МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

О. В. Коломійцев, В. І. Панченко, Д. О. Лисиця

ТЕОРІЯ РИЗИКІВ

Навчальний посібник
для студентів спеціальності 123 «Комп’ютерна інженерія»
денної та заочної форм навчання

Затверджено
редакційно-видавничою
радою НТУ «ХПІ»,
протокол № 1 від 13.02.2025 р.

Харків
НТУ «ХПІ»
2025

УДК 004.056: 005.334(075)

К61

Рецензенти:

О. Можаєв, проф., д-р техн. наук, проф. каф. кібербезпеки та DATA-технологій ННІ № 5, Харківський національний університет внутрішніх справ;

О. Сєвєрінов, доц., канд. техн. наук, проф. каф. безпеки інформаційних технологій, Харківський національний університет радіоелектроніки

Коломійцев О. В.

К61 Теорія ризиків : навчальний посібник для студентів спеціальності 123 «Комп'ютерна інженерія» денної та заочної форм навчання / О. В. Коломійцев, В. І. Панченко, Д. О. Лисиця. – Харків : НТУ «ХПІ», 2025. – 408 с.

ISBN 978-617-05-0542-2

У навчальному посібнику розглянуто основи теорії ризиків, ключові концепції та методи, які використовуються для виявлення, аналізу та мінімізації ризиків, пов'язаних з безпекою та надійністю комп'ютерних мереж. Автори розглядають як теоретичні основи, так і практичні інструменти для оцінки вразливостей, визначення потенційних загроз та розробки стратегій захисту. Розгляд даних питань забезпечує максимальну спроможність як користувачів, так і адміністраторів комп'ютерних мереж працювати в складному кіберсередовищі, мінімізуючи ризик атак. У посібнику наведено методи та техніки кількісної і якісної оцінки ризиків, аналізу можливих наслідків і ймовірностей виникнення небезпек, а також описано стратегії управління ризиками.

Призначено для студентів спеціальності 123 «Комп'ютерна інженерія» денної та заочної форм навчання. Також він буде корисним для фахівців з кібербезпеки та інформаційних технологій, аспірантів та усіх, хто займається теорією та практикою ризик-менеджменту в сучасних інформаційних системах.

Іл. 71. Табл. 21. Бібліогр. 24 назв.

УДК 004.056: 005.334(075)

ISBN 978-617-05-0542-2

ЗМІСТ

ВСТУП

Основи теорії ризиків закладено повсякденною діяльністю людей протягом століть. Будь-яка сфера діяльності людини так чи інакше пов’язана з ризиком зважаючи на вплив безлічі суб’єктивних і об’єктивних факторів на результати прийнятих людьми рішень.

На даний час інформаційні технології (ІТ) активно використовуються майже в усіх сферах діяльності людини, що, у свою чергу, відкриває для них безліч можливостей, але, одночасно, і піддає складним та різноманітним ризикам (загрозам).

Дослідження теоретичних питань, які пов’язані з управлінням ризиками, є актуальною науковою і практичною задачею. При цьому, окрім вивчення сутності, основних характеристик і функцій ризиків, велике значення мають класифікація ризиків та аналіз причин їх виникнення. Тому, класифікація ризиків та виявлення причин їх виникнення є основою аналізу, оцінки та визначення напрямків зниження ризиків.

У навчальному посібнику розглядаються основи теорії ризиків та дослідження системи захисту інформації (даних) у комп’ютерних мережах. Розгляд даних питань забезпечує максимальну спроможність як користувачів, так і адміністраторів комп’ютерних мереж працювати в складному кіберсередовищі, а також мінімізувати ризик різноманітних атак.

1. СУТНІСТЬ, ВИДИ ТА КЛАСИФІКАЦІЯ РИЗИКІВ

1.1. Ризик, невизначеність та ймовірність

Будь-яка діяльність є складним компромісом у досягненні двох суперечливих цілей – ефективності та надійності. Будь-яка сфера діяльності людини так чи інакше пов’язана з ризиком: зважаючи на вплив на результати прийнятих людьми рішень безлічі суб’єктивних і об’єктивних факторів.

Функціонування у форматі ринкових відносин характеризується неповною інформаційною відкритістю, наявністю протиріч, стохастичністю, тому при прийнятті управлінських рішень слід враховувати вплив ризику.

