ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО
ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Дослідження способів протидії перехопленню інформації на об’єкті виробничої діяльності»

на здобуття освітнього ступеня магістра
зі спеціальності __125_____
Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____Ігор ДРИНКІН

Виконав: здобувач вищої освіти групи СЗДМ-62

_____ДРИНКІН Ігор___

Керівник: _____КОТЕНКО Андрій
к.т.н., доцент (ПРІЗВИЩЕ, Ім’я)

Рецензент: _____
к.т.н., доцент (ПРІЗВИЩЕ, Ім’я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Систем інформаційного та кібернетичного захисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри СІКЗ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

_____ДРИНКІНУ Ігорю Олеговичу_____
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Дослідження способів протидії перехопленню інформації на об'єкті виробничої діяльності».
Керівник кваліфікаційної роботи: КОТЕНКО Андрій, к.т.н., доцент.
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)

Затверджена наказом Державного університету інформаційно-комунікаційних технологій від «____» _____2023 р. №_____.

2. Строк подання кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
__Загрози витоку інформації на об'єкті виробничої діяльності.
__Система захисту інформації та активів підприємства, що існувала.
__Оцінити ризики втрати інформації та запропонувати способи протидії перехопленню інформації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1.__Дослідження способів витоку інформації._____
2.__Аналіз складу системи захисту, що існувала та пошук вразливостей._____
3.__Оцінка ризиків та розробка способів протидії перехопленню інформації зловмисником.

5. Перелік графічного матеріалу: _____Презентаційний матеріал на слайдах_____
_____

6. Дата видачі завдання _____15.10.2023 р._____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання четвертого розділу роботи		
6	Написання висновків по роботі		
7	Підготовка демонстраційних матеріалів		
8	Підготовка доповіді		

Здобувач вищої освіти _____ Ігор ДРИНКІН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Андрій КОТЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи містить: 80 стор., 15 рис., 7 табл, та 20 джерел.

Об'єкт дослідження – приватне підприємство з оборотним капіталом.

Предмет дослідження – методи та способи протидії перехопленню інформації зловмисником.

Мета роботи – проаналізувати сучасний стан системи захисту інформації в залежності від оборотного капіталу підприємства і ступені важливості захищаємої інформації та запропонувати ефективну модель протидії перехопленню інформації на об'єкті виробничої діяльності.

Методи дослідження: порівняльний аналіз, ймовірнісні методи, аналітичні методи.

В роботі дослідженні питання економічних ризиків втрати конфіденційної інформації на підприємстві від різних чинників, таких як: канали витоку інформації, людський фактор та неефективна система захисту інформації. На основі цих досліджень проведено якісний та кількісний аналіз економічної ефективності вкладання коштів у побудову комплексної системи захисту інформації на виділеному об'єкті.

Розроблено рекомендації покращення ступеню захисту з урахуванням застарілого обладнання та втрати ефективності захисту конфіденційної інформації з часом.

Галузь використання – захист інформації на об'єкті інформаційної діяльності.

Ключові слова: ЗАГРОЗА ІНФОРМАЦІЇ, ЕКОНОМІЧНИЙ РИЗИК, ВТРАТА ІНФОРМАЦІЇ, ПРОТИДІЯ, БІЗНЕС-ПРОЕКТ.

ABSTRACT

The text part of the master's qualification work contains: 80 pages, 15 figures, 7 tables, and 20 sources.

The object of research – private enterprise with working capital.

Subject of research – methods and ways to counteract the interception of information by an intruder.

Purpose – to analyze the current state of the information security system depending on the working capital of the enterprise and the degree of importance of the protected information and to propose an effective model for counteracting information interception at the production facility.

Research methods: comparative analysis, probabilistic methods, analytical methods.

The paper examines the economic risks of losing confidential information at an enterprise from various factors, such as information leakage channels, human factors and an ineffective information security system. On the basis of these studies, a qualitative and quantitative analysis of the economic efficiency of investing in the construction of a comprehensive information security system at a dedicated facility was carried out.

Recommendations for improving the degree of protection have been developed, taking into account outdated equipment and the loss of effectiveness of protecting confidential information over time.

Field of application – information protection at the object of information activity.

Keywords: INFORMATION THREAT, ECONOMIC RISK, INFORMATION LOSS, COUNTERACTION, BUSINESS PROJECT.

ЗМІСТ

ВСТУП

Інформація набуває певної ваги, тобто цінності в залежності від її змісту та актуальності. Зрозуміло, що будуть зловмисники, які зацікавлені в перехопленні та несанкціонованому одержанні такої інформації. Тому необхідно постійно захищати її.

Для надійного захисту комерційної інформації підприємства необхідно побудувати надійну системи захисту інформації на об’єкті інформаційної діяльності.

Тому в роботі основна увага приділялася аналізу загроз інформації та каналам витоку інформації, методам протидії та економічним аспектам.

На будь-якому підприємстві постає питання побудови комплексної системи захисту інформації, але фінансова сторона відіграє вирішальну роль, тобто потрібно раціонально витратити кошти для одержання максимально ефективного захисту інформації.

В роботі увага приділялася економічним ризикам втрати інформації та фінансовим збиткам, які несе підприємство у разі нападу або несанкціонованого перехоплення такої інформації.

Також слід зазначити, що вирішальну роль відіграють працівники, що мають постійний доступ до інформації з обмеженим доступом і від їх порядності залежатиме багато чого. Тому актуально розглянути вимоги до таких працівників та фахові навички, що дозволять надійно охороняти та працювати з такою документацією.

Окремо в дипломі наведено нормативно-правову базу в сфері захисту інформації в Україні.

1 КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

1.1 Загальні характеристики

Комплекс засобів захисту – сукупність програмних і технічних засобів, що створені для забезпечення захисту засобів обчислювальної техніки або автоматизованих систем від несанкціонованого доступу до інформації.

Комплексність захисту – принцип захисту, що передбачає заходи проти всіх небезпечних видів і засобів технічної розвідки.

Розвиток засобів комунікації й технологій обробки даних і їхнє впровадження піднімає питання про комплексну систему захисту інформації. Сучасний захист інформації – це пошук оптимального співвідношення між доступністю й безпекою. Або, інакше кажучи, це постійна боротьба з непорядними користувачами та інтелектом хакерів.

Комплексність захисту інформації – це означає:

- організація захисту від всіх видів можливих погроз;

- всі можливі способи й засоби захисних заходів;

- захист інформації повинен здійснюватися на всіх етапах життєвого циклу об'єкта, що захищається;

- захист інформації повинен бути безперервним.

На світовому ринку інформації прийнято розрізняти наступні основні сектори:

1. Сектор ділової інформації;

2. Сектор інформації для фахівців;

3. Сектор масової, споживчої інформації.

Питання, пов'язані із захистом інформації, представляються звичайно її власниками й трактуються дуже неоднозначно. Деякі стверджують, що захищати нема чого, тому що в них відсутні відомості, що становлять державну таємницю, тоді як інші, зайво покладаються на територіальну неприступність даних (виділені приміщення, охороняємо територія й т.д.), треті взагалі не хочуть про це замислюватися.

Від чого захищають інформаційні системи – мета комплексної системи захисту інформації:

1. Порушення функціонування (зупинка приведе до втрати або зниження доступності даних);

2. Перекручування або знищення (іншими словами втрата цілісності) даних;

3. Несанкціонований доступ до даних, тобто їхнє незаконне розголошення й копіювання.

Призначення комплексної системи захисту інформації.

Насамперед, хотілося б розвіяти міф про те, що відкриту інформацію захищати немає необхідності. Що відбудеться, якщо зловмисник знищить або, що гірше, спотворить наявну базу даних партнерів або, наприклад, підприємств регіону, то в такій ситуації, коли через труднощі визначення вірогідності інформації, можливо ненавмисне використання співробітниками організації даних, що не відповідає реальному положенню справ. Дана погроза є реальною й особливо гострою, якщо ресурс, на якому розміщена дана інформація, підключений до глобальної мережі (наприклад, Internet).

Тепер, коли визначено, що захищати, необхідно скласти список погроз і вразливостей системи. У цей список повинні в обов'язковому порядку ввійти несанкціонований доступ, витік інформації технічними каналами і так званий «людський фактор» (тому що при певному рівні захисту дешевше заплатити тому хто вже має доступ до автоматизованої системи або чимсь незадоволеному співробітникові, чим намагатися пробитися крізь захист).

Після цього потрібно скласти модель порушника, при цьому необхідно враховувати його кваліфікацію й початковий рівень доступу до інформації. На цьому етапі можна скласти карти доступу співробітників до захищених ресурсів. Перш ніж переходити до розгляду захисних дій, необхідно провести аналіз ризиків інформаційної системи.

Після всього сказаного вище необхідно визначити дії, що вживаються у відповідь на дії порушника. Крім того, варто визначити дії по маскуванню вразливостей системи й мінімізації погроз.

Тепер, коли ми визначилися, що і від кого і як необхідно захищати, треба підготувати дуже відповідальний документ, що називається «Політика безпеки на підприємстві». Даний документ повинен не тільки відповідати на всі попередні питання, але й описувати відповідальність співробітників за порушення своїх обов'язків у плані безпеки системи. Крім того, цей документ повинен бути затверджений керівництвом підприємства й обов'язково виконуватися всіма співробітниками.

На цьому етапі визначається розумний баланс організаційних і технічних заходів щодо захисту. Проробляються технічне рішення й комплекс організаційних заходів щодо захисту інформаційної системи.

У технічному рішенні можуть бути враховані засоби захисту від витоку технічними каналами, захист переданих даних і реєстрації користувачів у системі за допомогою засобів криптографії, додаткові засоби аутентифікації користувачів, устаткування резервного копіювання, засобів антивірусного захисту, реалізація фізичного захисту встаткування й т.д.

Методика захисту будь-яких ресурсів поза залежністю від наявності або відсутності грифа таємності абсолютно однакова. Відрізняються тільки набір обов'язкових мінімальних вимог.

Під захистом інформації в інформаційній системі мається на увазі, безперервне використання засобів і методів, вживання заходів і здійснення заходів з метою системного забезпечення необхідної надійності інформації, збереженої й оброблюваної з використанням засобів інформаційної системи.

Під об'єктом захисту розуміється такий структурний компонент системи, у якому перебуває або може перебувати підлягаючий захист інформації.

Можна виділити типи об'єктів інформаційної системи: інформаційні, ресурсні (програмно-апаратні), фізичні, користувальницькі, логічні.

Об'єкт захисту повинен відповідати наступним умовам:

- приналежність до того самого організаційного компонента інформаційної системи;

- участь у здійсненні тих самих функцій, пов'язаних з автоматизованою обробкою інформації в інформаційній системі;

- локалізація (обмеження) з погляду територіального розташування.

Виходячи зі структури інформаційної системи, до об'єктів захисту можна віднести:

- робочі станції користувачів інформаційної системи;

- робочі станції адміністраторів (мережі, системи захисту й т.д.);

- сервери (мережні, баз даних, доданки);

- апаратуру зв'язку (модеми, маршрутизатори);

- канали зв'язку (виділені, що комутуються);

- периферійні пристрої колективного користування (принтери);

- приміщення, пов'язані з автоматизованою обробкою інформації (місця установки встаткування, сховища машинних носіїв інформації й т.п.).

Розглядаючи інформаційну систему як об'єкт захисту, особливо звертають увагу на наступні характеристики:

- категорія оброблюваної в інформаційній системі інформації, вищий гриф таємності інформації;

- загальна структурна схема й состав інформаційної системи (перелік і состав устаткування, технічних і програмних засобів, користувачів, даних і їхніх зв'язків, особливості конфігурації й архітектури й т.п.);

- тип інформаційної системи (однокористувальницька або багатокористувальницька система, відкрита мережа, однорівнева або багаторівнева система й т.п.);

- обсяги основних інформаційних масивів і потоків;

- швидкість обміну інформацією й продуктивність системи під час рішення функціональних завдань;

- тривалість процедури відновлення працездатності після збоїв, наявності засобів підвищення надійності й живучості й т.п.;

- технічні характеристики використовуваних каналів зв'язку (пропускна здатність, типи кабельних ліній, види зв'язків з вилученими сегментами інформаційної системи й користувача й т.п.);

- територіальне розташування компонентів інформаційної системи, їхні фізичні параметри й т.п.;

- наявності особливих умов експлуатації й ін.

Всі ресурси інформаційної системи, що вимагають захисти, можна розділити на два класи:

1. Інформаційні ресурси – це дані, що зберігаються й оброблюються в інформаційній системі, також сюди відносять інформацію про настроювання апаратури, що входить в інформаційну систему, і інформацію про аутентифікацію користувачів, тобто їхні імена й паролі.

2. Системні ресурси – це все, на чому зберігаються або обробляються дані й канали передачі даних в інформаційній системі, сюди відносять всі комп'ютери, сервери й мережне встаткування.

Інформаційні ресурси підрозділяються на:

1. Дані обмеженого доступу, як утримуючих, так і не утримуючих відомостей про державну таємницю.

2. Відкриті дані, тобто інформація відкритого доступу.

Системні ресурси краще розділити на 3 класи (за ступенем значимості для безперебійного функціонування):

1. До 1-го класу варто віднести встаткування, що утворить основу інформаційної системи, і вихід його з ладу приведе до зупинки системи повністю. Або, одержавши доступ до його керування, зловмисник може одержати доступ до всієї переданої інформації, що зберігається, або до більшої її частини. Крім того, сюди ж необхідно віднести «прикордонне» устаткування (міжмережні екрани й маршрутизатори).

2. До 2-го класу варто віднести встаткування, вивід якого з ладу спричинить зупинку окремих частин системи. Або зловмисник може одержати доступ до деякої частини, переданої й інформації, що зберігається.

3. До 3-го класу варто віднести встаткування, на якому працюють кінцеві користувачі, і вихід його з ладу приведе тільки до переходу даного користувача на інше робоче місце. А одержання керування цим устаткуванням дасть можливість несанкціонованого доступу до даних, що зберігається й оброблюються на цьому встаткуванні й інформації доступної для даного користувача.

При виявленні технічних каналів витоку інформації необхідно розглядати всю сукупність комп'ютерного встаткування, що включає технічні засоби обробки інформації, кінцеві пристрої, сполучні лінії, розподільні й комутаційні пристрої, системи електроживлення, системи заземлення та інше. Варто враховувати також допоміжні технічні засоби й системи, такі як:

- устаткування відкритого телефонного зв'язку;
- факсимільного зв'язку;
- гучномовного зв'язку;
- системи охоронної й пожежної сигналізації;
- електрифікації;
- радіофікації;
- часофікації;
- електропобутові прилади й інші.

1.2 Об’єкт захисту та його характеристики

На рис. 1.1, наведена узагальнююча схема можливих каналів витоку й несанкціонованого доступу до інформації, оброблюваної в типовому одноповерховому офісі.

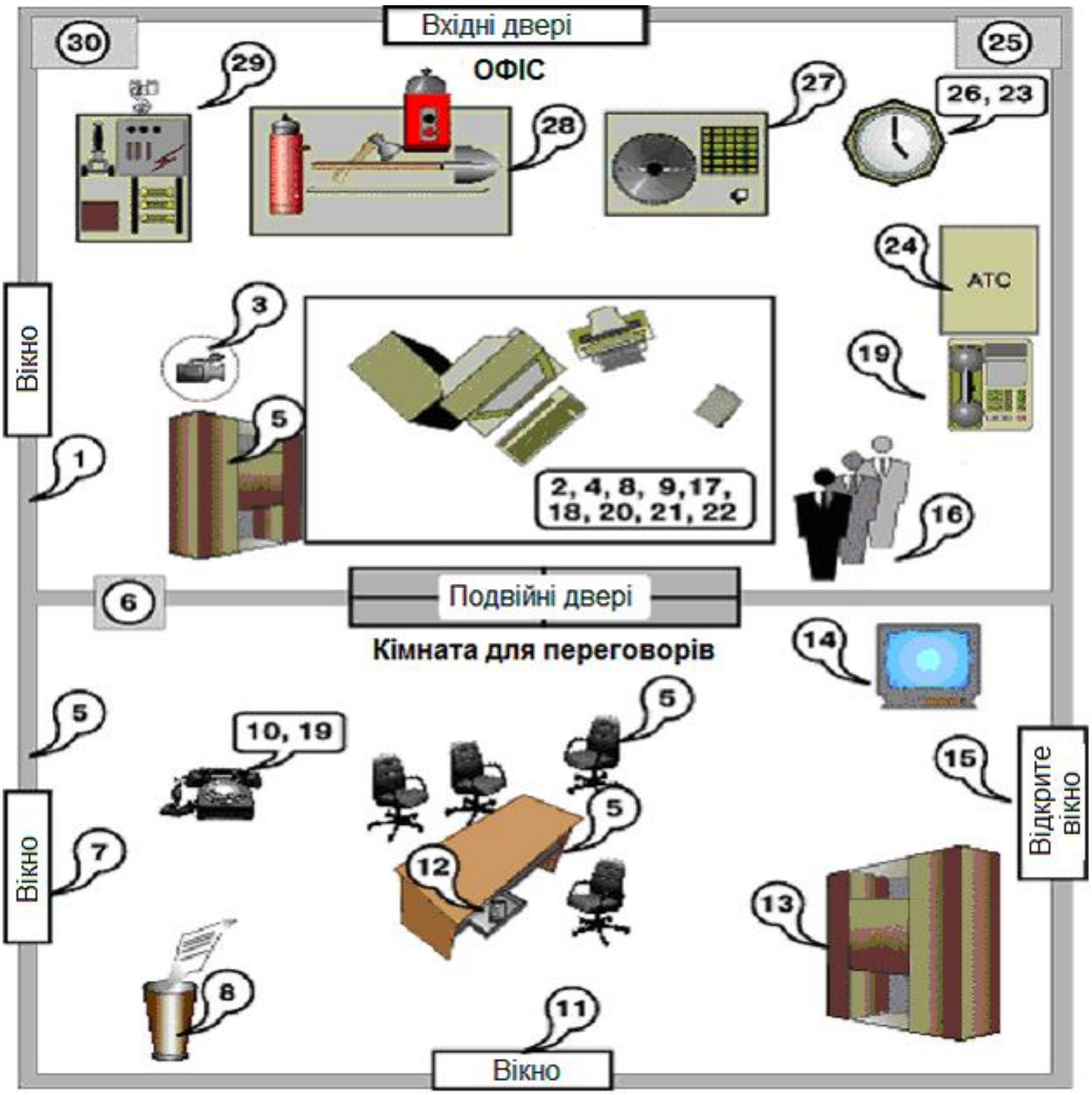

Рисунок 1.1 — Схема каналу витоку й несанкціонованого доступу до інформації в типовому одноповерховому офісі

На рис. 1.1 позначено:

1. Витік за рахунок структурного звуку в стінах і перекриттях;
2. Знімання інформації зі стрічки принтера, погано стертих дискет і т.п.;
3. Знімання інформації з використанням відео-закладок;
4. Програмно-апаратні закладки в комп’ютерах;
5. Радіозакладки в стінах і меблях;
6. Знімання інформації із системи вентиляції;

7. Лазерне знімання акустичної інформації з вікон;

8. Виробничі й технологічні відходи;

9. Комп'ютерні віруси, логічні бомби й т.п.;

10. Знімання інформації за рахунок наведень і "ВЧ-нав'язування";

11. Дистанційне знімання відеоінформації (оптика);

12. Знімання акустичної інформації з використанням диктофонів;

13. Розкрадання носіїв інформації;

14. ВЧ-канал витоку в побутовій техніці;

15. Знімання інформації спрямованим мікрофоном;

16. Внутрішні канали витоку інформації (через обслуговуючий персонал);

17. Несанкціоноване копіювання;

18. Витік за рахунок побічного випромінювання термінала;

19. Знімання інформації за рахунок використання "телефонного вуха";

20. Знімання із клавіатури й принтера по акустичному каналу;

21. Знімання з дисплею по електромагнітному каналу;

22. Візуальне знімання з дисплею й принтера;

23. Наведення на лінії комунікацій і сторонні провідники;

24. Витік через лінії зв'язку;

25. Витік по ланцюгах заземлення;

26. Витік по мережі електрогодинників;

27. Витік по трансляційній мережі й гучномовному зв'язку;

28. Витік по охоронно-пожежній сигналізації;

29. Витік по мережі електроживлення;

30. Витік по мережі опалення, газопостачання й водопостачання.

