. 232 ККУ)**

А) До 6 місяців;
Б) До 1 року;
В) До 2 років;
Г) До 5 років.

**3. Завдання системи безпеки інформації :**
А) Попередження і виявлення загроз;
Б) Локалізація злочинної діяльності і ліквідація наслідків;
В) Організаційно-технічні заходи захисту інформації;
Г) Правові заходи захисту інформації;
Д) Вірні відповіді А і Б;
Е) Вірна відповідь відсутня.

**4. До правових заходів забезпечення захисту інформації відносяться:**
А) Купівля та встановлення засобів захисту;
Б) Блокування ймовірних каналів витоку інформації;
В) Юридична регламентація використання методів і засобів захисту;
Г) Регламентація доступу і використання технічних засобів.

**5. Система організаційних заходів щодо захисту інформації являють собою комплекс заходів, що включають такі основні компоненти:**
А) Вивчення обстановки на об’єкті та розробку програми захисту;
Б) Діяльність з проведення зазначеної програми в життя та контроль за її дієвістю;
В) Організація секретного та КТ-діловодства;
Г) Організація надійної охорони приміщень;
Д) Вірні відповіді А і Б;
Е) Вірна відповідь відсутня.
**6. Елементи системи захисту інформації включає в себе регламентацію:**
А) Системи охорони території;
Б) Ведення всіх видів аналітичної роботи;
В) Дій персоналу в екстремальних ситуаціях;
Г) Всі відповіді вірні.

**7. Елементи системи захисту інформації бувають:**
А) Правовий, організаційний;
Б) Інженерно-технічний, криптографічний;
В) Програмно-апаратний;
Г) Вірні відповіді А і Б;
Д) Всі відповіді вірні.

**8. Розробка правил щодо захисту інформації передбачає знайти відповіді на запитання:**
А) Кому і в якому випадку може бути дано дозвіл на допуск інформації;
Б) Хто з керівників має право давати дозвіл на доступ і до яких відомостями;

В) В якому випадку надавати дозвіл на допуск інформації;
Г) Вірні відповіді А і Б;
Д) Вірна відповідь відсутня.

**9. Відповідно до Господарського кодексу України комерційну таємницю не складають :**
А) Документи про платоспроможність;
Б) Документи про сплату податків і обов'язкових платежів;
В) Відомості, що підлягають оголошенню, відповідно до діючого законодавства;
Г) Всі відповіді вірні;
Д) Вірні відповіді А, В.

**10. Дані, що складають комерційну таємницю:**
А) Інформація про ринок;
Б) Відомості про фінансову діяльність;
В) Відомості про штатний розпис;
Г) Вірні відповіді А і Б;
Д) Вірні відповіді А і В.

**11.Чотири рівні інформації, що складають комерційну таємницю:**
А) Життєво важлива, важлива, корисна, несуттєва;
Б) Надважлива, суттєва, несуттєва, корисна;
В) Некорисна, несуттєва, життєво важлива, вважлива;
Г) Вірна відповідь відсутня.

**12. До інформації про ринок, яка складає комерційну таємницю, входить:**
А) Канали і методи збуту;
Б) Програма реклами;
В) Ринкова політика і плани;
Г) Стан основних і оборотних фондів;
Д) Вірні відповіді А, Б і В;
Е) Вірні відповіді В і Г.

**13. Інформація, витік якої завдає матеріальної шкоди підприємству, однак вона може ефективно функціонувати й у випадку витоку цієї інформації – це …**
А) Несуттєва;
Б) Корисна;
В) Важлива;
Г) Життєво важлива.

**14. Конфіденційною інформація не може бути :**
А) Інформація комерційного і банківського характеру;
Б) Інформація, приховання якої створює загрозу життю і здоров'ю людей;

В) Інформація про основні фінансові показники діяльності підприємства.
Г) Вірні відповіді А і Б

**15. Конфіденційна інформація захищена :**
А) ЗУ «Про державну податкову службу»;
Б) Кодексом України про адміністративні правопорушення;
В) ЗУ «Про захист від недобросовісної конкуренції»;
Г) Господарським кодексом України;
Д) Всі відповіді вірні.