Ризик – обов’язковий атрибут бізнесу, для стимулювання розвитку якого необхідно впроваджувати в практику технічні та технологічні інновації та поширювати їх, приймаючи сміливі, неординарні рішення, що ще більшою мірою знижує визначеність [8].

Походження слова «ризик» сягає своїм корінням принаймні в сімнадцяте століття і імовірно має італійські корені. У той час слово використовувалося в розмовній мові як прототип англійського слова «hazard», що означає в перекладі – небезпека, шанс. В Англію «ризик» прийшов із Франції в середині 17 століття, як слово «risque», і одразу ж став використовуватись у Сполучених Штатах Америки. Англійське значення слова з’явилося в 1830 році у фінансових установах Лондона при страхуванні угод, які укладались з комісійними відрахуваннями.

Ці значення слова «ризик» незмінно застосовувалися протягом століть, аж до двадцятого століття, коли «risque» використовувалося в розмові як жарт.

Зараз поняття «ризик» застосовується в більш широкому сенсі, визначаючи небезпеку як таку і шлях для досягнення результатів, використовуючи шанс.

Ризикованість, як сутнісна ознака діяльності, обумовлює неможливість точного передбачення необхідних дій учасників будь-яких процесів в умовах конкуренції. Рішення в більшості випадків пов'язані з вибором сценарію розвитку подій з декількох можливих альтернатив і приймаються в умовах невизначеності прогнозування їх результатів.

Точність і достовірність проєктної інформації може бути гарантована тільки тоді, коли виконання прогнозних індикаторів повністю відповідає запланованим показникам, що в реальності практично нездійсненно [3]. В якості основних причин неточності і недостовірності планових параметрів слід відзначити такі:

- неповнота або спотвореність інформації про склад, значущість, взаємозумовленості, тенденції зміни істотних техніко-технологічних або фінансово-економічних планових показників;

- помилки в розрахунках показників внаслідок неточного використання оціночних методик або невірного підбору методів прогнозування;

- виробничо-технологічні і техногенні порушення і збої;

- коливання попиту на вироблену продукцію і валютні курси;

- закритість або неточність відомостей про фінансовий стан і ділову репутацію партнерів, що може викликати невиконання договірних зобов'язань, порушення термінів оплати і навіть банкрутство контрагентів;

- нечіткість поставлених цілей контрагентів, невизначеність їх інтересів і дій;

- нестійкість природно-кліматичних умов, можливість стихійних лих;

- нестабільність політичної ситуації, загроза негативних змін в економіці;

- недосконалість фінансово-економічного законодавства і нестійкість поточної економічної ситуації, умов інвестування, формування, розподілу і використання прибутку.

Отже, для оцінки реальних перспектив необхідна чисельна оцінка рівня потенційних ризиків.

Досвід розвитку всіх країн показує, що ігнорування або недооцінка господарського ризику при розробці тактики і стратегії, прийнятті конкретних рішень неминуче стримує розвиток суспільства, науково-технічного прогресу. Ігнорування ризику стало, мабуть, однією з причин краху СРСР, тому що держава фактично узяла ризики всіх господарюючих суб'єктів на себе. Виникнення інтересу до прояву ризику в господарській діяльності пов'язано з переходом України до ринкової системи господарювання, що вносить додаткові елементи невизначеності, розширює зони ризикових ситуацій. У цих умовах виникають неясність і невпевненість в отриманні очікуваного кінцевого результату.

У даний час не існує однозначного тлумачення терміна «ризик». Слід зазначити, що ризик у найзагальнішому його розумінні в словнику С. І. Ожегова визначається як «можлива небезпека, дія навмання в надії на щасливий результат». Найбільш широко поширена думка про ризик – можливість небезпеки або невдачі. Наприклад, з економічної точки зору ризик – це ймовірність виникнення збитків або недоотримання доходів у порівнянні з прогнозованим варіантом; ризик є об'єктивно-суб'єктивною категорією, яка пов'язана з подоланням невизначеності, випадковості і конфліктності в ситуації неминучого вибору й відображає ступінь досягнення очікуваного результату [18].