Серед каналів витоку помітну роль грають допоміжні засоби, що виходять за межі контрольованої зони, а також сторонні провідники, кабелі, металеві труби систем опалення, водопостачання й інші струмопровідні металоконструкції, що проходять через приміщення, де встановлені основні й допоміжні технічні засоби.

Необхідно відзначити, що акустичний канал може бути джерелом витоку не тільки мовної інформації. У літературі описані випадки, коли за допомогою статистичної обробки акустичної інформації із принтера або клавіатури вдавалося перехоплювати комп'ютерну текстову інформацію 20, у тому числі здійснювати знімання інформації із системи централізованої вентиляції 6.

До інших способів одержання необхідних даних можна віднести:

- аналіз відкритих джерел інформації;
- аналіз діяльності підприємств, його продукції, відходів і т.д.;
- шантаж;
- стеження.

Першорядними завданнями забезпечення безпеки інформації (рис. 1.2) є:

- захист інформації від витоку по акустичному каналу (АК).
- захист інформації від витоку по віброакустичному каналу (ВАК).
- захист інформації від витоку за рахунок електроакустичного перетворення (ЕАП);
- захист інформації від витоку за рахунок ВЧ-нав'язування (ВЧН);
- захист інформації від витоку по оптичному каналу (ОК).

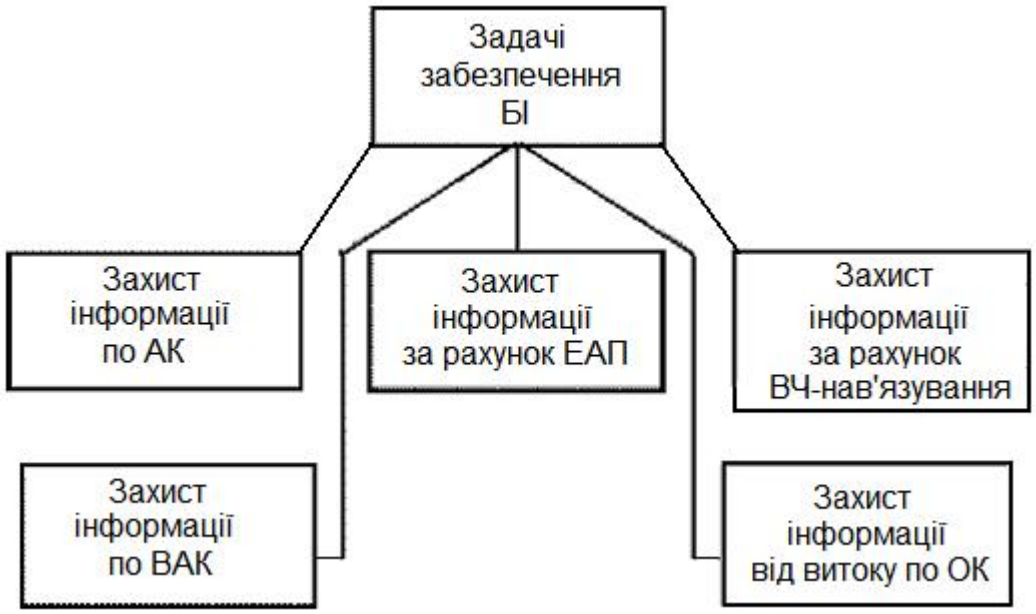

Рисунок — 1.2. Завдання забезпечення безпеки конфіденційної інформації

Основні методи одержання й захисту інформації наведені у табл. 1.1.

Таблиця 1.1

Основні методи одержання й захисту інформації

Типова ситуація	Канал витоку інформації	Методи й засоби	
		одержання інформації	захисту
Розмова в приміщенні й на вулиці	Акустичний	Підслуховування: диктофон, мікрофон, напівактивна система	Шумові генератори, пошук закладних пристроїв, захисні фільтри, обмеження доступу
	Віброакустичний	Стетоскоп, вібродатчик	
	Гідроакустичний	Гідроакустичний датчик	
	Акустоелектрон-ний	Спеціальні радіоприймачі	
Розмова по телефону:	Акустичний	Підслуховування (диктофон, мікрофон напівактивна система)	Ті ж
провідному	Сигнал у лінії	Паралельний телефон, пряме підключення, електромагнітний датчик, диктофон, телефонна закладка	Маскування, скремблювання, шифрування, спецтехніка
	Наведення	Спеціальні радіотехнічні пристрої	Спецтехніка
радіотелефону	ВЧ-сигнал	Радіоприймачі	Маскування, скремблювання, шифрування, спецтехніка
Документ на паперовому носії:	Безпосередньо документ	Крадіжка, прочитання, копіювання, фотографування	Обмеження доступу, спецтехніка
виготовлення	Продавлювання стрічки або паперу	Крадіжка, прочитання	Організаційно-технічні засоби
	Акустичний шум принтера	Апаратура акустичного контролю	Пристрою шумозаглушення
	Паразитні сигнали, наведення	Спеціальні радіотехнічні пристрої	Екранування
поштове відправлення	Безпосередньо документ	Крадіжка, прочитання	Спеціальні методи
Документ на не паперовому носії:	Носій	Розкрадання, копіювання, зчитування	Контроль доступу, фізичний захист, криптозахист

Продовження таблиці 1.1

виготовлення	Зображення на дисплеї	Візуальне, копіювання, фотографування	Контроль доступу, фізичний захист, криптозахист
	Паразитні сигнали, наведення	Спеціальні радіотехнічні пристрої	Контроль доступу, криптозахист, пошук закладок, екранування
	Електричний сигнал	Апаратні закладки	
	Програмний продукт	Програмні закладки	
передача документу по каналах зв'язку	Електричні й оптичні сигнали	Несанкціоноване підключення, імітація зареєстрованого користувача	Криптозахист
Виробничий процес	Відходи, випромінювання й т.п.	Спецапаратура різного призначення	Організаційно-технічні засоби, фізичний захист
Робота з вилученими базами даних	Сигнали, наведення	Програмні й апаратні закладки, несанкціонований доступ, комп'ютерні віруси	Криптозахист, спеціальне програмне забезпечення, організаційно-технічні засоби, антивірусний захист

Пошук каналів витоку інформації.

Пошук у конкретному приміщенні починається з огляду. Спочатку проводиться порівняння із планами, ідентифікація предметів меблів і інтер'єра. По можливості всі пристрої, що містять електроніку, повинні бути винесені із приміщення й обстежені окремо.

Під час огляду основне приділяється стороннім предметам. Ретельно оглядаються всі порожнини й щілини в плінтусах, підлогах і за батареями опалення, важкодоступних місцях на шафах, карнизах і т.п. Всі меблі відсуваються, виймається, і оглядаються ящики, внутрішні порожнини. Розкриваються й оглядаються електророзетки й вимикачі, розбирається електронна апаратура, проглядаються стояки, і виводи комунікації дотримуються правил безпеки роботи з електромережею – відключати електрощити, користуватися індикаторами мережі, гумовими рукавичками й

захисними килимами. Підготовка до пошуку може, здійснюється у звичайний робочий час із відповідним прикриттям.

Планомірно здійснювати розробку системи рекомендується проводити у відповідності з наступною методикою:

- аналіз об'єкта й ресурсів підмети до захисту;
- виявлення способів несанкціонованого доступу й канали витоку;
- складання моделі погроз і способів їхньої реалізації;
- вибір захисних заходів;
- аналіз ризику;
- формування політики безпеки;
- складання планів інженерно-технічних заходів комплексної системи захисту інформації;
- оцінка ефективності ухвалених рішень.

Аналіз ризику – процес визначення погроз безпеки системи в цілому й окремих її компонентах (тільки технічним), визначення характеристик погроз і потенційного збитку, що може бути нанесений у випадку їхньої реалізації.

1.3. Аналіз захищеності виділеного об'єкта

Захист виділеного приміщення – проведення комплексу організаційно-технічних заходів щодо запобігання витоку секретної мовної або конфіденційної інформації з технічних каналів за межі виділеного приміщення.

У загальним випадку комплекс заходів щодо захисту виділених приміщень включають: захист мовної інформації, оброблюваної технічними засобами від витоку за рахунок електромагнітних випромінювань; захист мовної інформації від витоку за рахунок ефекту електроакустичного перетворення допоміжних технічних засобів і систем; захист мовної інформації від витоку за рахунок лазерного зондування стекол або стетоскопічного прослуховування конструкцій, що обгороджують приміщення; захист мовної інформації від витоку за рахунок несанкціонованого доступу в приміщення й

сховану установку в ньому підслуховуючих приладів (мікрофонів, магнітофонів, радіопередавачів і т.д.); акустичний захист приміщення.

Захищеність – в обчислювальній техніці здатність системи протистояти несанкціонованому доступу до програм і даних (безпека, таємність), а також їхньому випадковому перекручуванню або руйнуванню (цілісності).

Необхідність в оцінки звичайно виникає при аналізі загальної ситуації з метою вибору стратегічних рішень при організації захисту інформації.

2 СПОСОБИ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

2.1 Причини перехоплення інформації

З огляду на відомий афоризм "ціль виправдує засоби", поставимо запитання: яку мету переслідує зловмисник, здійснюючи несанкціонований доступ до джерел конфіденційної інформації? У нових ринково конкурентних умовах виникає маса проблем, пов'язаних не тільки із забезпеченням схоронності підприємницької (комерційної) інформації, як виду інтелектуальної власності, але й фізичних і юридичних осіб, їхньої майнової власності й особистої безпеки. Відомо, що підприємницька діяльність тісно пов'язана з одержанням, нагромадженням, зберіганням, обробкою й використанням різноманітних інформаційних потоків. Як тільки інформація представляє певну ціну, то факт одержання інформації зловмисником приносить йому певний дохід, послабляючи тим самим можливості конкурента.

Звідси головна мета – одержання інформації про склад, стан і діяльність об'єкта конфіденційних інтересів (фірми, виробу, проекту, рецепта, технології й т.д.) з метою задоволення своїх інформаційних потреб. Можливо в корисливих цілях і внесення певних змін до складу інформації, що циркулює на об'єкті конфіденційних інтересів. Така дія може привести до дезінформації у певних сферах діяльності, обліковим даним, результатам рішення деяких завдань. Разом з тим слід зазначити, що внесення змін або дезінформацію важко здійснювати. Щоб видати помилкову інформацію за дійсну, необхідно передбачити комплекс соціальних заходів, погоджених із загальним ходом подій за часом, місцю, меті й змісту, що вимагає глибокого знання інформаційної обстановки на об'єкті. Окремі неправдиві відомості не завжди можуть дати позитивний ефект. Крім того, вони можуть повідомляти про розкриття намірів провести модифікацію або дезінформацію. Більш небезпечною метою є знищення накопичених інформаційних масивів у документальній або магнітній формі й програмних продуктів. Знищення – це

протиправні дії, спрямовані на нанесення матеріального або інформаційного збитку конкурентові з боку зловмисника. Таким чином, зловмисник переслідує три мети: одержати необхідну інформацію в необхідному для конкурентної боротьби обсязі й асортиментах; мати можливість вносити зміни в інформаційні потоки конкурента у відповідності зі своїми інтересами й, у крайніх випадках, завдати шкоди конкурентові шляхом знищення матеріальних і інформаційних цінностей. Повний обсяг відомостей про діяльність конкурента не може бути отриманий тільки яким-небудь одним з можливих способів доступу до інформації. Чим більшими інформаційними можливостями володіє зловмисник, тим більших успіхів він може домогтися в конкурентній боротьбі. На успіх може розраховувати той, хто швидше й повніше збере необхідну інформацію, переробить її й прийме правильне рішення. Від цілей залежить як вибір способів дій, так і кількісний і якісний склад приваблюваних сил і засобів зазіхання. Склад осіб, що добувають або забезпечують добування необхідної зловмисникові інформації може бути досить різноманітним. Це можуть бути інформатори, агенти (секретні співробітники), довірені особи, інформатори, стукачі й багато хто інші. Не виключається також впровадження "своїх" людей на конкуруючу фірму з метою рішення розвідувальних завдань. Для впровадження є два шляхи: перший – особа виступає під власним прізвищем і працює відповідно до наявної в нього професією; другий – особа працевлаштовується по підробленим документах, під прикриттям "легенди". Впровадження своєї людини на фірму складно, але на відміну від людини, що просто постачає інформацією зі своєї ініціативи, він більше надійний і легше керуємий. У вітчизняній літературі має місце різне тлумачення як поняття способу несанкціонованого доступу, так і його змісту.

Приведемо систематизований перелік шляхів несанкціонованого одержання інформації: застосування пристроїв, що підслухують, дистанційне фотографування, перехоплення електромагнітних випромінювань, розкрадання носіїв інформації й виробничих відходів, зчитування даних у масивах інших користувачів, читання залишкової інформації в системах пам’яті системи після

виконання санкціонованого запиту, копіювання носіїв інформації, несанкціоноване використання терміналів зареєстрованих користувачів за допомогою розкрадання паролів і інших реквізитів розмежування доступу, маскування несанкціонованих запитів під запити операційної системи (містифікація), використання програмних пасток, одержання даних, що захищаються, за допомогою серії дозволених запитів, використання недоліків мов програмування й операційних систем, навмисне включення в бібліотеки програм спеціальних блоків типу "троянських коней", незаконне підключення до апаратури й чи ліній зв'язку обчислювальної системи, злочинний вивід з ладу механізмів захисту.

Однієї із проблем захисту є класифікація можливих каналів витоку інформації. Під можливим каналом витоку інформації ми будемо розуміти спосіб, що дозволяє порушникові одержати доступ до оброблюваній або зберігаємої в комп’ютері інформації. До каналів витоку інформації відносять: розкрадання носіїв інформації (магнітних дисків, стрічок, дискет, карт); читання інформації з екрана сторонньою особою (під час відображення інформації на екрані законним користувачем або за відсутності законного користувача); читання інформації із залишених без догляду роздруківок програм; підключення до комп’ютерних пристроїв спеціально розроблених апаратних засобів, що забезпечують доступ до інформації; використання спеціальних технічних засобів для перехоплення електромагнітних випромінювань комп’ютерних технічних засобів; несанкціонований доступ програм до інформації; розшифровка програмою зашифрованої інформації; копіювання програмної інформації з носіїв.

Цікавий перелік способів одержання інформації про своїх конкурентів опублікував американський журнал "Chemical Engineering":

1. Збір інформації, що втримується в засобах масової інформації, включаючи офіційні документи, наприклад, судові звіти.

2. Використання відомостей, розповсюджуваних службовцями конкуруючих фірм.

3. Біржові звіти й звіти консультантів, фінансові звіти й документи, що перебувають у розпорядженні маклерів; виставочні експонати й проспекти, брошури конкуруючих фірм; звіти комівояжерів своєї фірми.

4. Вивчення продукції конкуруючих фірм; використання даних, отриманих під час бесід зі службовцями конкуруючих фірм (без порушення законів).

5. Замасковані опитування й "вивудження" інформації з працівників в конкуруючих фірм, на науково-технічних конгресах (конференціях, симпозіумах).

6. Безпосереднє спостереження, здійснюване потай.

7. Бесіди про наймання на роботу зі службовцями конкуруючих фірм (хоча опитувач зовсім не має наміру приймати дану людину на роботу у свою фірму).

8. Так звані "помилкові" переговори з фірмою-конкурентом щодо придбання ліцензії.

9. Наймання на роботу службовця конкуруючої фірми для одержання необхідної інформації.

10. Підкуп службовця конкуруючої фірми або особи, що займається її постачанням.

11. Використання агента для одержання інформації на основі платіжної відомості фірми-конкурента.

12. Підслуховування переговорів, що ведуться у фірмах-конкурентах.

13. Перехоплення телеграфних повідомлень.

14. Підслуховування телефонних переговорів.

15. Крадіжки креслень, зразків, документації й т.п.

16. Шантаж і вимагання.

З розглянутого можна визначити спосіб несанкціонованого доступу до джерел конфіденційної інформації як сукупність прийомів, що дозволяють зловмисникові одержати охоронювані відомості конфіденційного характеру. З урахуванням цього формулювання приведемо систематизований перелік

способів на високому рівні абстракції. Основні способи несанкціонованого доступу до конфіденційної інформації є:

1. Ініціативне співробітництво.
2. Відмова від співробітництва.
3. Випитування, вивідування.
4. Підслуховування переговорів різними шляхами.
5. Негласне ознайомлення з відомостями й документами.
6. Розкрадання.
7. Копіювання.
8. Підробка (модифікація).
9. Знищення (псування, руйнування).

Цей перелік є незалежними непересічним на обраному рівні абстракції. Погодившись із тим, що перелік джерел конфіденційної інформації також незалежний і не перетинаємий на даному рівні абстракції, можна спробувати провести аналіз їхнього взаємозв'язку й взаємозалежності. Навіть побіжний огляд дозволяє зрозуміти, що до певних джерел застосовні й певні способи. Як різноманітні джерела, так і різноманітні способи несанкціонованого доступу до них. Допускаємо можливість декомпозиції способів несанкціонованого доступу й джерел по їхній застосовності залежно від певних умов і ситуацій. Проте, маючи формальний набір джерел і способів несанкціонованого доступу до них, можливо на припустимому рівні абстракції побудувати формальну модель взаємозв'язку джерел і способів на якісному рівні з певним ступенем умовності. Таку модель можна було б назвати узагальненою для способів несанкціонованого доступу. Не вдаючись у сутність кожного несанкціонованого доступу на загальному рівні видно, що значна їхня частина застосовна до таких джерел, як люди, технічні засоби і документи. Інші, як би менш застосовувані по кількості охоплюваних джерел, ніяк не можна віднести до менш небезпечних. Ступінь небезпеки проникнення визначається не кількістю, а принесеним збитком. Таким чином, ми одержали певний

взаємозв'язок джерел і можливих способів доступу до них. Тепер розглянемо можливі реалізації способів несанкціонованого доступу.

2.2 Огляд методів одержання конфіденційної інформації

Методи одержання інформації приватного й комерційного характеру можна класифікувати по можливих каналах витоку:

1. Акустичний контроль приміщення, автомобіля, безпосередньо людини.