**16. До відомостей про наукові розробки, які складають комерційну таємницю входить:**
А) Нові алгоритми;
Б) Оригінальні програми;
В) Програми НДР;
В) Всі відповіді вірні;
Д) Вірні відповіді Б і В.

## ТЕМА 9

**1. Основними завданнями департаменту інформаційної безпеки є:**
А) впровадження різних засобів захисту інформації;
Б) контроль за виконанням встановлених вимог та оцінка ефективності роботи підрозділів і персоналу підприємства щодо забезпечення інформаційної безпеки;
В) адміністрування окремих інформаційних систем;
Г) всі відповіді вірні;
Д) вірні відповіді б і в

**2. Склад завдань департаменту інформаційної безпеки визначається такими особливостями функціонування підприємства, як:**
А) фінансовий стан підприємства; організація роботи та структура ІТ –служби;
Б) кількість інформації в організації;
В) ставлення підлеглих підприємства до питань інформаційної безпеки;
Г) вірна відповідь відсутня

**3. Функції, пов'язані з формуванням, підтримкою і документальним забезпеченням політики інформаційної безпеки підприємства, можуть включати в себе :**
А) самостійну розробку політики безпеки, її узгодження і подання її керівництву підприємства для затвердження, а також внесення необхідних змін у міру зміни умов роботи підприємства;
Б) управління навчанням персоналу компанії;
В) розробку техніко-економічного обґрунтування для проектів;
Г) вірні відповіді а, б

**4. Функції, пов'язані з адмініструванням інформаційних систем і систем захисту інформації можуть включати в себе :**
А) управління навчанням персоналу компанії;
Б) перевірку стану поточної господарської та кадрової документації;
В) установку (в тому числі і спільно з фахівцями IT-підрозділу) програмних і апаратних засобів захисту інформації на робочі місця користувачів і в інші елементи інформаційних систем;
Г) вірна відповідь відсутня

**5. Функції, пов'язані з впровадженням засобів захисту інформації можуть включати в себе:**
А) аналіз сучасних програмних і апаратних засобів захисту інформації та пов'язаних з ними методик захисту;
Б) управління навчанням персоналу компанії
В) розробку техніко - економічного обґрунтування для проектів впровадження засобів захисту інформації;
Г) вірні відповіді а, в

**6. Функції, пов'язані з контролем виконання вимог політики інформаційної безпеки та проведенням аудитів можуть включати в себе:**
А) збір та аналіз відомостей про порушення різних вимог політики безпеки;
Б) організацію контрольних перевірок захищеності окремих елементів інформаційних систем;
В) вірні відповіді а, б
Г) вірна відповідь відсутня

**7. Функцій, пов'язаних з охороною майна підприємства і вирішенням завдань, які пов'язані з забезпеченням безпеки підприємства у більш широкому сенсі –це:**
А) охорона території та майна підприємства;
Б) контроль за ввезенням на територію підприємства і вивезенням готової продукції, матеріалів, документів та іншого майна;
В) контроль за дотриманням тимчасового режиму роботи, а також за дотриманням правил внутрішнього розпорядку;
Г) всі відповіді вірні

**8. Співробітники департаменту інформаційної безпеки знаходяться в такому підпорядкуванні у керівника департаменту:**
А) адміністративному та управлінському;
Б) адміністративному та функціональному;
В) контрольне та управлінське;
Г) охоронному та функціональному

**9. У складі департаменту інформаційної безпеки можуть бути виділені самостійні групи (відділи) це**
А) відділ нормативної документації;
Б) відділ аудиту інформаційної безпеки;
В) відділ впровадження інформаційних систем і систем захисту інформації;
Г) всі відповіді вірні

**10. Відділ адміністрування інформаційних систем, а також відділ впровадження інформаційних систем і систем захисту інформації повинні включати в себе:**
А) фахівців з інформаційних технологій та засобів захисту інформації;
Б) фахівців з менеджменту та бізнес-аналізу;
В) фахівці з безпеки організації, юристи;
Г) вірна відповідь відсутня