З точки зору інформаційних технологій (які розглядаються як комплекс дисциплін, що дозволяє вивчати методи для ефективної організації роботи співробітників, що займаються обробкою та збереженням важливої інформації для бізнесу) ризики передбачають можливість негативних наслідків через різні загрози, такі як віруси, методи крадіжки інформації, хакерські атаки та спеціальні види пошкодження обладнання.

До інформаційних технологій належать способи організації роботи фахівців, комп'ютерна техніка, а також низка економічних і соціальних факторів у компанії. У вузькому розумінні інформаційні технології – це система методів і структура виробничих процесів, а також програмних і

технічних засобів, що утворюють технологічний ланцюжок для збору, зберігання, обробки та обміну інформацією. Це знижує трудомісткість використання інформаційних ресурсів і забезпечує захист даних.

Вказані загрози для інформаційних технологій можуть виникати не лише на етапі створення систем, але й під час їх використання. Коли здійснюється проєктування, розробка або впровадження та модернізація інформаційних систем, виникнення IT-ризиків можна спровокувати цілою низкою чинників, які пов’язані з цією системою. До них можливо віднести такі:

- вибір неправильного рішення, спрямованого на автоматизацію;
- помилки в проєктній діяльності;
- невідповідності інфраструктури та ухваленого рішення щодо автоматизації;
- помилки під час встановлення будь-якої системи.

Під час експлуатації інформаційної системи слід враховувати такий перелік чинників, що перешкоджають досягненню бажаних цілей:

- малоефективна взаємодія таких структур, як бізнес та IT, коли потрібно визначити оптимальний рівень підтримки;
- слабкий потенціал застосування наявних технологій;
- неможливість власними силами забезпечити належний рівень супроводу та всебічного розвитку систем;
- помилки, пов’язані з розвитком інформаційних технологій.

Для попередження появи подібних загроз підприємства створюють комплексні системи, що інтегрують так званий ризик-менеджмент. А також внутрішній контроль і аудит, що виконується у вигляді основної діяльності або як засіб підтримки інформаційних технологій. Важливо розуміти, що найбільш зріла IT система має мінімальні ризики в IT сфері. Відповідно, ефективність використання IT тут на рівень вища.

У теорії ризиків використовується системний підхід. При системному підході взаємообумовленими і важливими факторами виступають як

інтеграція всіх видів діяльності для досягнення спільної мети, так і забезпечення роботи підсистем та системи в цілому в ефективному режимі. Судження і рекомендації щодо поведінки об’єкта будуються на даних аналізу і синтезу частин в інтегроване єдине ціле, яке може мати новими властивостями.

Системний підхід розглядає всю систему як сукупність складових її підсистем і різних елементів, взаємодіючих і пов’язаних між собою. При цьому і саме для цього, частини мають цільову спеціалізацію, що враховує не тільки вертикальні, але також горизонтальні і пересічні зв’язки між підсистемами.

Можна визначити такі індикатори ризику:

1) Потенційні втрати. При аналізі цих втрат можливі дві ситуації:

а) у результаті проведення заходів ситуація буде гірше;

б) результат буде по суті не відрізнятися від передбачуваного результату.

2) Випадкові втрати. Ці втрати дуже важко виміряти, оскільки вони не є очевидними до певного моменту. Випадкові втрати можуть абсолютно змінити ризикову ситуацію: усунути ризик або, навпаки, посилити його вплив.

3) Надійність. Надійність пов’язана з виробничою і підприємницькою діяльністю, визначаючи впевненість у майбутньому. Вона показує ймовірність того, що втрати не перевищують деякого рівня. При оцінці надійності вона проявляється впливом на ризик більшою мірою суб’єктивних факторів на дії, події і наслідки прийнятих рішень.

У результаті розгляду основних індикаторів ризику визначаються наступні об’єктивні позиції по відношенню до ризику: прихильне ставлення до ризику (favoring risk), вороже ставлення до ризику (adverse risk) і нейтральне ставлення до ризику (neutral risk). Ці поняття пов’язують теорію попиту і споживчого вибору з теорією ризику. Тому слід зупинитися на принципі граничної корисності.

У випадку визначеності ситуації, пов’язаної з постійною корисністю, матиме місце нейтральне ставлення до ризику. У випадку ворожого ставлення до ризику матиме місце спадна гранична корисність і тому ризикова альтернатива не вибирається. При зростаючій граничної корисності в разі успіху можливий великий виграш і, отже, має місце позитивне ставлення до ризику і вибір ризикової альтернативи.