2. Контроль і прослуховування телефонних каналів зв'язку, перехоплення факсимільного і модемного зв'язку.

3. Перехоплення комп'ютерної інформації, у тому числі радіовипромінювань комп'ютера, несанкціоноване впровадження в бази даних.

4. Схована фото й відеозйомка, спеціальна оптика.

5. Візуальне спостереження за об'єктом.

6. Несанкціоноване одержання інформації про особистість шляхом підкупу або шантажу посадових осіб відповідних служб.

7. Шляхом підкупу або шантажу співробітників, знайомих, що обслуговує персоналу або родичів, що знають про рід діяльності.

Найбільш інформативними методами одержання конфіденційних відомостей з перерахованих вище є акустичний контроль і перехоплення переговорів у лініях зв'язку, причому обидва методи передбачають використання спеціальних технічних засобів несанкціонованого знімання інформації.

Акустичний контроль.

Для перехоплення й реєстрації акустичної інформації існує величезний штат засобів розвідки: мікрофони, електронні стетоскопи, акустичні закладки, спрямовані й лазерні мікрофони, апаратура магнітного запису. Набір засобів акустичної розвідки, використовуваних для рішення конкретного завдання, сильно залежить від можливості доступу агента в контрольоване приміщення або до осіб, що цікавлять.

У тому випадку, якщо є постійний доступ до об'єкта контролю, можуть бути використані найпростіші мініатюрні мікрофони, сполучні лінії які виводять у сусідні приміщення для реєстрації й подальшого прослуховування акустичної інформації. Такі мікрофони діаметром 2.5 мм можуть уловлювати нормальний людський голос із відстані до 20 м.

Якщо агенти не мають постійного доступу до об'єкта, але є можливість його короткочасного відвідування під різними приводами, то для акустичної розвідки використовуються мініатюрні диктофони й магнітофони закамуфльовані під предмети повсякденного побуту: книгу письмові прилади, пачку сигарет. Крім цього, диктофон може перебувати в одного з осіб, що є присутнім на закритій нараді. У цьому випадку часто використовують виносний мікрофон, захований під одягом або закамуфльований під годинники, авторучку, ґудзик.

Сучасні диктофони забезпечують безперервний запис мовної інформації від 30 хвилин до 7-8 годин, вони оснащені системами акустопуска (VOX, VAS), автореверса, індикації дати й часу запису, дистанційного керування. Прикладом такого диктофона може виступати модель OLYMPUS L-400, що обладнана всіма перерахованими вище системами. Як носій інформації крім магнітної стрічки використовуються цифрові мікрочипи й міні-диски.

У випадку якщо агентам не вдається проникнути на об'єкт навіть на короткий час, але є доступ у сусідні приміщення, то для ведення розвідки використовуються електронні стетоскопи, чутливим елементом яких є п’єзоелемент. Електронні стетоскопи підсилюють акустичний сигнал, що поширюється крізь стіни, підлогу, стелю в 20-30 тисяч разів і здатні вловлювати шорохи й цокання годинами через бетонні стіни товщиною до 1 м.

Поряд з диктофонами для перехоплення акустичної інформації використовуються акустичні закладки, несанкціоновані й потай установлювані в приміщеннях, автомашинах. Як канал передачі перехопленої інформації використовуються радіо й оптичний канали, силові, слабкострумові й знеструмлені комунікації.

Найбільше поширення одержали радіозакладки, які можна класифікувати по декількох критеріях:

1. По використовуваному діапазоні частот.

2. По потужності випромінювання: малопотужні – до 10 мВт, середньої потужності – від 10 мВт до 100 мВт, великої потужності – понад 100 мВт.

3. По виду використовуваних сигналів: простий сигнал (з AM, FM і WFM), складний сигнал (шумоподібні сигнали).

4. По способу модуляції: з модуляцією несучої, з модуляцією проміжної частоти.

5. По способу стабілізації частоти: нестабілізовані, зі схемотехнічною стабілізацією (м'який канал), із кварцовою стабілізацією (кварцовані).

6. По виконанню: у вигляді окремого модуля, закамуфльовані під різні предмети (авторучка, калькулятор, електротройник, дерев'яний брусок).

Термін служби радіозакладки сильно залежить від типу живлення. При використанні акумуляторних батарей час безперервної роботи – від декількох годин (авторучка – 2 години) до декількох діб (калькулятор – 15 діб). Якщо використовується зовнішнє живлення від телефонної лінії, електромережі, ланцюгів живлення побутової апаратури, то термін служби радіозакладок практично не обмежений. Радіозакладки забезпечують дальність передачі від десятків метрів (авторучка – 50 метрів) до 1 кілометра. При використанні ретрансляторів дальність передачі перехопленої інформації збільшується до десятків кілометрів. З метою підвищення скритності роботи радіозакладки обладнаються системами акустопуска, дистанційного керування, пакетної передачі, використовуються шумоподібні, скремблювання, шифровані сигнали.

Прийом інформації від радіозакладок здійснюється на широкосмуговий приймач-радіосканер, наприклад AR-8000 фірми або IC-R10.

Мережні закладки, що використовують як канал передачі інформації електромережу, установлюються в електророзетки, подовжувачі, побутову апаратуру або безпосередньо в силову мережу. Їхнім недоліком є мала дальність передачі (у межах одного будинку до трансформаторної підстанції).

Перевага мережної закладки – складність виявлення. Прийомна частина виконана у вигляді спецприймача.

Для перехоплення акустичної інформації з передачею по телефонній лінії використовується телефонне вухо. Після дозвону на абонентський номер за певною схемою агентові надається можливість прослуховувати приміщення навіть із іншого міста.

Контроль і прослуховування телефонних переговорів.

Прослуховування телефонних каналів зв'язку об'єкта в цей час є одним з основних способів одержання конфіденційної інформації. Знімання інформації з телефонної лінії зв'язку може здійснюватися або безпосереднім підключенням до лінії (у розрив або паралельно), або безконтактно за допомогою індуктивного датчика. Факт контактного підключення до лінії легко виявити, використання ж індуктивного підключення не порушує цілісності кабелю й не вносить зміни в параметри телефонної лінії.

Сигнали з телефонної лінії можуть записуватися на магнітофон (використовується спеціальний адаптер) або передаватися по радіоканалу.

Виконуються телефонні закладки у вигляді окремих модулів (брусок) або камуфлюються під елементи телефонного встаткування: адаптери, розетки, телефонні й мікрофонні капсулі, конденсатори. Телефонні закладки встановлюються безпосередньо в телефонний апарат, слухавку, розетку, а також безпосередньо на телефонну лінію. Передача інформації від телефонної закладки починається в момент підняття трубки абонентом.

Поряд з телефонними й радіозакладками використовуються комбіновані закладки, які при веденні телефонних переговорів здійснюють їхнє перехоплення, а по закінченні – автоматично перемикаються на перехоплення акустичної інформації.

2.3 Необхідність захисту інформації

Спроба заощадити на захисті інформації обходиться недешево. За даними опитування, проведеного Ernst&Young LLP, що зневажають захистом

інформації компанії зазнають незлічимих збитків від випадкових помилок, вірусів, а також вторгнень внутрішніх і зовнішніх хакерів.

Збиток, заподіюваний крадіжками грошей і встаткування, підрахувати неважко, але от виразити в доларах втрати, понесені у зв'язку зі злодійством комерційних секретів, навмисним видаленням або псуванням даних і збоями мережі, практично неможливо.

У випадку з компаніями-розроблювачами програмного забезпечення, їхньою основною перевагою є дослідження й розробка. Якщо буде украдена написана такою компанією програма, фірма розстанеться не тільки з вартістю проробленої роботи. Не можна не враховувати також майбутній дохід і судові витрати, які підуть на доказ факту крадіжки.

54 % з 1320 опитаних заявили, що протягом останніх двох років були випадки, коли вони зазнавали збитків, пов'язані зі зневагою захистом інформації й відновленням від збоїв. Якщо до двох вищезгаданих причин втрат додати ще й комп'ютерні віруси, то число потерпілих складе 78 % опитаних, причому три чверті з них не змогли оцінити обсягу своїх втрат.

Для проведення опитування Ernst&Young і InformationWeek розіслали анкети відповідальним співробітникам американських і канадських компаній, пов'язаним з інформаційними системами. Нижче наведені причини збитків і відсоток опитаних, потерпілих із цих причин.

Результати опитування показують, що багато керівників не піклуються належним чином про безпеку своїх компаній. У найкращому разі вони знають про уразливі місця, але нічого не вживають. Компаніям варто ввести в себе посаду адміністратора із захисту інформації.

Погроза може виникнути через незахищене з'єднання з Internet, злочині дій роздратованого чим-небудь працівника, втрати мобільного комп'ютера з відповідальною інформацією, промислового шпигунства або простої недбалості. У США промислове шпигунство переслідується законом, але в інших країнах такого немає.

З даних опитування видно, що електронна комерція здобуває популярність не настільки швидко, як очікувалося. Торік біля чверті опитаних користувалися Internet для ведення важливої ділової переписки, виконання роботи (у тому числі фінансових операцій і оплати рахунків) і замовлення продукції.

Близько 40 % виразили незадоволеність загальною захищеністю з'єднання їхньої компанії з Internet. Менш однієї третини опитаних уважають, що вони змогли б виявити наявність уразливих місць, які можуть атакувати хакери через Internet. 25 % респондентів стверджують, що за останній рік у мережу їхньої компанії були випадки проникнення ззовні через Internet.

Оскільки з ростом числа фірм-партнерів і службовців, найнятих за контрактом, небезпека збільшується, компаніям необхідно організувати моніторинг з'єднань між ними і їхніми постачальниками послуг. Керівництво компаній ще не усвідомило собі, що, надаючи комп'ютерний доступ службовцеві, найнятому за контрактом, вони вручають "ключ від скарбниці" випадковій людині, що навряд чи проробить у них довго.

Мета – це захист інформації. Основні причини збитків компаній, що зневажають захистом даних наведені в табл. 2.1.

Таблиця 2.1

Основні причини збитків компаній

Збитки через помилки, зроблених через недбайливість	65%
Віруси	63%
Непрацездатність системи	51%
Злочинні дії з боку компанії, що служить	32%
Злочинні дії людей, що не працюють у компанії	18%
Стихійні дії	25%
Невідомі причини	15%
Промислове шпигунство	6%

71 % не впевнені в захищеності своїх мереж. Наведемо 10 рад по захисту інформації:

1. Змусьте службовців, постачальників і найнятих за контрактом працівників підписати договір про нерозголошення.

2. Регулярно створюйте резервні копії інформації, що зберігається на мобільних комп'ютерах.

3. Встановіть правила завантаження в мобільні комп'ютери й використання інформації.

4. Забороніть користувачам залишати на робочих місцях пам'ятки, що містять ідентифікатори й паролі доступу в корпоративну мережу.

5. Забороніть залишати на корпусах мобільних комп'ютерів пам'ятки, що містять ідентифікатори й паролі, застосовувані для вилученого доступу.

6. Забороніть використовувати доступ до Internet не для ділових цілей.

7. Застосування пароля на завантаження комп'ютерів повинне бути обов'язковим для всіх.

8. Створіть класифікацію всіх даних по категоріях важливості й підсильте контроль над обмеженням доступу відповідно до неї.

9. Замикайте комп'ютери або у будь-який інший спосіб запобігайте доступу до всіх комп'ютерних систем по закінченні робочого дня.

10. Уведіть правило використання паролів доступу до файлів, що містять секретну або відповідальну інформацію.

2.4 Структура управління персоналом організацією

Можливі небезпечні канали витоку інформації, що підлягають захисту в організації приведені на рис. 2.1.

Організація системи захисту об'єкта від витоку інформації, як передбачено державними стандартами України в галузі технічного захисту інформації потребує складати окрему модель загроз. Формалізований опис технічних каналів витоку інформації є суттєвою складовою окремої моделі загроз і основою для розробки необхідних заходів захисту. Класифікація

каналів являє собою якісну модель сукупності матеріального об'єкту, що містить інформацію з обмеженим доступом, середовища її розповсюдження та засобів технічних розвідок. Декомпозиція каналів дає змогу зробити адекватний кількісний опис кожної з окремих складових каналу, провести їх дослідження як без заходів захисту інформації, так і з певним набором останніх. Наведене далі відкриває шлях до оцінки ефективності захисту від витоку інформації технічними каналами.

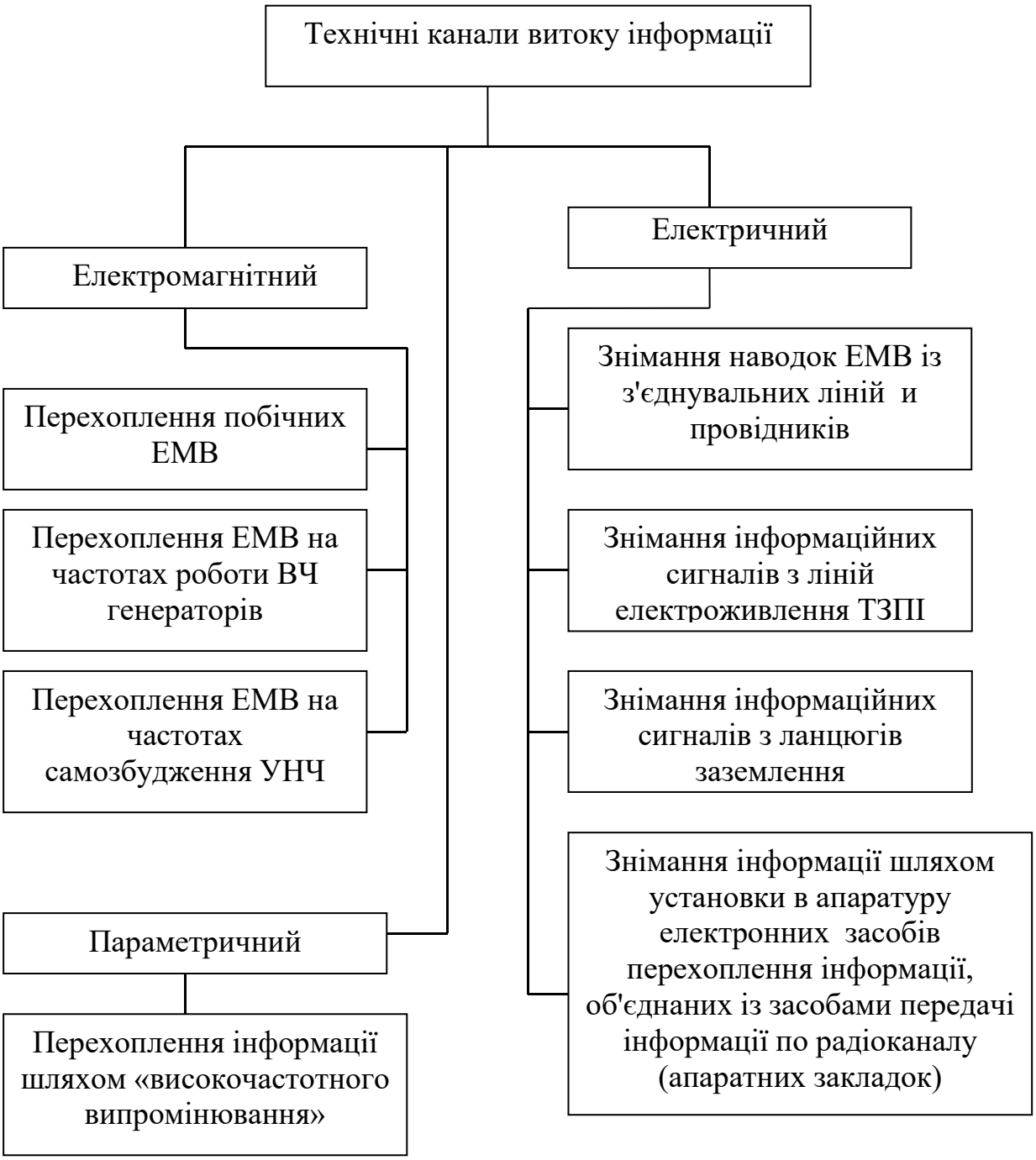

Рисунок 2.1 — Технічні канали витоку інформації

Аналіз змісту Положення про технічний захист інформації в Україні, дозволяє зробити висновки щодо існування двох взаємопов'язаних форм проявлення даних, що підлягають захисту від технічних розвідок: знакову та предметну.

Знакова форма являє сукупність символів, літер, цифр, звуків, які відображають предмети та явища реального світу у віртуальному світі. Носіями є документи на папері, магнітна, кіно-, відео-, фотоплівка, інші носії. Також інформація може зберігатися, відображатися або передаватися у вигляді інформаційних сигналів у формі фізичних полів (електромагнітних, оптичних, акустичних), електричних сигналів, вібраційних коливань у твердих предметах.

Предметна форма існування даних проявляється самими матеріальними об'єктами реального світу в процесі виробництва й застосування продукції різного призначення. Це електромагнітні, оптичні, гравітаційні, акустичні та інші поля й випромінювання, хімічні речовини.

Конкурентна боротьба вимагає добувати відомості як віртуального світу, так і реального: розвідувати інформацію і дані предметної форми існування. Надалі не розглядаються такі шляхи здобуття даних конкурентами, як несанкціоноване придбання або викрадення документів, зразків продукції тощо. Навпаки, приділяється увага аналізу механізмів добування відомостей за рахунок використання різноманітних засобів технічних розвідок.

Предмети та явища реального світу: продукція підприємств, вихідні комплектуючі та речовини, виробничі технології їх створення, способи застосування продукції в сучасному суспільстві, породжуються завдяки розробці й використанню комплектів документів, обговоренню цього безпосередньо вголос та в засобах зв'язку. При цьому віртуальний світ відображає реальний завдяки природним мовам (різних народів): вголос та письмово й штучним – кресленнями, кодами та символами, електричними сигналами та полями.

Джерелом утворення акустичного каналу витоку інформації є вібруючі, тіла й механізми, такі як голосові зв'язки людини, телефонні апарати, звукопідсилювальні системи й т.д. (рис. 2.2).