**11. До цілей роботи з персоналом належить:**
А) навчання співробітників;
Б) соціальна підготовка співробітників;
В) досягнення взаєморозуміння керівників і співробітників в питаннях забезпечення інформаційної безпеки;
Г) вірні відповіді а, в

12. Методика психологічної оцінки підборі і розстановці кадрів включають в себе:
А) аналіз мотиваційних аспектів особистості;
Б) оцінку психологічної стійкості особистості;
В) оцінку активності особистості в досягненні поставленої мети, уміння об'єктивно оцінювати ситуацію і людей, вміння виробляти оптимальну стратегію поведінки;
**Г) всі відповіді вірні**

**13. Співробітник підприємства не може бути допущений до виконання своїх посадових обов'язків і роботі з інформаційними системами доти, поки він :**
А) детально не ознайомлений з усіма діючими на підприємстві вимогами і загальними правилами;
Б) повністю навчений методам і прийомам забезпечення інформаційної безпеки, необхідним для виконання його посадових обов'язків;
В) вірні відповіді а, б;
Г) вірна відповідь відсутня

**14. До числа психологічних схильностей та особливостей працівника можна віднести:**
А) нездатність адекватно оцінити небезпеку в деяких ситуаціях;
Б) специфічне ставлення до рідко відбувається подій;

В) надмірна довіра і покладання на засоби автоматизації;
Г) всі відповіді вірні

**15. Характерними способами того, як підприємство може постійно нагадувати своїм співробітникам про необхідність дотримуватися обережності, є:**
А) періодична розсилка відповідних брошур, бюлетенів та буклетів, а також повідомлень електронною поштою;
Б) використання голосової пошти і гучного зв'язку для періодичної передачі повідомлень про необхідність дотримання правил інформаційної безпеки;
В) особисто повідомляти кожного співробітника про дотримання правил безпеки;
Г) вірні відповіді а, б

## ТЕМА 10

**1. Під інцидентом розуміють:**
А) відхилення від нормального процесу використання інформаційних ресурсів та функціонування інформаційних систем, що спричинило збитки для певних інформаційних активів підприємства або безпосередньо створює загрозу нанесення такої шкоди;
Б) часте надходження хибних сигналів (помилкових або спеціально спровокованих) про деякі пригоди;
В) встановлення тієї інформації, яка була відома нападаючим до початку нападу і якій вони скористалися для здійснення цього нападу;
Г) вірна відповідь відсутня

**2. У загальному випадку організаційні процедури (регламенти) реагування на надзвичайні ситуації повинні включати в себе:**
А) ініціювання технічного переоснащення окремих ділянок інформаційної інфраструктури підприємства;
Б) регламенти альтернативних процесів обробки інформації;
В) визначення груп персоналу, відповідальних за виконання тих чи інших функцій у разі виникнення надзвичайної ситуації;
Г) вірні відповіді б, в;
Д) вірні відповіді а, б

**3. На етапі локалізації та усунення наслідків відбувається:**
А) визначення конкретних параметрів порушення;
Б) попередній аналіз дій порушника;
В) блокування дій порушника;
Г) всі відповіді вірні

**4. Припинення нападу і відновлення нормальної роботи інформаційних систем може зажадати скоординованих дій не тільки самих співробітників департаменту інформаційної безпеки, але й:**
А) фахівців ІТ-підрозділів, що відповідають за яких атакували інформаційні сервіси;
Б) підприємств-партнерів, що мають відношення до атакованим інформаційних ресурсів;
В) споживачів;
Г) вірні відповіді а, б;
Д) вірні відповіді б, в

**5. Ідентифікація нападника:**
А) є важливим кроком у процесі реагування, наступним безпосередньо за локалізацією **нападу;**
Б) відповідає за реагування на інциденти;
В) блокування дій порушника;
Г) вірні відповіді а і б
Д) вірні відповіді б, в