Таким чином, термін корисності вносить нову рису в поняття ризику, що характеризується і суб’єктивними факторами.

Для того, щоб проаналізувати ситуацію, що склалася, і прийняти рішення, необхідно з’ясувати, що відомо про дану ситуацію. Для цього необхідно на додаток до категорії «ризик» ввести такі категорії, як «впевненість» і «невизначеність».

На рис. 1.1 наведені рівні прийняття рішення і взаємозв’язок між ними.

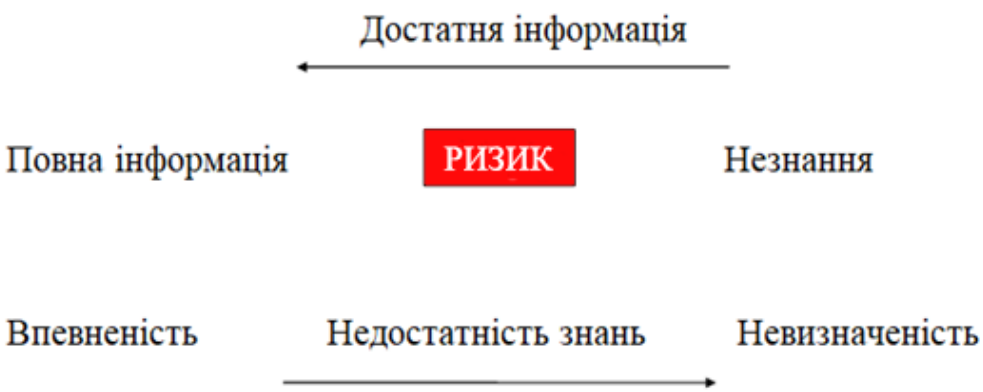


Рисунок 1.1 – Рівні прийняття рішення

Рішення, що приймаються на основі повної інформації, носять певний характер. Ці рішення приймаються з упевненістю в їх кінцевому результаті. Такі ситуації, коли кінцевий результат не можна передбачити з дійсною вірогідністю, детерміновані за своєю суттю. У плануванні такі ситуації можливі при вирішенні питань близької перспективи (оперативне рішення).

Ризик тісно пов’язаний з ймовірністю і невизначеністю.

Імовірність – це можливість отримання певного результату. Імовірність події – це певне число, яке тим більше, чим більш можлива подія. Термін

ймовірності є фундаментальним для теорії ймовірностей і дозволяє кількісно порівнювати події за можливості їх реалізації. Очевидно, що більш імовірна та подія, яка відбувається частіше. Отже, поняття ймовірності пов'язане з досвідченим практичним поняттям частоти події. Точність вимірювання ймовірностей залежить від обсягу статистичних даних і можливості їх використання для майбутніх подій, тобто збереження умов, в яких відбувалися минулі події. Але разом з тим у багатьох випадках при прийнятті рішень статистичні дані дуже малі за обсягом або взагалі відсутні. Тому використовується інший шлях вимірювання ймовірностей ситуації, заснований на суб'єктивних поглядах особи, що приймає рішення.

У зв'язку з цим вимірювані таким шляхом ймовірності називають суб'єктивними ймовірностями ситуації. При визначенні суб'єктивних ймовірностей на перше місце виступає думка суб'єкта, що відображає стан його інформаційного фонду. Інакше кажучи, суб'єктивна ймовірність визначається на основі припущення, що ґрунтується на судженні або особистому досвіді оцінювача (експерта), а не на частоті, з якою подібний результат був отриманий в аналогічних умовах. Звідси виходить широке варіювання суб'єктивних ймовірностей, яке пояснюється спектром різної інформації або можливостей оперування з однієї і тієї ж інформацією.

Практично, в момент прийняття рішення неможливо отримати повні і точні знання про віддалене в часі середовище реалізації рішення, про всі дії, які потенційно можуть проявитися у внутрішніх та зовнішніх факторах. Все це є сутністю вираження невизначеності як об'єктивної форми існування економічної діяльності. Об'єктивно існує і принципово непереборна невизначеність, що має місце при прийнятті рішень, що приводить до того, що ризик ніколи не буває нульовим. Наслідком цього є невпевненість у досягненні поставленої мети, коли в результаті реалізації обраного рішення намічена мета в більшій чи меншій мірі не досягається.