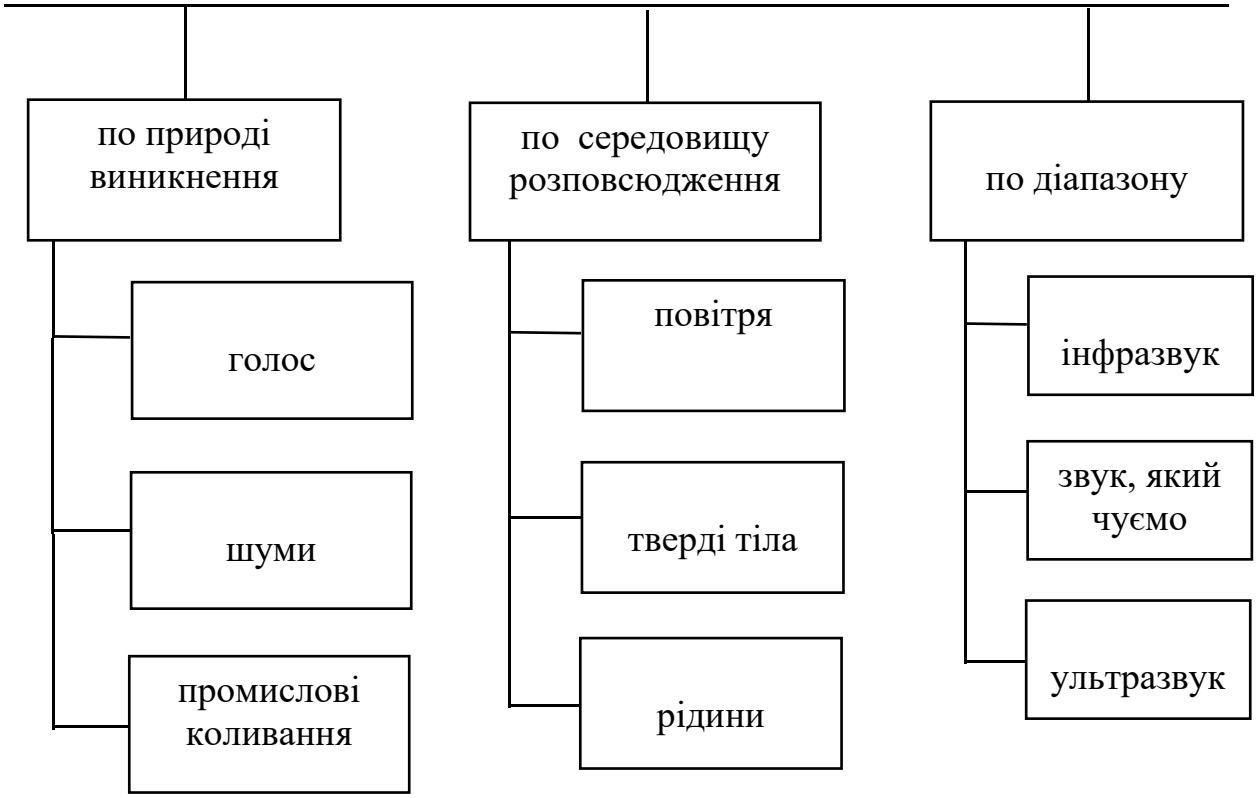

Рисунок 2.2 — Класифікація акустичних каналів витоку інформації

В умовах приміщень або інших обгороджених просторів на шляху звукових хвиль виникає кілька перешкод, на які хвилі утворюють змінний тиск (вікна, двері, стіни, стелі, підлоги й т.д.), приводячи їх у коливальний режим. Цей вплив звукових хвиль і є причиною утворення акустичного каналу витоку інформації.

Небезпека такого акустичного каналу витоку інформації по елементах будівлі складається у великій і неконтрольованій дальності поширення звукових хвиль, перетворених у пружні поздовжні хвилі в стінках і перекриттях, що дозволяє прослуховувати розмову на значних відстанях.

Акустичне розповсюдження сигналів можна показати у вигляді схеми, яка приведена на рис. 2.3.

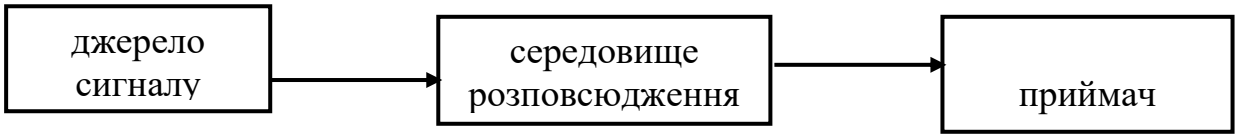

Рисунок 2.3 — Акустичне розповсюдження сигналів

За допомогою спеціальних технічних засобів можна несанкціоновано використовувати електромережу змінного струму 220 В, 50 Гц для перехоплення мовної інформації.

Часто використовуються радіозакладні пристрої, які мають високий рівень випромінювання за межі контролюємої приміщення. Радіозакладні пристрої мають дуже малий розмір, для зменшення можливості виявлення.

Найпростіші закладки не обладнані схемами дистанційного включення, функціонують протягом деякого часу. Пристрої з дистанційним включенням мають переривчастий режим роботи всунь і практично повне мовчання вночі. Також існують телефонні закладки, які вмикаються одночасно з підняттям трубки й призначені для безпосереднього витоку інформації.

На об'єкті інформаційної діяльності витік інформації може відбутися через наступні канали.

Акустичний канал може бути створений безпосереднім підслуховуванням розмов із-за недостатньої ізоляції стін та дверей, а також за рахунок проходження повітряних каналів системи вентиляції. Ще канал витоку може бути реалізований перехопленням мовних сигналів за допомогою портативних технічних засобів акустичної розвідки. Ці засоби технічної розвідки можуть використовувати спеціальні вмонтовані та виносні мікрофони.

Акусто-електричний канал може утворитися під впливом акустичного поля мови на технічні засоби за рахунок акустоелектричних перетворень в електричних схемах цих засобів і може бути створеним за рахунок поширення інформаційних сигналів дротовими лініями зв’язку, що володіють мікрофонним ефектом, а також інші електромагнітні випромінювання, модульовані мовним сигналом. Перехоплення засобами технічної розвідки інформаційних сигналів

ведеться із застосуванням радіоприймальних пристроїв елементів розвідки в діапазоні від одиниць Гц до одиниць ГГц.

Високочастотне нав'язування можливо реалізувати шляхом передачі високочастотного сигналу в провідні лінії, що виходять за межі контрольованої зони (телефонні лінії та лінії електроживлення) В основу методу покладено використання фізичного явища відбиття високочастотного сигналу від неузгоджених напруг.

Існує можливість утворення технічного каналу витоку мовної й видової інформації за рахунок несанкціонованого використання закладних пристроїв.

2.5 Режим роботи персоналу на об'єкті виробничої діяльності

Територія промислової зони, на якій знаходиться об’єкт має бетонну огорожу. Потрапити на територію промислового комплексу можна виключно через контрольно-перепускний пункт. Вхід на територія здійснюється лише за пропусками. Пропуски видаються усім працівникам комплексу. Особам, що не є працівниками комплексу, але проводять певні роботи, чи запрошені для здійснення певних заходів, видається тимчасовий пропуск.

Для нормального функціонування підприємства необхідно, щоб керівництво вело виважену кадрову політику, яку можна представити у вигляді схеми (рис. 2.4). Інструменти реалізації кадрової стратега підприємства

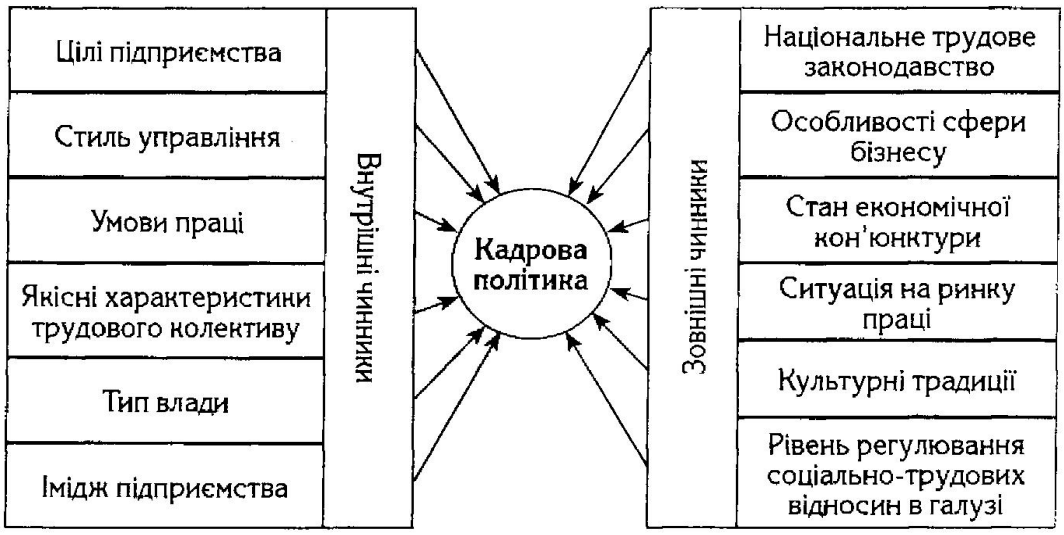

Рисунок 2.4 — Кадрова політика

Контрольно-перепускний пункт обладнаний караульним постом для охорони та телефоном для внутрішнього й зовнішнього зв'язку.

У неробочий година всі приміщення закриваються, ключі здаються охороні на прохідній, а також проводитися патрулювання території.

На вході в приміщення будівлі розміщена камера реєстрації працівників та відвідувачів.

Прохідний пункт, що знаходиться на при вході в будинок обладнаний терміналом контролю доступом. Термінал контролю доступу призначений для підключення двох унікальних номерів для зчитування проксіміті-карток, які є у кожного працівника, керування різними виконавчими пристроями: турнікетом у двох напрямках, двома електромеханічними виконавчими елементами, сиреною й т.д.

2.6 Заходи захисту інформації на підприємстві

Організаційний захист – це регламентація виробничої діяльності та взаємовідносин виконавців на нормативній основі, що виключає або суттєво ускладнює неправомірне оволодіння конфіденційною інформацією та прояву внутрішніх та зовнішніх загроз. Його можна представити у вигляді, що приведений на рис. 2.5.

Організаційний захист забезпечує:

- організацію режиму, охорони, роботові з кадрами, з документами;

- використання технічних засобів безпеки та інформаційно-аналітичну діяльність із виявлення внутрішніх і зовнішніх загроз діяльності компанії.

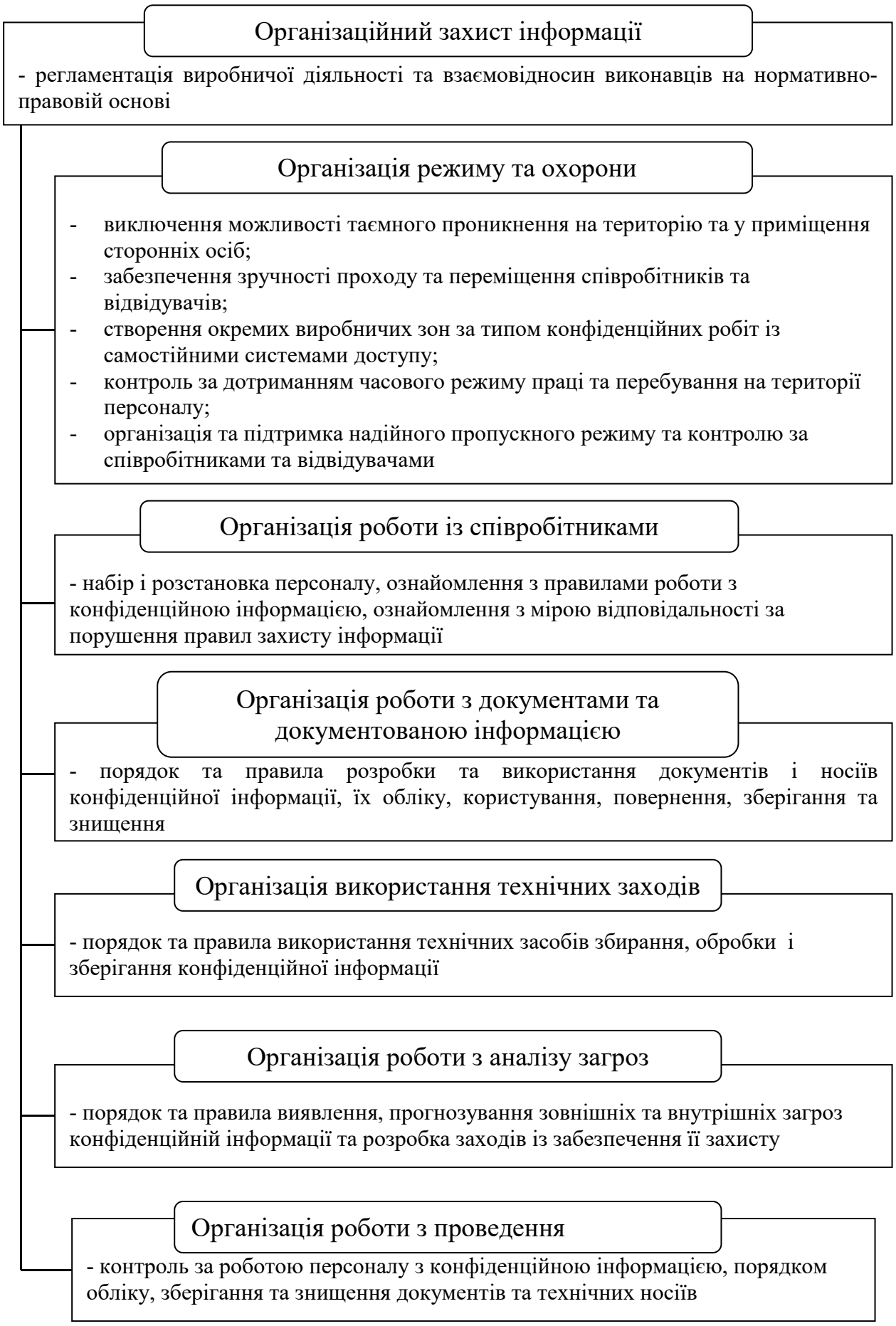

Рисунок 2.5 — Організаційний захист інформації

Організаційні заходи відіграють суттєву роль у створенні надійного механізму захисту інформації, оскільки можливості несанкціонованого використання конфіденційних відомостей у значній мірі обумовлюються не технічними аспектами, а зловмисними діями та недбалістю користувачів або персоналу. Впливу цих аспектів практично неможливо запобігти за допомогою технічних заходів. Для цього необхідна сукупність організаційно-правових і організаційно-технічних заходів, які вилучали б (або зводили до мінімуму) можливість виникнення небезпеки конфіденційності інформації.

До основних організаційних заходів відносять наступні:

1) організація режиму та охорони їх позначка:

- виключення можливості таємного проникнення на територію та в приміщення сторонніх осіб;

- забезпечення зручності проходу та переміщення співробітників та відвідувачів;

- створення окремих виробничих зон за типом конфіденційних робіт із самостійними системами доступу;

- контроль та дотримання вартового режиму праці та перебування на території персоналу підприємства;

- організація та підтримка надійного пропускного режиму та контролю співробітників і відвідувачів і т. ін.;

2)організація роботи із співробітниками, яка передбачає підбір і розстановку персоналу, включаючи ознайомлення із співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з мірою відповідальності за порушення правил захисту інформації;

3)організація роботи з документами та документованою інформацією, включаючи організацію розробки та використання документів і носіїв конфіденційної інформації, їх облік, використання, повернення, зберігання та знищення;

4)організація використання технічних засобів збирання, обробки,

нагромадження та зберігання конфіденційної інформації;

5)організація роботи з аналізу внутрішніх та зовнішніх загроз конфіденційній інформації та розробка заходів із забезпечення її захисту;

6)організація роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів та технічних носіїв.

У конкретному випадку організаційні заходи носять специфічну для даної організації форму та зміст, які спрямовані на забезпечення безпеки інформації в конкретних умовах.

Застосування організаційно-технічних заходів запобігає значній частині загроз безпеці інформації й блокує їх та поєднує в єдину систему всі заходь захисту. Організаційні заходи включають:

- визначення технологічних процесів обробки інформації;

- обґрунтування та вибір завдань захисту;

- розробку та впровадження правил реалізації заходів З;

- визначення та встановлення обов’язків підрозділів і осіб, що беруть доля в обробці інформації;

- вибір засобів забезпечення;

- оснащення структурних елементів автоматизованих систем нормативними документами і засобами забезпечення;

- встановлення порядку впровадження засобів обробки інформації, програмних і технічних засобів захисту інформації та контролю їх ефективності;

- визначення зон безпеки інформації;

- обґрунтування структури та технології функціонування систем;

- розробка правил та порядку контролю функціонування систем захисту;

- встановлення порядку проведення атестації технічних засобів та систем обробки інформації, систем зв'язку та передачі даних, технічних засобів та систем, що розташовані в приміщеннях, де вона циркулює, приміщень для засідань, а також усієї автоматизованої системи у цілому на відповідність вимогам безпеки інформації.

Організаційні заходь щодо захисту інформації полягають у розробці й реалізації адміністративних та організаційно-технічних заходів при підготовці та експлуатації системи, методів відбору всіх працівників (рис. 2.6).

Організаційні заходи щодо захисту системи в процесі її функціонування та підготовки до нього охоплюють рішення та процедури, які приймаються керівництвом організації – користувачем системи. Хоч деякі з них можуть визначатися зовнішніми факторами, наприклад законами або урядовими постановами, більшість проблем вирішується в самій організації в конкретних умовах.

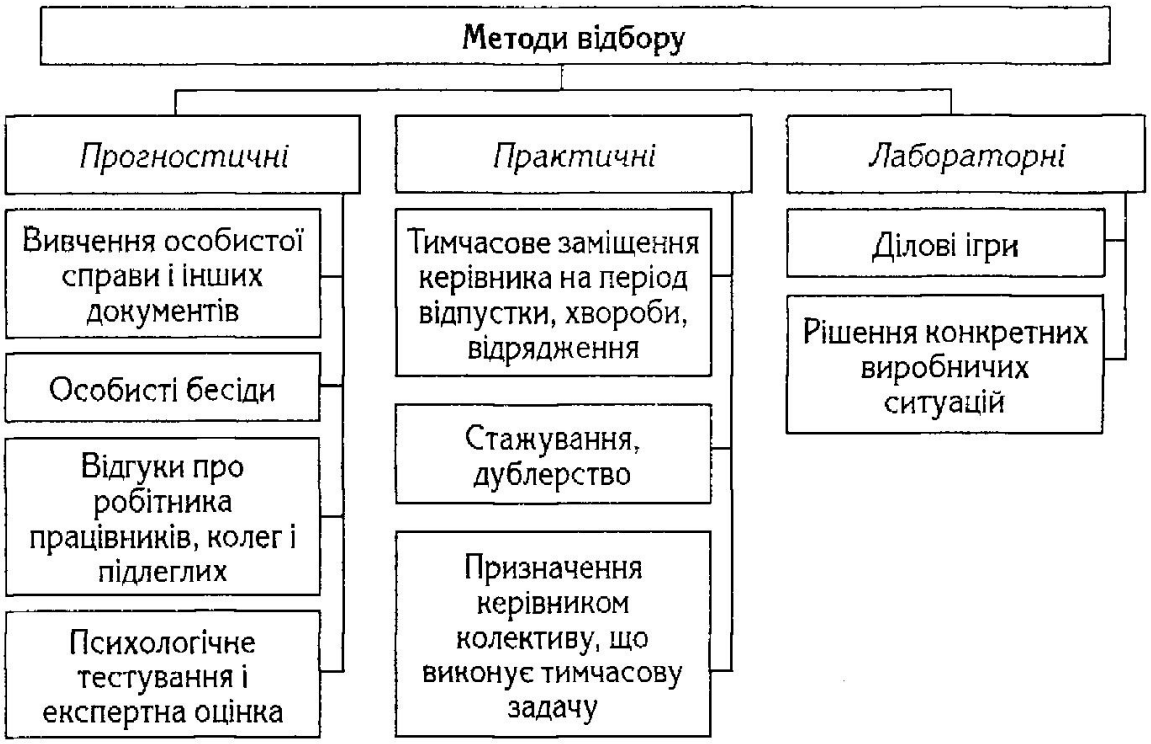

Рисунок 2.6 — Структура типового оперативного плану роботи з персоналом підприємства

Складовою будь-якого плану заходів захисту має бути чітке визначення цілей, розподіл відповідальності та перелік організаційних заходів захисту. Конкретний розподіл відповідальності та функцій щодо реалізації захисту від одної організації до іншої може змінюватися, але ретельне планування й точний розподіл відповідальності є необхідними умовами створення ефективної та життєздатної системи захисту.