**6. Для виявлення джерела нападу необхідно:**
А) детально вивчити всі технічні аспекти нападу;
Б) провести якісний аналіз процесу нападу в контексті функціонування атакується системи захисту інформації;
В) відхилення від нормального процесу використання інформаційних ресурсів;
Г) вірні відповіді а,б
Д) вірні відповіді б, в

**7. Важливим завданням аналізу процесу нападу є:**
А) встановлення тієї інформації, яка була відома нападаючим до початку нападу і якій вони скористалися для здійснення цього нападу;
Б) регламентація альтернативних процесів обробки інформації;
В) визначення груп персоналу, відповідальних за виконання тих чи інших функцій у разі виникнення надзвичайної ситуації;
Г) ініціювання технічного переоснащення окремих ділянок інформаційної інфраструктури підприємства

**8. Другим важливим напрямком організаційної та аналітичної роботи при встановленні (ідентифікації) нападників, які вчинили напад ззовні, є:**
А) ініціювання технічного переоснащення окремих ділянок інформаційної інфраструктури підприємства;
Б) регламентація альтернативних процесів обробки інформації;
В) взаємодія з адміністраторами систем, з використанням яких було здійснено напад;
Г) вірна відповідь відсутня

**9. Одним із заключних кроків процесу реагування на інцидент є:**
А) блокування дій порушника;
Б) детально вивчити всі технічні аспекти нападу;
В) оцінка та аналіз процесу нападу і його обставин;
Г) вірна відповідь відсутня

**10. Результатом аналізу процесу нападу повинні бути висновки, які можуть послужити основою для організаційної роботи в різних напрямках:**
А) встановлення тієї інформації, яка була відома нападаючим до початку нападу і якій вони скористалися для здійснення цього нападу;
Б) ініціювання технічного переоснащення окремих ділянок інформаційної інфраструктури підприємства;
В) проведення додаткової роботи з персоналом підприємства;
Г) вірні відповіді а, б

**11. Усунення негативних наслідків нападу може включати в себе:**
А) зміну скомпрометованих паролів окремих користувачів;
Б) переустановку пошкоджених операційних систем, а також пошкодженого програмного забезпечення;
В) відновлення пошкодженої інформації ,як з раніше створених резервних копій, так і іншими способами;
Г) всі відповіді вірні;
Д) вірні відповіді б, в

**12. У процесі відновлення працездатності інформаційних систем на деякий час можуть бути задіяні такі платформи:**
А) резервні (альтернативні);
Б) апаратні;
В) програмні;
Г) всі відповіді вірні;
Д) вірні відповіді б, в

**13. Джерелом інформації про порушення є:**
А) повідомлення користувачів про відхилення в роботі інформаційних систем і поява явних негативних наслідків;
Б) детальне вивчення всіх технічних аспектів нападу;
В) вірні відповіді а і б;
Г) вірна відповідь відсутня

**14. Важливою складовою аналізу нападу є:**
А) резервні (альтернативні)платформи;
Б) програмні платформи;
В) оцінка збитку від події порушення інформаційної безпеки;
Г) вірна відповідь відсутня

**15. Негативний вплив позаштатної ситуації – це:**
А) втрата довіри до підприємства, що приводить до відтоку замовників, формуванням негативного іміджу підприємства і т. п.;
Б) зміна скомпрометованих паролів окремих користувачів;
В) передачу деяких відомостей про напад в засоби масової інформації;
Г) вірні відповіді б, в

## ТЕМА 11

**1. Аудит інформаційної безпеки це –**
А) комплексне (по можливості, вичерпним) дослідження всіх аспектів інформаційної безпеки (як технічних, так і організаційних) в контексті всієї господарської діяльності підприємства з урахуванням діючої політики інформаційної безпеки, об'єктивних потреб підприємства і вимог, що пред'являються третіми особами (державою, контрагентами тощо);
Б) процес виявлення, вимірювання, накопичення, аналізу, підготовки, інтерпретації та передачі інформації, що використовується управлінською ланкою для планування, оцінки і контролю всередині організації та для забезпечення відповідного підзвітного використання ресурсів;
В) облік господарських операцій, тобто подій, що відбуваються з активами, капіталом і зобов'язаннями;
Г) вірна відповідь відсутня

**2. До цілей аудиту інформаційної безпеки відносять:**
А) організація виробництва товарів і послуг з урахуванням попиту споживачів на основі ресурсів, що є;
Б) встановлення ступеня захищеності інформаційних ресурсів підприємства, виявлення недоліків та визначення напрямків подальшого розвитку системи захисту інформації;
В) стимулювання співробітників організації шляхом створення для них відповідних розумів труда і системи його сплати;
Г) вірні відповіді б і в

**3. Демонстрація надійності підприємства, його здатності виступати в якості сталого партнера, здатного забезпечити комплексний захист інформаційних ресурсів, що може бути особливо важливо при здійсненні операцій, що передбачають обмін конфіденційною інформацією, що має велику вартість (фінансовими відомостями, конструкторсько-технологічною документацією, результатами НДДКР і т п ) є одним із**
А) методів, що вирішуються при проведенні аудиту;
Б) визначень аудиту;
В) стратегічних завдань, що вирішуються при проведенні аудиту інформаційної безпеки та отриманні відповідного сертифіката;
Г) задач підприємства при виході на ринок

**4. Підприємство звертається за допомогою до зовнішніх аудиторів з метою:**
А) підвищення об'єктивності, незалежності та професійного рівня перевірки;
Б) розробка стратегії розвитку організації і реалізації товару;
В) отримання висновків про стан інформаційної безпеки та відповідно міжнародним стандартам від незалежних аудиторів;
Г) вірні відповіді а і в;
Д) вірні відповіді б і в

**5. Компанії, що спеціалізуються на проведенні аудитів, можуть здійснювати перевірки стану інформаційної безпеки на відповідність таким загальновизнаним стандартам і вимогам, як:**
А) ISO 15408 ; BSI \ IT ;
Б) COBIT; ЕОМ ;
В) UKAS; ФСТЕК ;
Г) вірна відповідь відсутня

**6. Перш ніж приступити до аудиту інформаційної безпеки, аудиторам (зокрема, якщо проводиться зовнішній аудит) необхідно:**
А) визначити, що в результаті має бути, а також перспективи розвитку підприємства;
Б) ознайомитися зі структурою підприємства, його функціями, завданнями та основними бізнес - процесами, а також з наявними інформаційними системами;
В) вивчити свою посадову інструкцію і спочатку, ще не приступивши до своїх обов'язків, обговорити з замовником всі пункти інструкції ;
Г) вірні відповіді а і б

**7. Одним з перших завдань комплексного аудиту є …**
А) визначити можливості відносно тривалого існування даного підприємства в постійно змінюваних умовах середовища існування;
Б) встановлення закономірностей взаємозв’язків між підприємствами, їхніми угрупованнями та умовами навколишнього середовища;
В) встановлення того, якою мірою діюча політика відповідає об'єктивним потребам даного підприємства в безпеці, чи можуть дії в рамках даної політики забезпечити необхідний рівень захищеності інформації та засобів її обробки, зберігання та передачі;
Г) виявити чинники, що сприяють комерційному успіху або перешкоджають йому

**8. Основна робота аудиторів у процесі збору інформації полягає у**
А) одержання прибутку і реалізація на цій основі, відповідно до законодавства, соціально-економічних інтересів членів трудового колективу підприємства, взаємовідносин з бюджетом і господарюючими партнерами-постачальниками, споживачами та ін ;

Б) складанні виробничої програми, набиранні кадрів, здійсненні управління виробничим процесом, реалізації виробленої продукції, відшкодуванні своїх витрати та отриманні прибутку;
В) вивченні фактично застосованих заходів щодо забезпечення захисту інформаційних активів підприємства;
Г) вірні відповіді а і б

**9. Одним з важливих напрямків аудиторської перевірки є**
А) пошук результативних методів управлінського впливу на персонал;
Б) контроль того, наскільки своєчасно і повно положення та вимоги політики безпеки та інших організаційних документів доводяться до персоналу підприємства;
В) вірні відповіді а і б;
Г) вірна відповідь відсутня