Організаційні заходь щодо захисту інформації охоплюють наступні етапи:

- проектування;
- розробка;
- виготовлення;
- випробування;
- підготовки до експлуатації;
- експлуатації системи;
- виведення з експлуатації.

Відповідно до вимог технічного завдання організація-проектувальник поряд з технічними заходами та способами розробляє організаційні заходи на етапі створення системи. Під етапом створення розуміється проектування, розробка, виготовлення та випробування системи. При цьому слід чітко розрізняти заходь щодо захисту інформації, які проводяться організацією-проектувальником і розраховуються на захист від витоку в даній організації, і заходи, що закладаються в проект та документацію на систему й торкаються принципів організації захисту в самій системі. Саме з їх випливають необхідні організаційні заходи щодо захисту інформації. До організаційних заходів щодо захисту інформації у процесі створення системи відноситься:

- проведення на необхідних ділянках робіт з режимом секретності;
- розробка посадових інструкцій щодо забезпечення режиму секретності відповідно до чинного законодавства;
- виділення в разі споживи окремих приміщень з охоронною сигналізацією та пропускною системою;
- розмежування завдань між виконавцями щодо випуску документації;
- присвоєння грифів секретності матеріалам та документації і збереження їх під охороною у виділених приміщеннях з урахуванням та контролем доступу виконавців;
- постійний контроль за дотриманням виконавцем режиму та відповідних інструкцій;
- встановлення і розподіл відповідальних осіб за витік інформації;

- інші заходи, що встановлюються в конкретних системах.

У процесі підготовки системи до експлуатації з метою захисту інформації необхідно:

- при виділенні території, будинків та приміщень визначити контрольовану зону навколо об’єктів інформаційної діяльності;

- встановити охоронну сигналізацію в межах контрольованої зони;

- створити контрольно-пропускну систему;

- перевірити схеми розміщення та місця установки об’єктів;

- перевірити стан системи життєзабезпечення людей, функціонування системи та збереження документації;

- підібрати кадри для обслуговування об’єктів, їх захисту і створити централізовану службу безпеки при керівництві;

- провести навчання кадрів;

- організувати розподіл функціональних обов’язків і відповідальності посадових осіб;

- встановити повноваження посадових осіб щодо доступу до об’єктів та інформації;

- розробити посадові інструкції щодо виконання функціональних обов’язків персоналу всіх категорій, включаючи службу безпеки.

З точки зору способів реалізації основні організаційно-технічні заходи щодо створення й підтримки функціонування системи захисту інформації включають:

- одноразові заходи (проектування системи, створення системи захисту інформації, розробка нормативних документів, створення служби безпеки та інше);

- заходи, що проводяться при виникненні певних змін у самій системі, яка захищається, або зовнішньому середовищі (у разі ремонту, модифікації, кадрові зміни та інше);

- періодичні заходи (розподіл паролів, ключів шифрування, аналіз системних журналів тощо);

- постійні заходи (контроль за роботою персоналу, підтримка функціонування систем З, забезпечення фізичного захисту тощо).

У процесі експлуатації системи здійснюється централізований контроль доступу до інформації за допомогою технічних та організаційних заходів.

Інженерно-технічні заходи.

Інженерно-технічний захист – це сукупність спеціальних органів, технічних засобів та заходів для їхнього використання в інтересах захисту конфіденційної інформації (рис. 2.7).

Основне завдання інженерно-технічного захисту – це попередження розголошення, витоку, несанкціонованого доступу та інших форм незаконного втручання в інформаційні ресурси.

Різноманітність цілей, завдань, об'єктів захисту та заходів, що проводяться, передбачають розгляд деякої системи класифікації засобів інженерно-технічного захисту за видом, орієнтацією та іншими характеристиками.

Наприклад, засоби інженерно-технічного захисту можна класифікувати за об'єктами впливу, характером заходів, способами реалізації, масштабом охоплення, класом засобів зловмисників, яким здійснюється протидія з боку служби безпеки.

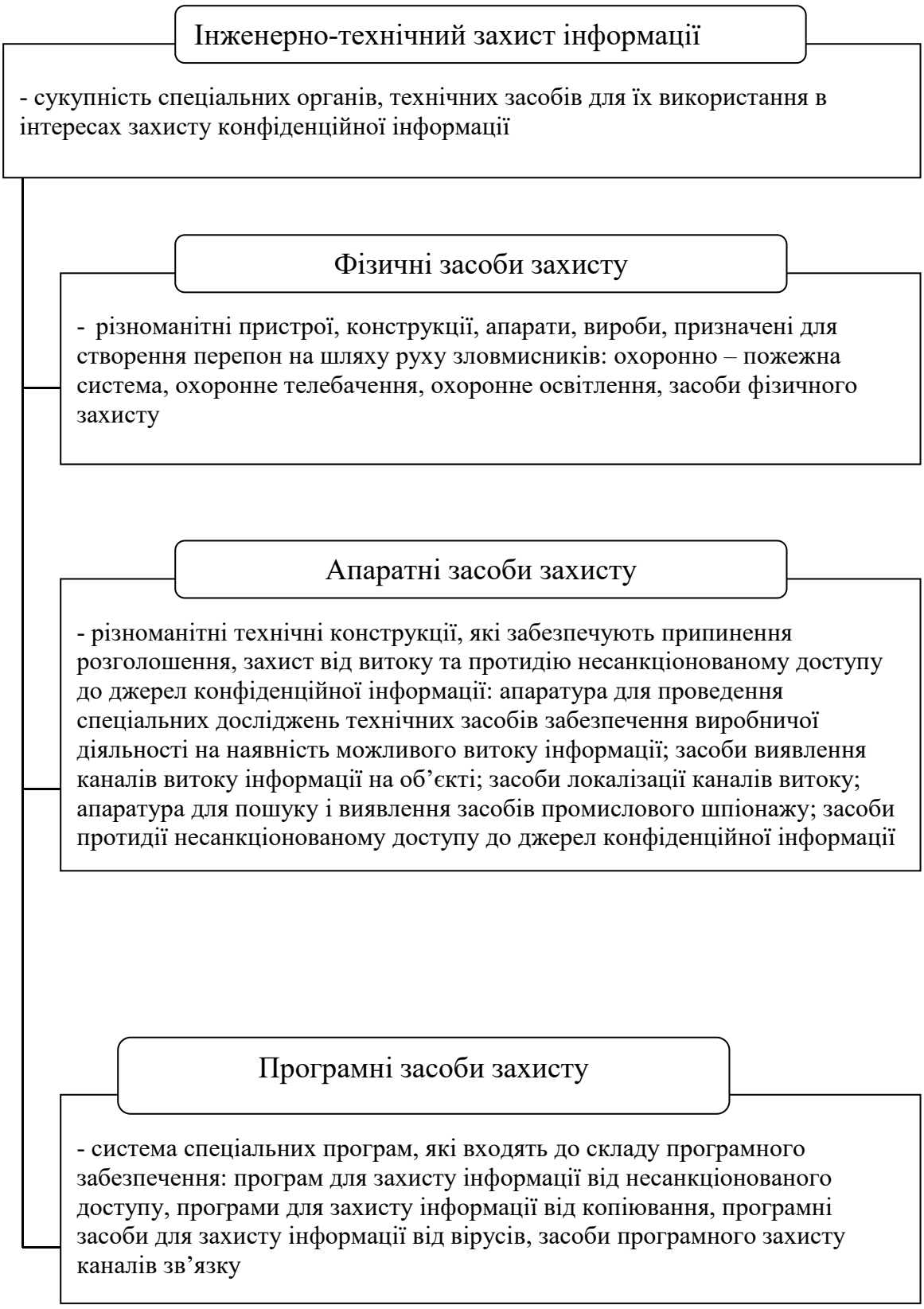

Рисунок 2.7 — Інженерно-технічний захист інформації

За функціональним призначенням засоби інженерно-технічного захисту поділяються на наступні групи: фізичні засоби захисту, апаратні засоби захисту, програмні засоби захисту, криптографічні засоби захисту.

Фізичні засоби включають різноманітні пристрої та споруди, які перешкоджають фізичному проникненню (або доступу) зловмисників на об'єкти захисту та матеріальних носіїв конфіденційної інформації та здійснюють захист персоналу, матеріальних носіїв, фінансів та інформації від протиправних дій.

До апаратних засобів відносяться прилади, пристрої, та інші технічні рішення, які використовуються в інтересах захисту інформації. Основне завдання апаратних засобів – забезпечення стійкого захисту від розголошення, витоку й несанкціонованого доступу через технічні засоби забезпечення діяльності організації (підприємства).

Програмні засоби охоплюють спеціальні програми, програмні комплекси та системи захисту інформації в інформаційних системах різноманітного призначення та засобах обробки (збирання, нагромадження, зберігання, обробки та передачі) даних.

Криптографічні засоби – це спеціальні математичні та алгоритмічні засоби захисту інформації, що передається системами та мережами зв'язку, зберігається та обробляється на комп’ютері із використанням різноманітних методів шифрування.

Апаратні методи та засоби захисту знайшли достатньо широке розповсюдження. Проте із-за того, що смороду не мають достатньої гнучкості, часто втрачають свої захисні властивості при розкритті принципу їхньої дії й у подальшому не можуть бути використані.

Програмні методи та засоби більш надійні, період їхнього гарантованого використання значно більший, ніж апаратних методів та засобів.

Криптографічні методи та засоби займають важливе місце і є надійним засобом забезпечення захисту інформації на тривалі періоди.

Очевидно, що такий поділ засобів захисту інформації достатньо умовний, оскільки на практиці дуже часто вони взаємодіють і реалізуються у вигляді програмно-апаратних засобів із широким використанням алгоритмів закриття інформації.

Для захисту комп'ютерної техніки застосовуємо: блок безперебійного живлення.

Для того, щоб уникнути витоку інформації через допоміжні технічні засоби (сигнальних ліній мережі Ethernet, кабелів телефонного зв'язку, ліній мережі електроживлення, системи пожежної сигналізації), необхідно використовувати екрановані кабелі. У якості кабелів, по яких передається найбільш важлива інформація, доцільно використовувати екрановану віту пари.

Переговорний пристрій, проводовий телефон та радіотелефон. Для того, щоб уникнути вищезгаданих загроз для цих пристроїв, необхідно використовувати різноманітні глушники, які б перешкоджали перехопленню інформації варто було б використовувати сертифіковані пристрої, у яких є захист від перехоплення інформації. Комплексний захист телефонних ліній від прослуховування за допомогою різних засобів знімання акустичної інформації шляхом формування в телефонну лінію маскуючих сигналів. Блокування несанкціонованого підключення паралельного телефону й сигналізація "піратського" підключення. Виконує роль скремблювання звукового сигналу з метою його захисту від прослуховування за межами контрольованої території методом гальванічного підключення або безконтактного знімання інформації за рахунок випромінювання самого кабелю).

Для захисту від прослуховування розмов у приміщеннях за допомогою провідних мікрофонів, стетоскопів, мережених передавачів, лазерних та інфрачервоних віконних статоскопів використовуємо генератора шуму, який призначений для генерації звукових коливань у стінах, стелях, вікнах, перегородках, витяжках.

Для фіксації факту розбиття віконного скла, використовуємо детектор розбиття скла.

Для захисту периметру приміщення використаємо комбінований сповіщувач.

У якості пожежних сповіщувачів використовуємо димовий сповіщувач.

Для контролю доступу на об'єкт використовуємо замки на відбитки пальців.

У якості системи передачі сповіщень використаємо систему, яка являє собою класичну систему централізованого спостереження. І може працювати як з кабельною системою, так і на радіочастотах. Тип зв'язку – односторонній.

У якості центральної системи використовується інтегрована система захисту: комплекс ”Кодос”, до якої підключені вище згадані пристрої й системи.

У якості постійної авторизації користувачів у мережі використовуємо систему „SecureCard”, яка дозволяє використовувати смарт-карти.

Підбір персоналу.

Вирішальна роль у системі збереження інформації з обмеженим доступом належить людському факторові. Незалежно від того, на скільки добрі розроблена та впроваджена комплексна система захисту інформації, вона в решті-решт ґрунтується на людській діяльності, у якій можливі помилки або свідомі дії, направлені на знищення інформації, або передачу її зацікавленим організаціям. Неможна, також, не відзначити, що сьогодні, як і завжди між різноманітними організаціями йде постійна боротьба за сфери своїх інтересів. І методи цієї боротьби різноманітні, починаючи від дипломатичної діяльності й закінчуючи збройними конфліктами. Велику актуальність сьогодні мають методи "Психологічної війни". Відомо що завданнями психологічної війни є вплив на особу, як носія інформації та як основну ланку в системах управління різноманітного призначення. Потрібно розглянути систему чинників, що визначають кадрову політику підприємства (рис. 2.8.).

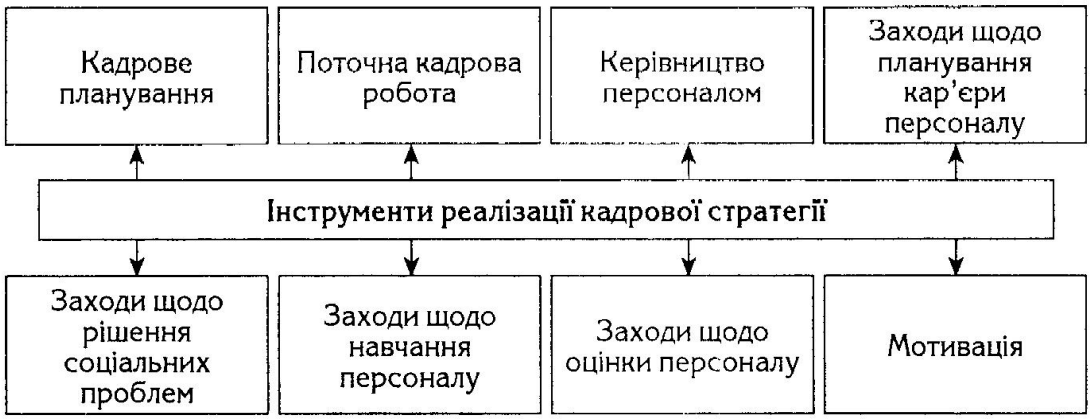

Рисунок 2.8 — Система чинників, що визначають кадрову політику підприємства

Таким чином, особа сьогодні може розглядатися як основний об'єкт атаки нетрадиційними методами ведення війни. Тому на сучасному етапі розвитку методів і засобів захисту інформації, одним із головних напрямків необхідно виділити процес виявлення й оперативної ліквідації загроз для інформації, які можуть виникати в процесі діяльності персоналу установ і організацій.

Процедура відбору на вакантні посади працівників також є складною і її потрібно не оминати (рис. 2.9).

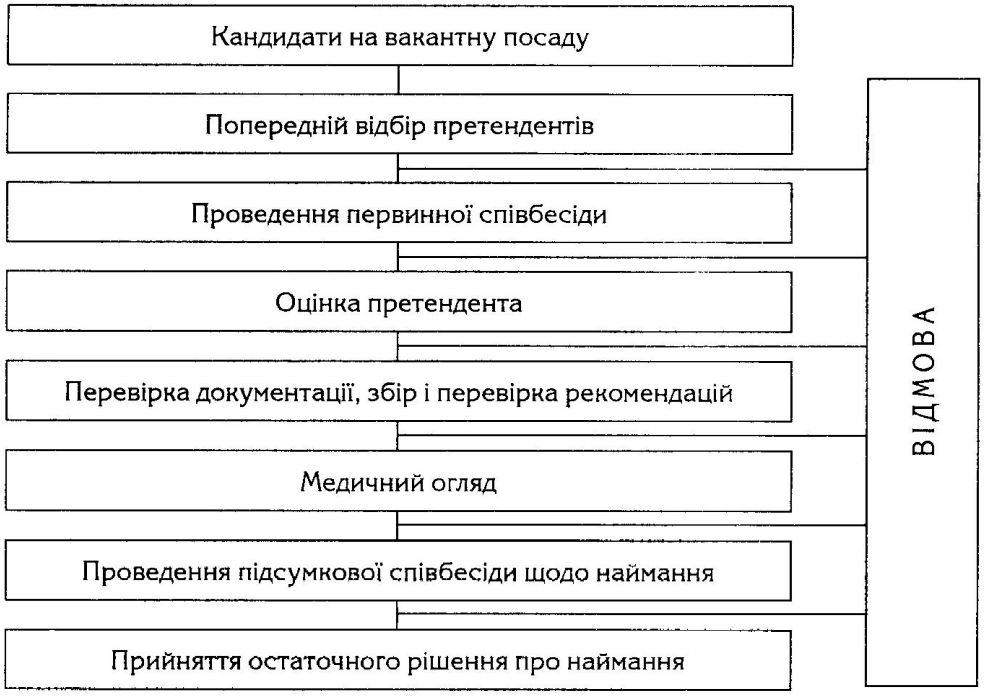

Рисунок 2.9 — Процедура відбору персоналу на вакантні посади

Ніяка технічна система безпеки не забезпечить надійний захист інформації, якщо хтось із персоналу встанови буде свідомо здійснювати її несанкціоноване копіювання, або навмисне пошкодження. Відомо багато методів впливу на особу з метою одержання від неї потрібної інформації, які завжди активно використовуються зацікавленими особами.

Методи впливу:

- підкуп;
- шантаж;
- погрози;
- одержання потрібної інформації при веденні звичайної розмови;
- обмін інформацією;
- переконання;
- використання психологічних методів;
- впровадження співробітником організації "своєї людини".

Ще до моменту працевлаштування для забезпечення безпеки з боку персоналу керівництво організації переконується, що працівники, контрагенти та користувачі третіх сторін розуміють свої обов'язки, підходять для ролей, що розглядаються. Працівникам, контрагентам та користувачам третіх сторін, що застосовують засоби обробки інформації, підписують угоду про ролі та обов'язки щодо безпеки.

При відборі кандидатів на вакантну посаду контрольні перевірки проводяться у відповідності із законодавством, нормами й етикою, відповідно до вимог бізнесу, класифікації інформації, що підлягає доступу, а також із існуючими прийнятними ризиками. Під час проведення контрольних перевірок приймаються до уваги всі відповідні заходи для забезпечення конфіденційності й захисту особистих даних, законодавства про працевлаштування, а при наявності санкцій враховуються також наступні моменти: наявність задовільних рекомендацій, перевірка повноти й точності професійної біографії, підтвердження заявленої академічної й посесійної кваліфікації, незалежна

перевірка особистості, більш детальні перевірки (кредитних карт, наявності судимостей).

Планування персоналу передбачає оцінку наявних ресурсів підприємства; визначення можливих потреб у трудових ресурсах; вивчення ринку праці й розробку програми залучення персоналу для задоволення потреб підприємства.

Оцінюючи потреби в кадрах, необхідно враховувати характер і вид діяльності підприємства, ефективне навантаження працівників з метою оптимального використання коштів, пов'язаних з оплатою праці; можливість залучення спеціалістів, що мають високу кваліфікацію й відповідний досвід роботи на зовнішньому ринку.

Ефективне планування персоналу ґрунтується на володінні такою інформацією:

- скільки працівників, якої кваліфікації, коли й де будуть потрібними;

- яким чином можна залучити потрібний і скоротити чи оптимізувати надлишковий персонал;

- як краще використовувати персонал відповідно до його здібностей, досвіду й внутрішньої мотивації;

- яким чином забезпечити умови для розвитку персоналу;

- яких витрат потребують дані кадрові заходи.

Визначити необхідну чисельність працівників, їхній професійний і кваліфікаційний склад дають змогу: виробнича програма, норми виробітку, заплановане підвищення продуктивності праці й структура робіт.

Якість трудових ресурсів підприємства тім вища, чим більша частка працівників, що забезпечують високу продуктивність праці, тобто персоналу високої кваліфікації. Тому в сучасних умовах значно зростає значимість та рівень вимог до підбору персоналу. В процесі відбору можливе навчання або перекваліфікація персоналу згідно схеми (рис. 2.10).

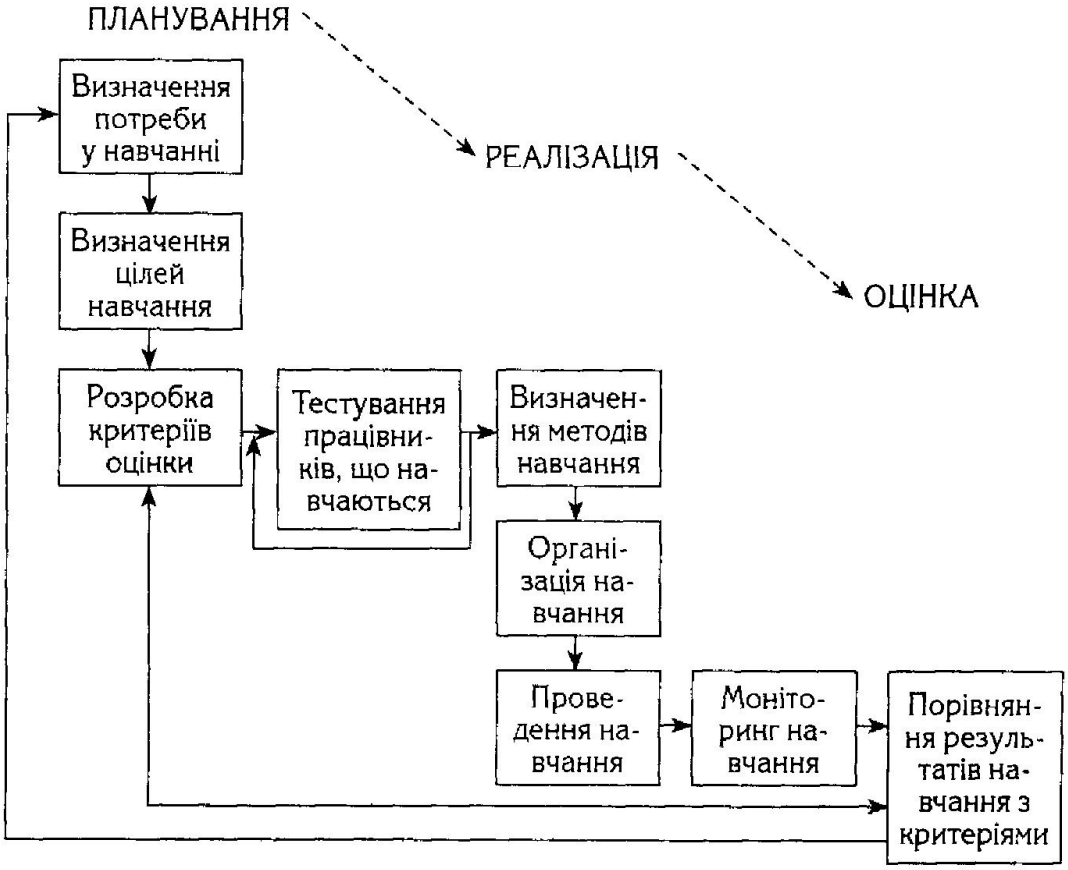

Рисунок 2.10 — Модель організації процесу навчання працівників

Підбір персоналу – це ряд дій, спрямованих на залучення кандидатів, які володіють якостями, необхідними для досягнення цілей, що стоять перед підприємством.

Підбір персоналу починається з маркетингу персоналу. Управління по роботі з персоналом проводять внутрішній маркетинг персоналу та маркетинг персоналу на ринку праці. Орієнтуючись на зовнішні джерела підбору персоналу на підприємстві, створюється власна база даних потенційних кандидатів для зайняття вакантних посад або дається замовлення організаціям, які займаються підбором персоналу. Це, зокрема, кадрові агентства, які володіють базами даних та сучасними методиками підбору персоналу. Проте більшість вітчизняних підприємств, підбираючи персонал, спираються на власні сили. Хоча все-таки можна прослідкувати тенденцію до співпраці між двома зацікавленими сторонами – підприємствами та кадровими агентствами.

Послуги з підбору персоналу надають також бюро з працевлаштування, які підпорядковані переважно місцевим органам влади й сприяють працевлаштуванню тимчасово безробітних спеціалістів. Як правило, вони надають послуги з підбору малокваліфікованої робочої сили.

В процесі відбору можливо застосовувати тести та методики щодо виявлення професійних та інших якостей (табл. 2.2).

Досвід провідних підприємств дає змогу виокремити низку заходів, що традиційно вживаються при підборі персоналу:

- створення системи підбору, що включає співбесіди з працівниками управлінь по роботі з персоналом, керівниками підрозділів, психологічні тести, ділові ігри, випробувальний термін на робочому місці;

- використання "портрета компетенцій" як основного інструменту визначення фахової придатності кандидата;

- перенесення акценту у відборі працівників із формальних моментів у біографії кандидата (освіта, фах, стаж роботи) на аналіз його компетенцій і життєвих цінностей;

- залучення фахових експертів для підбору персоналу. Якщо раніше такі питання вирішувалися вищим керівництвом, а доля консультантів зводилася до підбору кандидатів для співбесіди, те сьогодні кадрові агентства, що спеціалізуються в сфері підбору персоналу, повністю виконують цю функцію – описують виробничу поведінку, складають "портрет компетенцій", здійснюють пошук кандидатів, проводять їхнє тестування й оцінюють результати;

- продовження процесу підбору після прийому співробітника на роботові: випробувальний термін є сьогодні обов'язковим на більшості підприємств, оскільки ніякі тесті не дають такого уявлення про кандидата, як робота певний година на займаній посаді;

- організація спеціальних програм адаптації для всіх прийнятих на роботові працівників, метою яких є не тільки й не стільки навчання фаховим навичкам, скільки знайомство нового працівника з цілями підприємства, його філософією – своєрідне "обернення в нову віру".

Таблиця 2.2

Види тестів, що застосовуються в процесі відбору персоналу

Найменування	Короткий опис
Методика «Оперативна пам'ять»	Для вивчення короткочасної пам'яті в тихнув випадках, коли вона несе основне функціональне навантаження
Методика «Пам'ять на числа»	Для оцінки зорової пам'яті, її обсягу і точності
Методика «Пам'ять на образи»	Для вивчення образної пам'яті
Методика «Червоно-Чорна таблиця»	Для оцінки переключення уваги
Методика Мюнстерберга	Для визначення вибірковості уваги
Методика «Розміщення чисел»	Для оцінки довільної уваги
Методика «Компаси»	Для визначення просторових представлень
Методика «Складні аналогії»	Для оцінки логічного мислення
Методика Равена	Для вивчення логічності мислення
Опитувальник К. Леонгарда	Для виявлення напрямків характеру
Тест-опитувальник Кеттела 16 PF. Форма А – 187 питань, форма 3 – 105 питань	Оцінка виразності 16 особистісних рис, запропонованих Кеттелом як модель структури особистості (доброзичливість, інтелект, домінантність, безтурботність та ін.)
Особистісний опитувальник (варіант тесту MMPI, 556 питань)	Оцінка відповідності психологічних особливостей особистості професіограмам більш ніж по 60 видам діяльності
Ціннісні орієнтації М. Рокича	Визначає змістовну сторону спрямованості особистості і складає основу її відносин до навколишнього світу, до інших людей, до собі, ядро мотивації, основу життєвої концепції
Найменування	Короткий опис
Орієнтаційна анкета Б. Басса	Для визначення особистісної спрямованості
Методика В.П. Захарова(на основі опитувальника А.Л. Журавльова)	Визначення стилю керівництва трудовим колективом
Тест-опитувальник Т. Ліри (діагностика міжособистісних відносин)	Оцінка взаємодії особистості з оточенням, формування ідеальних образів «я» і найближчого оточення. Виявлення внутрішніх конфліктів, пов'язаних з самореалізацією особистості
Тест-опитувальник К. Томаса (діагностика реагування на ситуації конфлікту)	Оцінка типу поведінки особистості в конфліктній ситуації по п'ятьох узагальнених типах: суперництво, запобігання конфлікту, компроміс, співробітництво, пристосування
Диференційно-діагностичний опитувальник Е.А. Клімова	Оцінка відповідності професійних схильностей особистості по п'ятьох основних сферах діяльності: людина — техніка, людина — знакова система, людина — художній образ, людина — природа
Колірний тест Люшера	Діагностика психофізичного стану особистості і розробка характеристик, що можуть бути використані для побудови психологічного портрету

При підборі персоналу мова йде про ті, щоб із числа зацікавлених осіб (кандидатів), що подали анкету, вибрати тихнув, хто найкраще відповідає вимогам вакансії.

Для цього необхідно виявити показники придатності кандидатів (можливості, знання, досвід, ціннісні установки тощо) і порівняти їх із заздалегідь визначеними показниками вимог до вакансії.

Персонал підприємства поділяється на керівників різних рівнів, спеціалістів, службовців, технічний персонал, робітників.

Керівник – це працівник, який управляє певним колективом, має необхідні повноваження для прийняття рішень у конкретних видах діяльності підприємства, відповідає за результати роботи.

Спеціалісти – працівники, що виконують визначені функції управління, аналізують зібрану інформацію й готують варіанти рішень для керівників відповідного рівня. До спеціалістів належать, наприклад, економісти, юристи, бухгалтери. Особливістю їхньої діяльності є робота в умовах певних обмежень: їхню діяльність обмежують накази, розпорядження керівників, техніко-технологічні нормативи та організаційні регламенти, кваліфікаційні вимоги. У діяльності спеціалістів переважають логічні операції, що не заважають прояву творчої активності.

Службовці – працівники, що обслуговують діяльність спеціалістів і керівників. Вони повинні виконувати інформаційно-технічні операції, звільняючи керівників і спеціалістів від цієї роботи. Специфіка діяльності службовця полягає в тому, що в ній використовуються стандартні процедури й операції, вона значною мірою відповідає відомим нормам.

Сучасний розвиток теорії управління призводить до того, що дедалі частіше терміни "керівник" і "менеджер" вживаються як синоніми. Менеджер – це керівник або управляючий, що займає постійну посаду й має повноваження в сфері прийняття рішень із зазначених видів діяльності підприємства.

Оцінювання персоналу використовується для визначення відповідності працівника вакантному чи робочому місцю (посаді), яку він у даний час займає. Оцінювання персоналу включає:

- оцінювання потенціалу працівника;
- оцінювання індивідуального внеску (оцінювання праці);
- атестацію кадрів.

Оцінювання потенціалу працівника здійснюється при заміщенні їм вакантного робочого місця. Воно дає змогу визначити ступінь підготовки працівника до виконання саме того виду діяльності, яким він буде займатись, а також виявити рівень його потенційних можливостей для оцінювання перспектив зростання. Ця процедура включає оцінювання професійних знань, умінь, виробничого досвіду, ділових та особистісних якостей, ціннісних орієнтацій, працездатності та загального рівня культури працівника, що претендує на зайняття вакантної чи посади робочого місця.

Оцінювання індивідуального внеску дає змогу встановити якість, складність і результативність праці конкретного працівника та його відповідність займаній посаді (робочому місцю).

Атестація кадрів виступає як комплексне оцінювання, що враховує потенціал та індивідуальний внесок шкірного працівника в кінцевий результат. Вихідними даними для оцінювання персоналу виступають:

- філософія підприємства та стратегічний план його розвитку;
- моделі робочих місць працівників;
- методики рейтингового оцінювання кадрів;
- положення про атестацію кадрів;
- правила внутрішнього розпорядку підприємства;
- штатний розклад;
- особові справи співробітників;
- кадрові накази;
- соціологічні анкети;
- психологічні тести.

Оцінювання персоналу на підприємствах відбувається шляхом залучення до оцінювання співробітника колег, підлеглих і навіть зовнішніх клієнтів. Популярною стає "360-градусна" атестація, коли співробітник одержує оцінку від свого керівника, підлеглих і партнерів. Багато підприємств починають проводити опитування клієнтів із метою оцінювання своїх представників.

У процесі оцінювання співробітника враховуються результати роботи підрозділу й підприємства в цілому. Співробітник, як би добре він не працював на своєму місці, не може одержати високу оцінку, якщо його підрозділ не впорався зі своїми завданнями. При цьому останнім часом відбувається перегляд традиційних термінів оцінювання (рік, півроку) на користь періодів, що змінюються, – завершення проекту або його стадії, перехід до нової структури й т.д.

3 ЕКОНОМІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Аналіз доцільності вкладень на забезпечення захисту інформації

Кошти, які компанія використовує для впровадження та підтримку комплексної системи захисту інформації доцільніше називати вкладеннями, а не витратами, адже це свого роду інвестиції в активи підприємства з метою запобігання фінансових втрат, збільшення прибутку, підвищення конкурентоспроможності й ринкової стабільності.

Для оцінювання ефективності вкладень необхідно визначити величину можливих втрат від реалізації загроз втрати інформації до впровадження засобів захисту на об'єкті та після нього.

Об'єктом інформаційної діяльності є не ціла компанія, а лише її одна функціональна складова – дослідницька лабораторія, тому доцільно розглядати господарську діяльність підприємства як сукупність бізнес-процесів.

3.2 Моделювання бізнес-процесів на підприємстві

В основі бізнесу знаходяться бізнес-процеси. Правильне виділення й удосконалювання бізнес-процесів дає компанії величезні переваги перед конкурентами.

Бізнес-процес – це сукупність різних видів діяльності, у рамках якої "на вході" використовується один чи більш видів ресурсів, і в результаті "на виході" створюється продукт, що представляє цінність для споживача чи так званого "клієнта бізнес-процесу".

Підхід до аналізу й оптимізації бізнесу компанії на основі бізнес-моделі може бути цікавий широкому колу осіб, що здійснюють аналіз чи приймають рішення про довгостроковий розвиток компанії (рис. 3.1).

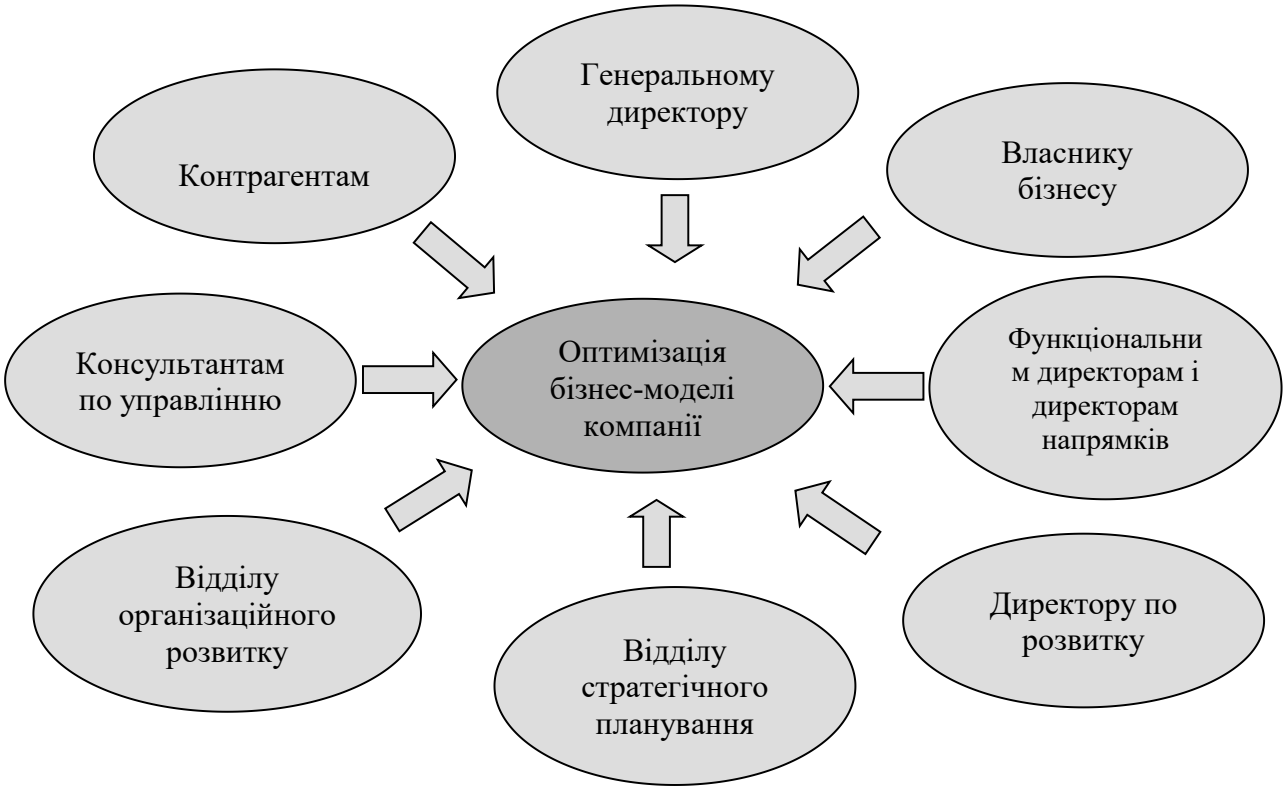

Рисунок 3.1 — Коло зацікавлених осіб в оптимізації бізнес-моделі компанії

Бізнес-модель – це сполучення ряду параметрів, що описують принципову схему побудови бізнесу компанії. Принципово важливими в бізнес-моделі є не стільки параметри самі по собі, скільки їхнє взаємне ув'язування.

На підставі зіставлення існуючої бізнес-моделі з закордонними аналогами, з урахуванням цілей компанії й ринкових розумів, формуються альтернативи розвитку компанії.

Ефективна реалізація бізнес-процесів – це позначка й завдання будь-якого підприємства. Для їхнього досягнення розроблені методи й інструментальні засоби опису, проектування, аналізу й оцінки бізнес-процесів, концепції й правила їхньої реорганізації. Бізнес-процес являє собою набір взаємозалежних бізнес-процедур у результаті яких виробляється певна група продуктів і послуг. Усі бізнес-процеси існують для виконання функцій підприємства й повинні відповідати встановленій на підприємстві ієрархії цілей.

Бізнес-процес – це логічний, послідовний, взаємозалежний набір заходів, що залучає ресурси виробника, створює цінність і видає результат споживачеві.