**10. Для встановлення того, наскільки підприємство здатне протидіяти внутрішнім загрозам можуть бути досліджені:**
А) розподіл функцій між різними співробітниками і мінімізація їх привілеїв, а також можливу наявність надлишкових прав у деяких користувачів та адміністраторів;
Б) стан безпеки підприємства за останні роки;
В) внутрішнього середовища для з'ясування сильних та слабких сторін організації підприємства ;
Г) усі відповіді вірні

**11. Перевірка стану фізичної безпеки інформаційної інфраструктури, як правило, включає в себе:**
А) перевірка працівників на предмет дотримання правил забезпечення економічної, інформаційної та фізичної безпеки;
Б) перевірку того, щоб найбільш важливі об'єкти інформаційної інфраструктури та системи захисту інформації розташовувалися в зонах (частинах будинків, приміщеннях), що мають пропускний режим, а також обладнаних камерами відеоспостереження та іншими засобами контролю;
В) організацію персоналу і призначення осіб, відповідальних за організацію гігієни і безпеки праці, а також за здійснення нагляду на підприємстві;
Г) документування, складання звітів та ознайомлення з ними працівників

**12. «Безпосереднє вивчення роботи окремих серверів, робочих станцій і мережевого устаткування відповідними технічними фахівцями, які можуть перевірити різні аспекти їх функціонування» відносять до:**
А) безпосереднього здійснення збору інформації та проведення обстеження аудиторами;
Б) підготовки аудиторського звіту та атестаційного висновку;
В) основних завдань менеджера;

Г) напрямків інструментального та технічного контролю

**13. Ведення журналів інформаційних систем і застосування інших інструментів збору та аналізу інформації, необхідних для забезпечення поточного контролю за дотриманням вимог інформаційної безпеки та своєчасного реагування на інциденти перевіряють**

А) на етапі підготовка аудиторського звіту та атестаційного висновку;
Б) у процесі нарахування податків;
В) у процесі аудиту;
Г) у процесі гарантування безпеки;

**14. Результати аналізу у процесі аудиту інформаційної безпеки можуть бути представлені як:**

А) у вигляді узагальнених коротких формулювань, що характеризують захищеність інформації підприємства (адресованих керівництву та власникам підприємства), так і у вигляді переліку конкретних зауважень і пропозицій, що відносяться до окремих ділянок роботи;
Б) планові калькуляції для нових видів продукції, як сума економічного ефекту від освоєння нової техніки, впровадження новітніх технологій, механізації й автоматизації виробництва;
В) у вигляді наступних основних кроків: Побудова моделі Визначення потреби у фінансуванні Розробка стратегії фінансування Аналіз фінансових результатів Формування і друк звіту;
Г) матричні (балансові) моделі, що дозволяють у найбільш компактній формі представити взаємозв'язок витрат і результатів виробництва ;

**15. Остаточним результатом аналізу та узагальнення даних, отриманих у процесі аудиту, є звіт (висновок), який може включати в себе:**

А) обробку, інтерпретацію та аналіз даних, побудова емпірично вивірених і обґрунтованих узагальнень, висновків, рекомендацій та проектів;
Б) висновок про ступінь відповідності політики безпеки підприємства та всього комплексу заходів щодо захисту інформації вимогам чинного законодавства та відомчих нормативних актів;
В) організація процесу навчання користувачів прийомам і правилам безпечного використання інформаційних систем;
Г) володіти необхідними програмними та апаратними засобами для вичерпної перевірки наявної у підприємства програмного і апаратного забезпечення

**Навчальне видання**

**КОПИТКО Марта Іванівна**
доктор економічних наук, доцент, доцент кафедри менеджменту
Львівського державного університету внутрішніх справ

# Менеджмент інформаційних ресурсів та інформаційна безпека підприємств.

Навчально-методичний посібник.

---

Видавництво ТзОВ «Ліга-Прес»

Підписано до друку 21.04.2016 р.
Формат 60×48 1/16. Спосіб друку – різограф.
Умов. др. арк. 6,76. Тираж 300 прим.
ПП «Марусич М.М.» тел.: 261-51-31

---