Серед основних причин, що спонукують організацію оптимізувати бізнес-процес, можна виділити необхідність зниження витрат або тривалості виробничого циклу, вимоги, пропоновані споживачами й державою, впровадження програм керування якістю, злиття компаній, внутрішньо-організаційні протиріччя й ін.

Моделювання бізнес-процесів дозволяє не тільки визначити, як компанія працює в цілому, як взаємодіє із зовнішніми організаціями, замовниками й постачальниками, але і як організована діяльність на шкірному робочому місці.

Моделювання бізнес-процесів – це ефективний засіб пошуку шляхів оптимізації діяльності компанії, засіб прогнозування й мінімізації ризиків, що виникають на різних етапах реорганізації підприємства. Цей метод дозволяє дати вартісну оцінку шкірному окремому процесу й всім бізнес-процесам організації в сукупності.

Найважливішими поняттями будь-якого методу моделювання бізнес-процесів є поняття об'єкта й зв'язку. Кожний об'єкт моделі відбиває деякий реальний об'єкт так званої предметної області: люди, документи, машини й устаткування, програмне забезпечення й т.д. Як правило, у рамках одному методу об'єкти моделі, що відбивають різні сутності реального світу, також є різними. Зв'язки призначені для опису залежностей об'єктів один з одним. До числа таких взаємин можуть ставитися: послідовність виконання в часі, зв'язок за допомогою потоку інформації, використання іншим об'єктом і т.д.

Для об'єкта й зв'язків характерний ряд параметрів, або, як прийнято говорити, атрибутів, що відбивають певні характеристики реального об'єкта. Склад атрибутів залежить від типу відображуваного за допомогою моделі реального об'єкта організації. Атрибутами можуть служити такі характеристики, як номер об'єкта, назва, опис, тривалість виконання (для функцій), вартість і ін. На практиці при створенні моделей організації опис атрибутів об'єктів моделі здійснюється за допомогою спеціальних інструментальних засобів моделювання бізнес-процесів. Це дозволяє зробити з найпростішого «опису»

бізнесу-процесу більш складну «модель», на основі якої роблять певні обчислення, здійснюють аналіз і оцінку процесу.

Як правило, основу для класифікації бізнес-процесів становлять чотири базові категорії:

а) основні бізнес-процеси;

б) забезпечуючі бізнес-процеси;

в) бізнес-процеси розвитку;

г) бізнес-процеси керування.

Основними бізнес-процесами є ті процеси, які орієнтовані на виробництво продукції або надання послуги, що представляють цінність для клієнта, та забезпечують одержання доходу для підприємства. Ці процеси роблять “Виходи” процесів. Як правило, основних бізнес-процесів на підприємстві небагато (не більше десяти).

Забезпечуючі бізнес-процеси – це допоміжні процеси, які призначені для забезпечення виконання основних бізнес-процесів. У загальному виді вони забезпечують ресурсами всі бізнес-процеси підприємства.

Процеси керування – це бізнес-процеси, які охоплюють весь комплекс функцій керування на рівні шкірного бізнесу-процесу й бізнес-системи в цілому, тобто взаємозалежної безлічі всіх бізнес-процесів підприємства.

Базові категорії можуть бути розширені додатковими категоріями. Наприклад, крім основних процесів, які приносять основний дохід підприємству, можна виділити не основні бізнес-процеси, які приносять незначну частку доходу.

При проведенні виділення й класифікації для кожного бізнесу-процесу визначається склад учасників бізнес-процесу. Важливе місце при визначенні учасників займає власник бізнес-процесу, як правило, посадова особа – топ-менеджер.

Проведення виділення й класифікації бізнес-процесів, визначення їхніх параметрів – індивідуальна й досить не проста робота при переході на процесну організацію й керування діяльністю підприємства. Тому, важливою заключною

стадією виконання даної роботи є узгодження результатів проведеної класифікації між власниками бізнес-процесів, а також власниками підприємства.

Функціональна модель об’єкту захисту містить безліч бізнес-процесів. Кожний бізнес-процес відіграє конкретну роль у загальному механізмі функціонування організації. Проте, бізнес-процеси можуть бути розподілені по групах. Розподіл по групах у більшості випадків проводитися за принципом орієнтації генерованої цінності. За даним принципом бізнес-процеси компанії можуть бути класифіковані в такий спосіб:

- Основні бізнес-процеси – бізнес-процеси, що приймають доля в створенні основної цінності орієнтованої на споживача:

- компонування нових, наприклад, будматеріалів та сумішей;

- виробництво продукції;

- перевірка та контроль за якістю продукції, що виготовляється;

- маркетинг;

- збут.

Допоміжні бізнес-процеси – бізнес-процеси, що підтримують протікання основних бізнес-процесів:

- матеріально-технічного забезпечення;

- управління інфраструктурою;

- управління персоналом;

- управління логістикою;

- юридичне забезпечення.

Бізнес-процеси управління – спрямовані на планування й контроль функціонування всієї мережі бізнес-процесів компанії:

- стратегічне планування;

- бюджетування;

- менеджмент якості.

На об’єкті інформаційної діяльності, яким є науково-дослідна лабораторія при підприємстві, протікають такі бізнес-процеси, як компонування нових будматеріалів та сумішей та перевірка і контроль за якістю продукції, що

виготовляється. Вартість інформації, за допомогою якої смороду реалізуються, експерти оцінюють в 100000 грн.

3.3 Виявлення та оцінка ризиків втрати інформації

Одним із етапів проведення аналізу ефективності вкладання коштів у забезпечення захисту інформації є визначення величини збитків від порушення інформаційної безпеки. Велика кількість каналів витоку та невизначеність у діях порушника в значній мірі ускладнює розрахунок економічної ефективності. Виходячи з того, що в реальній ситуації мають місце випадкові фактори, які призводять до порушення захищеності, можна розглядати суму збитків як очікування суми збитків по всіх каналах витоку інформації з урахуванням «вартості інформації». Так,

$$C_{\text{можл.зб.}} = BI \cdot P_{\text{заг.}} \tag{3.1}$$

де $C_{\text{можл.зб.}}$ – загальні збитки при порушенні інформаційної безпеки; BI – загальна вартість інформації в копійчаному вираженні; $P_{\text{заг.}}$ – загальна ймовірність реалізації загрози:

$$P_{\text{заг.}} = 1 - \prod_{i=1}^{n} (1 - p_i), \tag{3.2}$$

де p_i – ймовірність порушення інформаційної безпеки через i-й канал витоку;

n – кількість каналів витоку.

Як видно з формули (3.2), щоб точно оцінити величину можливих збитків, необхідно правильно визначити область ризику втрати інформації через певний канал.

Як економічна категорія ризик являє собою подію, яка може відбутися або не відбутися. У випадку виникнення такої події можливі 3 економічні результати:

- негативний – програш, збиток;

- нульовий;

- позитивний – виграш, вигода, прибуток.

Слід зазначити, що ризик існує завжди, і можна спробувати захиститись від ризику до задовільного рівня, але повністю усунути не можливо. Одержати прибуток від проведення тієї чи іншої операції можна тільки у випадку, якщо ризики були заздалегідь передбачені, вивчені, виміряні та підстраховані.

Неможливо повністю звільнитися від ризику: намагаючись позбутися однієї ризикованої ситуації, можна потрапити в іншу. Навіть абсолютна бездіяльність в економічному житті спряжена з ризиком невикористаних можливостей.

Загалом фінансова діяльність завжди ставить за позначку одержання доходів у залежність від ризику. Тому між величиною прибутків і рівнем ризику існує пряма пропорційна залежність.

Відповідно, чим більший очікуваний дохід, тім більший рівень ризику. Зрозуміло, що ймовірність одержання доходу протистоїть можливостям збитків.

Для того, щоб описати бізнес-процеси управління ризиками, необхідно визначити життєвий цикл ризику.

Під час оцінки фінансово-господарської діяльності перше, що слід зробити, – це виявити й зафіксувати ризики, тобто обмежити кількість існуючих ризиків, використовуючи принцип “розумної достатності”. Цей принцип ґрунтується на урахуванні найбільш значимих та найбільш поширених ризиків.

Невизначеність призводить до ризику через відсутність повної інформації та неможливість точного передбачення. Суттєво впливати на його виникнення можуть такі чинники як погодні умови, науково-технічний прогрес, ринковий попит і ціни на товари тощо. Ризик виникає тоді, коли приймається рішення з кількох можливих, і є непевність у тому, що воно, це рішення, призведе до найефективніших наслідків.

Призначення аналізу ризику – прийняття рішень стосовно доцільності участі в певній економічній діяльності (проекті) і передбачити заходь захисту від можливих збитків.

У літературі з економіки та теорії бізнесу, а також у практиці приватного підприємництва часто можна зустрітися з термінами „жорстокий ризик”, або „низький ризик”, коли йдеться про різні рівні ризику. Рівень ризику залежить від співвідношення масштабу очікуваних втрат (збитків) до обсягу майна підприємця чи фірми, а також від імовірності настання збитків.

Теорія економічного ризику дозволяє створити гнучку мережу вербальних, графічних та математичних моделей, застосувати сукупність математичних методів та широкий спектр експертних процедур.

Використовуючи економічний аналіз, визначаючи ймовірність сподіваного результату та оцінюючи ризик за допомогою економіко-математичних методів, можна одержати можливість зменшення впливу ризику на фінансові результати та прийняття рішення щодо вибору певної програми комерційної діяльності.

Слід чітко усвідомлювати, що виключити економічний ризик повністю неможливо. Він існує через об'єктивні, притаманні економіці категорії конфліктності та невизначеності, відсутність повної (вичерпної) інформації, неможливість здійснення точного прогнозу щодо цілого ряду параметрів економічних об'єктів та процесів, що аналізуються. Основне завдання – це керування ризиком, зведення його до прийнятних величин (а не виключення), зниження можливих збитків.

Посилення впливу ризику це насправді зворотний бік свободи підприємництва, своєрідна плата за неї. Під година розвитку ринкових відносин в Україні безумовно буде посилюватися конкуренція. Щоб вижити за цих розумів, необхідно впроваджувати нові технології й технічні новинки, йти на сміливі, нетрадиційні дії, які, у свою чергу, підвищують ризик. Отже, необхідно навчитися прогнозувати події, оцінювати економічний ризик, йти на нього, але не переходити допустимих меж.

У кожній ситуації, що пов'язана з ризиком, виникає питання: що означає виправданий (допустимий) ризик, де проходити межа, що відділяє допустимий ризик від нерозумного. Відповісти на ці запитання означає, що треба знайти

рівень „прийнятного ризику”, кількісну та якісну оцінки конкретних ризикованих рішень.

Економічний ризик – це об'єктивно-суб'єктивна категорія, що пов'язана з подоланням невизначеності та конфліктності в ситуації неминучого вибору й відображає міру (степінь) досягнення сподіваного результату, невдачі та відхилення від цілей з урахуванням впливу контрольованих та неконтрольованих чинників за наявності прямих та зворотних зв'язків.

Всі це визначає системний підхід до категорії ризику й вплив на систему внутрішніх чинників, конкуруючих систем та надсистеми в цілому.

Важливою є розробка методик стосовно оцінювання ризику в різних сферах економічної діяльності, розвиток відповідного механізму контролю та керування економічним ризиком на принципах системного аналізу.

Системний аналіз – це методологія дослідження об'єктів з метою визначення найбільш ефективних методів керування ними.

Об'єктом ризику називають економічну систему, ефективність та умови функціонування якої наперед точно не відомі.

Під суб'єктом ризику розуміють особу (індивід або колектив), яка зацікавлена в результатах керування об'єктом ризику й має компетенцію приймати рішення щодо об'єкта ризику.

Джерело ризику – це чинники (явища, процеси), які спричиняють невизначеність результатів (конфліктність).

Під інформаційною ситуацією будемо розуміти певний ступінь градації невизначеності знаходження середовища в одному з станів заданої множини, якою володіє суб'єкт управління (менеджер) у момент прийняття рішення.

Коли говорять про необхідність урахування ризику в певному виді економічної діяльності (певному проекті), мають на увазі інтереси суб'єктів, котрі беруть у ньому доля: замовника, інвестора, виконавця (підрядника) чи продавця, покупця, а також страхову компанію.

Для аналізу ризику використовуємо критерії, запропоновані відомим американським експертом Б. Берлімером:

- збитки від ризику незалежні один від одного;

- збитки за одним напрямком із „портфеля ризиків” не обов'язково збільшують ймовірність збитків за іншим (за виключенням форс-мажорних обставин);

- максимально можливі збитки не повинні перевищувати фінансових можливостей суб'єктів, що беруть доля в даному виді економічної діяльності.

Нижче наведена схема логічного процесу аналізу ризику під година прийняття управлінських рішень (рис. 3.2).

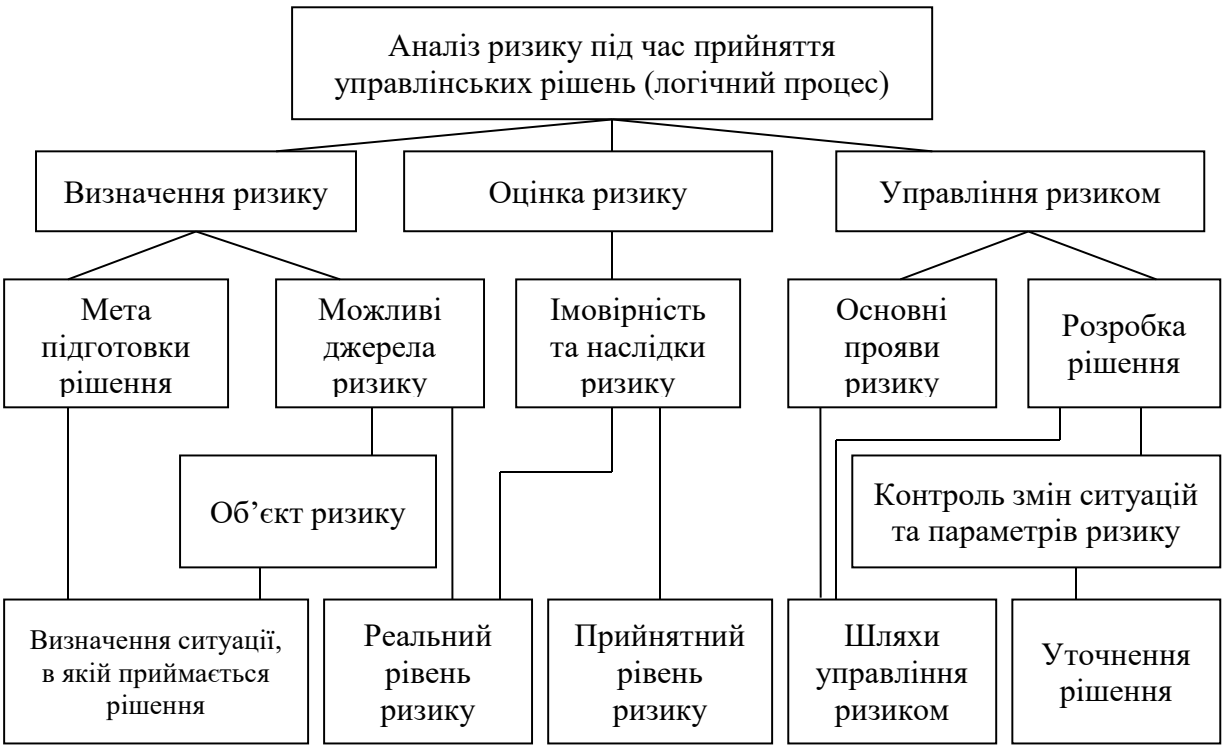

Рисунок 3.2 — Логічний процес аналізу ризику під час прийняття управлінських рішень

Аналіз ризику проводять у такій послідовності:

1) визначення внутрішніх та зовнішніх чинників, що збільшують чи зменшують ступінь певного виду ризику;

2) аналіз виявлених чинників;

3) оцінювання певного виду ризику за двома підходами:

4) визначення економічної доцільності (ефективності вкладених засобів);

5) розробка заходів щодо зниження ступеня ризику.

Всі менеджери (суб'єкти) у будь-якій сфері економічної діяльності зацікавлені в уникненні значних збитків. За розумів нестабільної та швидко змінюваної ситуації суб'єкти економічної діяльності змушені враховувати всі можливі наслідки дій своїх конкурентів, а також інших змін у ринковій ситуації.

Аналіз ризиків поділяють на два взаємодоповнюючі один одного види: якісний та кількісний.

Якісний аналіз є найбільш складним і вимагає ґрунтовних знань, досвіду та інтуїції в даній сфері економічної діяльності. Його головна позначка визначити чинники ризику, області ризику, після чого ідентифікувати усі можливі ризики.

Кількісний аналіз ризику, тобто кількісне (числове) визначення ступеня окремих ризиків і ризику даного виду діяльності (проекту) у цілому, що є теж досить складною проблемою.

Якісний аналіз ризику.

Якісний аналіз ризику включає декілька аспектів. Перший аспект пов'язаний з необхідністю порівняння сподіваних позитивних результатів з можливими економічними, соціальними та іншими, як сьогоднішніми так і майбутніми наслідками. Взагалі мало мати схильність до ризику: потрібен ризик обґрунтований, в іншому випадку він може набути характер авантюри. Ризикувати доцільно, якщо це призводить до кращих наслідків, при обґрунтуванні правильності своїх дій.

Проблеми ризику повинні розглядатися та враховуватися як під час розробки стратегії, так і в процесі реалізації оперативних завдань. Характер стратегічних підходів слід визначити в межах загальної стратегії. У протилежному випадку не уникнути неприємних „сюрпризів”.

Другий аспект якісного аналізу ризику пов'язаний з виявленням впливу рішень, що приймаються за розумів невизначеності, на інтереси суб'єктів економічного життя. Без урахування інтересів (зацікавленості), без керування

ними неможливі реальні якісні перетворення в соціально-економічному житті. Необхідно виявити: кому ризик корисний? Чиїм інтересам відповідає?

Минулий практичний досвід управління економікою в нашій країні свідчить про те, що в цілому ряді випадків особині, що очолювали ту чи іншу ланку економічної діяльності, визначали її стратегію й тактикові, матеріально не вигравали й не програвали залежно від того, до яких наслідків, позитивних чи негативних, призводили їх рішення. Тобто суб'єкти при прийнятті економічних рішень, у переважній більшості випадків, перекладали ризик на суспільство в цілому. Мова йде про ті, що коли немає зацікавленості в результатах економічних рішень, те немає й ризику.

Отже, ризикованій ситуації притаманні такі основні умови:

- наявність невизначеності;
- наявність альтернатив та необхідність вибору однієї з їх (відмова від вибору також є різновидністю вибору);
- зацікавленість у результатах;
- можливість оцінити наявні альтернативи прийняття рішення.

Усі чинники, що чи так інакше впливають на ступінь ризику, можна умовно поділити на дві групи: об'єктивні та суб'єктивні.

До об'єктивних чинників відносять такі, що не залежати безпосередньо від фірми та менеджерів (суб'єктів прийняття рішень): інфляція, конкуренція, політичні та економічні кризи, екологія, мита, наявність режиму найбільшого сприяння, можлива робота в зоні вільного економічного підприємництва тощо.

До суб'єктивних чинників відносять ті, котрі характеризують суб'єкт прийняття відповідних рішень (безпосередньо менеджерів, фірму): виробничий потенціал, технологічне забезпечення, рівень предметної та технологічної спеціалізації, організація праці, ступінь кооперативних зв'язків, рівень техніки безпеки, рівень компетентності та інтелектуальний потенціал суб'єкта прийняття рішень, вибір типу контрактів з інвестором чи замовником тощо. Так, зокрема, від типу контракту залежить ступінь ризику та розмір винагороди після завершення контракту. Сподівання на максимальний прибуток, з одному

боку, і страх підприємницького ризику з іншого, переконують, що успіх у менеджменті можливий лише для тихнув, хто добре володіє обраною галуззю діяльності, на високому професійному рівні вирішує задачі, що постають, хто мислить не ординарно й у змозі творчо застосувати знання в реальній економічній і фінансовій ситуаціях.

Кількісний аналіз ризику.

Під час цього аналізу можна використовувати різні методи. Найбільш розповсюдженими є:

- статистичні;
- використання аналогів;
- експертні методи;
- аналіз доречності витрат.

Ризики втрати інформації через кожний з каналів витоку визначаємо за допомогою залучення експертів.

Метод експертних оцінок є, мабуть, тім єдиним методом, що, дозволяє оцінювати ступінь ризику різних видів виробничо-збутової і фінансової діяльності підприємств в умовах дефіциту інформації. Оцінка ризику виконується на основі суб'єктивних думок експертів – фахівців у конкретній галузі діяльності.

Кожному експерту надається перелік можливих ризиків і пропонується оцінити ймовірність їхнього настання, користуючись шкалою оцінок (табл. 3.1).

Таблиця 3.1

Шкала ризику

Оцінка, %	Ризик
0	несуттєвий ризик
25	ризикова ситуація ймовірніше не настане
50	про можливість ризикової ситуації нічого певного сказати не можна
75	ризикова ситуація швидше за все настане
100	ризикова ситуація настане однозначно

Оцінка ризику виконується поетапно:

- ранжирування – виділення оціночних критеріїв і їхнє ранжирування стосовно конкретної ситуації;

- зважування – визначення вагових характеристик оціночних критеріїв для шкірного з можливих каналів витоку;

- комплексна оцінка – комплексна оцінка каналів витоку з урахуванням рангів і вагових характеристик оціночних критеріїв і прийняття рішень.

Потім результати оцінки перевіряють на суперечність за таким правилом: припустима різниця між оцінками двох експертів з будь-якого виду ризику не винна перевищувати 25 %:

$$\max(a_i - b_i) \le 50, \tag{3.3}$$

де a і b – вектори оцінок кожного з двох експертів; i – вид оцінюваного ризику.

Якщо результати не суперечливі, їх приймають. Якщо ні, проводитися ще один тур експертного опитування, але вже з відповідними обґрунтуваннями й уточненнями, а також з дрібнішою градацією шкали ризику.

Результати експертного опитування наведено в таблиці 3.2.

Таблиця 3.2

Ймовірність втрати інформації через обрані канали витоку

Канал витоку	Значення ймовірності, %
Акустичний	12,5
Акусто-електричний канал	25
ВЧ-нав'язування	12,5
Радіоканал	25

Тоді сумарна ймовірність $P_{\text{заг.}}$ набуде значення:

$$P_{\text{заг.}} = 1 - \left[(1 - 0{,}125) \cdot (1 - 025) \cdot (1 - 0{,}125) \cdot (1 - 0{,}25)\right] = 0{,}57,$$

тобто $P_{\text{заг.}} = 57$ %.

Результату кількісної оцінки відносять до однієї з п'яти можливих областей ризику (рис. 3.3): безризикова область, область мінімального ризику, область підвищеного ризику, область критичного ризику або область неприпустимого ризику.

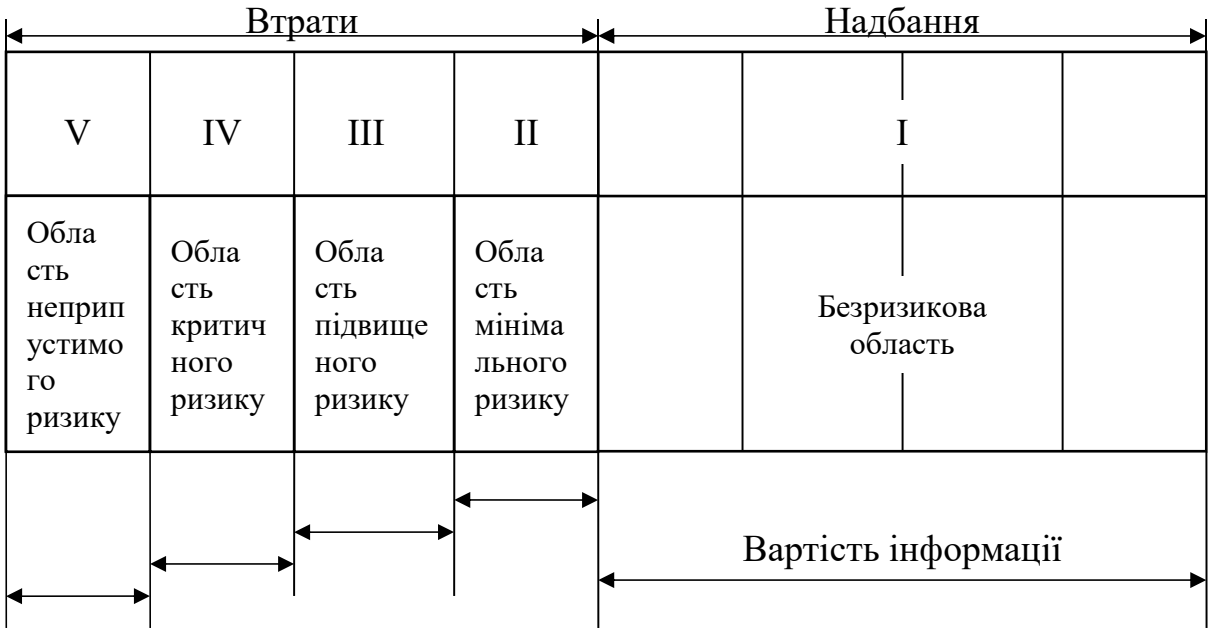

Рисунок 3.3 — Схема областей ризику

Областю ризику називається деяка частина загальних втрат, у межах якої вони не перевищують встановленого граничного значення.

Віднесення результатів діяльності підприємства до певної області ризику виконується залежно від рівня втрат.

Рівень втрат визначається залежно від частки втрат у загальній величині власних коштів підприємства.

Для кількісної оцінки рівня втрат використовують коефіцієнта ризику (K), який виводиться з формули (3.1). Коефіцієнт ризику можна розраховувати як відношення розміру втрат до величини власних коштів підприємства:

$$K = \frac{B_m}{BI} = P_{\text{заг.}}, \tag{3.4}$$

де K – коефіцієнт ризику; B_m – втрати від успішної атаки; BI – загальна вартість інформації; $P_{\text{заг.}}$ – загальна ймовірність реалізації загрози.

В табл. 3.3 приведені рівні ризику, тобто ризик підприємства від недооцінювання різних видів загроз.

Таблиця 3.3

Рівні ризику залежно від співвідношення величини можливих втрат і величини власних коштів підприємства

$K = \frac{B_m}{BI}$	Рівень ризику
$K \leq 0{,}25$	Прийнятий
$0{,}25 < K \leq 0{,}50$	Припустимий
$0{,}50 < K \leq 0{,}75$	Критичний
$K > 0{,}75$	Катастрофічний

В табл. 3.4 наведені основні типи поведінки керівництва підприємства залежно від коефіцієнтів ризику.

Таблиця 3.4

Типи поведінки керівництва підприємства залежно від коефіцієнту ризику

Коефіцієнт ризику, K	Тип поведінки
$K \leq 0{,}2$	Песимістичний
$0{,}2 < K \leq 0{,}4$	Обережний
$0{,}4 < K \leq 0{,}6$	Середньоризикований
$0{,}6 < K \leq 0{,}8$	Ризикований
$0{,}8 < K \leq 1$	Високого ступеня ризику
$K \geq 1$	Азартний

Розглянемо характеристику кожної з областей згідно рис. 3.3.

Безризикова область (I) – характеризується відсутністю будь-яких втрат при здійсненні господарської діяльності з гарантією одержання розрахункового прибутку. Теоретично прибуток не обмежений. Коефіцієнт ризику $K = 0$.

Область мінімального ризику (II) – характеризується розмірами втрат, які не перевищують чистого прибутку. Коефіцієнт ризику *К*=0 - 0,25. Підприємство ризикує тім, що, у гіршому випадку, воно не одержить чистого прибутку. У кращому випадку – чистий прибуток буде менше його розрахункового значення.

Область підвищеного ризику (III) – характеризується втратами, що не перевищують валового доходу. Коефіцієнт ризику *К*=0,25 - 0,50. Підприємство ризикує тім, що, у гіршому випадку, воно не зможе виплатити заробітну плату своїм працівникам за виконану роботові, але при цьому покриє матеріальні витрати, пов'язані з виробництвом продукції.

Область критичного ризику (IV) –характеризується втратами, величина яких не перевищує виторгу від реалізації продукції. Коефіцієнт ризику *К*=0,50 - 0,75.

Область неприпустимого ризику (V) – характеризується втратами, порівняними з розміром власних коштів підприємства, тобто можливе повне банкрутство. Коефіцієнт ризику *К*=0,75 - 1,0.

Таким чином, внаслідок проведених операцій визначено, що якщо компанія не застосує запобіжні заходь, може втрати кошти на суму 57 000 грн. (від 100 000 грн. чистого прибутку)

Наступним етапом є проведення аналогічних процедур визначення коефіцієнта ризику й величини можливих втрат після застосування контрзаходів. Коефіцієнт визначає група експертів – фахівців у галузі захисту інформації для шкірного каналу витоку окремо. Після чого знаходять загальний показник за формулою (3.2).

4 НОРМАТИВНО-ПРАВОВА БАЗА З ПИТАНЬ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

4.1 Закони України в сфері захисту інформації

Конституція України має найвищу юридичну чинність. Закони й інші нормативно-правові акти приймаються на основі Конституції України й повинні відповідати їй.

У нинішній час законодавча база України з питань захисту інформації опирається на дію наступних Законів:

- “Про інформацію”;
- “Про державну таємницю”;
- “Про захист інформації в автоматизованих системах”;
- “Про науково-технічну інформацію”;
- “Про Службу безпеки України”;
- “Про міліцію”;
- “Про державну податкову службу України”;
- “Про оперативно-розшукову діяльність”.

Закон України “Про інформацію” уведений у дію 02.12.92 р. Цей Закон закріплює право громадян України на інформацію й накладає правові основи інформаційної діяльності.

Другим основним Законом України є Закон “Про державну таємницю”.

Цей Закон регулює суспільні відносини, пов'язані з відношенням інформації до державної таємниці, її засекречуванням і охороною з метою захисту життєво важливих інтересів України в сфері оборони, економіці, зовнішнім відносинам, державній безпеці й охороні правопорядку.

Всі інші закони України базуються на основі двох основних законів: “Про державну таємницю” і “Про інформацію”.

Першим у цьому рядку коштує Закон “Про захист інформації в автоматизованих системах”.

Метою цього Закону є встановлення основ регуляції правовий відносин по захисту інформації в автоматизованих системах за умови дотримання права власності громадян України і юридичних осіб на інформацію й права доступу до неї, право власника інформації на її захист, а також установленого чинним законодавством обмеження на доступ до інформації.

Наступним важливим Законом є Закон “Про науково-технічну інформацію”.

Цей Закон визначає основи державної політики в області науково-технічної інформації, порядок її формування й реалізації в інтересах соціального прогресу в Україні. Метою Закону є створення в Україні правової бази для одержання й використання науково-технічної інформації.

Найбільш важливим щодо положень захисту інформації є Закон України “Про оперативно-розшукову діяльність”, що визначає головні положення діяльності попередніх Законів.

Головними статтями Закону щодо завдань захисту інформації є статті 1, 4, 5, 8 і 9.

Згідно ст. 17: “Захист суверенітету й територіальної цілісності України, забезпечення її економічної й інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу”.

4.2 Стандарти в сфері захисту інформації

1. ДСТУ 3396 0-96. Захист інформації. Технічний захист інформації. Основні положення.

Встановлює об'єкт, мета, основні організаційно-технічні положення щодо забезпечення технічного захисту інформації.

Поширюється на підприємства, організації й установи всіх форм власності, органи державної власності всіх рівнів, які використовують і розпоряджаються інформацією з обмеженим доступом.

2. ДСТУ 3396 1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

Встановлює вимоги до порядку проведення робіт з технічного захисту інформації.

Поширюється на підприємства, організації й установи всіх форм власності, органи державної власності всіх рівнів, які використовують і розпоряджаються інформацією з обмеженим доступом.

3. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Строки й визначення.

Встановлює строки й визначення понять у сфері технічного захисту інформації.

Поширюється на підприємства, організації й установи всіх форм власності, органи державної власності всіх рівнів, які використовують і розпоряджаються інформацією з обмеженим доступом.

У стандарті наведений алфавітний покажчик українською, російською і англійською мовами.

4. ДБН А.2.2-2-96. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування й проектної документації для будівництва.

Встановлюють вимоги до забезпечення технічного захисту інформації під час організації проектування будівництва підприємств, будинків і споруджень.

Призначені для суб'єктів інвестиційної діяльності України і її представництв за кордоном під час виконання проектних і будівельних робіт з урахуванням вимог технічного захисту інформації з обмеженим доступом.

5. Тимчасове положення про категорирування об'єктів (ВПКО-95).

Поширюється на центральні й місцеві органи державної виконавчої влади, на підприємства, організації й установи всіх форм власності, представництва України за кордоном і громадян, які володіють, користуються й розпоряджаються інформацією з обмеженим доступом.

Категорированню підлягають об'єкти, у яких циркулює інформація з обмеженим доступом.

6. Тимчасові рекомендації з технічного захисту інформації в засобах обчислювальної техніки, автоматизованих системах і мережах від

випромінювань по каналах побічних електромагнітних випромінювань і наведень (ВР ЕОТ-95).

Призначені для організації захисту інформації з обмеженим доступом у засобах обчислювальної техніки, автоматизованих системах і мережах від випромінювань по каналах побічних електромагнітних випромінювань і наведень.

Поширюються на центральні й місцеві органи державної виконавчої влади, на підприємства, організації й установи всіх форм власності, представництва України за кордоном і громадян, які володіють, користуються й розпоряджаються інформацією з обмеженим доступом.

7. Тимчасові рекомендації з технічного захисту інформації від випромінювання по каналах побічних електромагнітних випромінювань і наведень (ВР ТЗІ-ПЕМВ-95).

Призначені для організації захисту інформації з обмеженим доступом від випромінювань по каналах побічних електромагнітних випромінювань і наведень.

Поширюються на центральні й місцеві органи державної виконавчої влади, на підприємства, організації й установи всіх форм власності, представництва України за кордоном і громадян, які володіють, користуються розпоряджаються інформацією з обмеженим доступом.

ВИСНОВКИ

Метою дипломної роботи був аналіз економічних аспектів інформаційної безпеки вибраної організації, в залежності від застосованого обладнання для захисту інформації.

Для цього в роботі був зроблений аналіз існуючих методів і засобів захисту інформації, проаналізовані можливі причини утворення каналів витоку інформації та небезпека витоку інформації цими каналами, розглянуті питання нормативно-правового забезпечення.

За результатами такого всебічного аналізу було запропоновано розробити стратегію відбору персоналу на роботу з документацією, що має обмежений доступ, оцінені ризики бездіяльності керівництва щодо захисту інформації на об’єкті інформаційної діяльності.

Запропоновані методики організації ефективного управління процесами роботи підприємства з документацією, що має обмежений доступ, висунуті вимоги до керівного складу підприємства, оцінена кваліфікація працівників та можливі наслідки від роботи неякісних працівників.

Також у дипломі розглянуті економічні ризики втрати конфіденційної інформації, запропоновані методи виявлення вразливостей, що можуть нести суттєві економічні наслідки для роботи та нормального функціонування підприємства.

ПЕРЕЛІК ЛІТЕРАТУРИ

1. Халяпин Д. К. Защита информации в телефонных линиях (каналах) связи // Охрана, № 4. - 2021. - С. 24 - 55.

2. Гирин С. Н., Лысов А. В. Защита информации в телефонных сетях // Разведка, № 4. - 2022. - 52 с.

3. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

4. Андрианов В. И., Бородин В. А., Соколов А. В. Шпионские штучки и устройства защиты объектов и информации: справочное пособие. - М.: Лань, 1997. - 272 с.

5. Лазарев Г. П. Защита информации в информационно-телекоммуникационных системах // Безопасность информации, № 2, 2000. – С. 45 - 50.

6. Виханский О. С. Стратегическое управление: Учебник. – 2-е изд., перераб. и доп. – М.: Гардарика, 1998. – 296 с.

7. Газета “Бизнес” № 17 (328) от 26 апреля 1999 года и № 19 (330) от 10.05.99 г.

8. Мескон М., Альберт М., Хедоури Ф. Основы менеджмента. – М.: Дело, 1994. — 215 с.

9. Основы управления персоналом: Учеб. для вузов/ Б. М. Генкин, Г. А. Кононова, В. И. Кочетков и др.; Под ред. Б. М. Генкина. – М.: Высш. шк., 1996. – 383 с.

10. Управление персоналом: Учебник для вузов/ Под ред. Т. Ю. Базарова, Б. Л. Еремина. – М.: Банки и биржи, ЮНИТИ, 1998. – 423 с.

11. Управление персоналом организации: Учебник/ Под ред. А. Я. Кибанова. – М.: ИНФРА-М, 1997. – 512 с.

12. Ананский Е. В. Защита информации – основа безопасности бизнеса. - СПб: «ЛОТ». - 2003. - 230 с.

13. Матвеев В. А., Молотков С. В. Проблемы организации защиты информации. - К.: ООО «ПолиграфКонсалтинг». - 2001. - 330 с.

14. Дмитриев Ю. В., Минаев В. А., Потанин В. Е., Скрыль С. В. Классификация видов угроз безопасности в информационно-телекоммуникационных системах // Журнал депонированных рукописей, № 9. - 2000. - С. 32 - 40.

15. Чернявский А. А. Радиозакладка на частоты 22,95 МГц и 100 МГц // Защита информации: сборник научных трудов. - 2004. - С. 25 - 30.

16. Максименко Г. А., Хорошко В. А. Методы выявления, обработки и идентификации сигналов радиозакладных устройств. - К.: ООО «ПолиграфКонсалтинг», 2004. - 317 с.

17. Мусиенко Д. И. Радиоизлучающая подслушивающая аппаратура // «Бизнес и безопасность», №4. - 2004. - С. 23 - 30.

18. Виноградов А. В., Волков В. В. Спецтехника. - М.: Связь, 1996. - 136 с.

19. Хорошко В. А. Чекатков А. А. Методы и средства защиты информации. – К.: Юниор, 2003. - 502 с.

20. Ронин Р. Своя разведка: практическое пособие. - М: «АСТ», 2001. - 234 с.