Основне джерело невизначеності – недостатність знань про навколишній світ. З подібного роду невизначеністю людина зіштовхнулася,

коли вперше стала приймати рішення. Необізнаність про закони природи заважала виробничій діяльності, не дозволяла ефективно вести господарство.

Інше джерело невизначеності – випадковість. Випадковістю називається те, що в подібних умовах відбувається неоднаково, причому заздалегідь не можна передбачити, як буде цього разу. Спланувати кожен даний випадок неможливо. Вихід обладнання з ладу, постачання неякісної сировини, непередбачене падіння попиту на продукцію – все це прояв випадковості.

Третя причина невизначеності – протидія. Так, протидія проявляється в невизначеності забезпеченням деякими ресурсами, порушенням договірних зобов'язань постачальниками, аваріями техніки, невизначеністю попиту на продукцію, труднощами її збуту.

Під ризиком розуміється можливість (ймовірність) виникнення умов, які призведуть до негативних наслідків. Негативними наслідками можуть стати: втрата частини ресурсів, недоотримання доходів, поява додаткових витрат, збитки тощо.

Ризик пов'язаний з настанням ризикових ситуацій, тобто з сукупністю подій (обставин) і умов, що створюють обстановку невизначеності, яка може як сприяти, так і перешкоджати досягненню цілей. Наявність елементів невизначеності обумовлює виникнення ситуації, яка не має однозначного результату, і тому, коли існує можливість не тільки якісної і кількісної оцінки ймовірності будь-якого з варіантів, то можна говорити про ризикову ситуацію, яка пов'язана зі статистичними процесами і характеризується такими умовами:

- наявність невизначеності, що проявляється у відсутності достовірної і повної інформації про майбутнє;
- наявність кількох альтернативних варіантів результатів (розвитку майбутнього);
- оцінка ймовірності здійснення альтернативних варіантів;
- необхідність вибору альтернативи (у тому числі і відмова від вибору);

- можливість матеріальних, моральних та інших втрат, пов’язаних з настанням ризикової ситуації.

Ситуація ризику якісно відрізняється від ситуації невизначеності. Ситуація невизначеності (тобто неповноти і неточності інформації про майбутнє) характеризується тим, що ймовірність настання результатів рішень або подій невідома. Слід розрізняти поняття «ризик» і «невизначеність». По-перше, ризик має місце тільки в тих випадках, коли приймати рішення необхідно (якщо це не так, немає сенсу ризикувати). Інакше кажучи, саме необхідність приймати рішення в умовах невизначеності породжує ризик, за відсутності такої необхідності немає і ризику.

По-друге, ризик суб’єктивний, а невизначеність об’єктивна. Наприклад, об’єктивна відсутність достовірної інформації про потенційний обсяг попиту на вироблену продукцію призводить до виникнення спектра ризиків для учасників проєкту.

Невизначеність може бути задана по-різному:

- у вигляді імовірнісних розподілів (розподіл випадкової величини точно відомо, але невідомо, яке саме значення прийме випадкова величина);

- у вигляді суб’єктивних ймовірностей (розподіл випадкової величини невідомо, але відомі ймовірності окремих подій, певні – експертним шляхом);

- у вигляді інтервальної невизначеності (розподіл випадкової величини невідомо, але відомо, що вона може приймати будь-яке значення в певному інтервалі).

Крім того, слід зазначити, що природа невизначеності формується під впливом різних факторів:

- тимчасова невизначеність зумовлена тим, що неможливо точно передбачити значення того чи іншого фактора в майбутньому;

- непередбачуваність поведінки учасників у ситуації конфлікту інтересів також породжує невизначеність.

Ситуація ризику є різновидом невизначеній ситуації. Іншими словами, ризик виникає в умовах вибору в прагненні визначити найкращий результат, коли в разі невдачі існує можливість (ступінь небезпеки) опинитися в гіршому становищі, ніж до вибору (чим у випадку нездійснення цієї дії).

В явищі «ризик» виділяють такі основні елементи, взаємозв'язок яких і становить його сутність:

- можливість відхилення від передбачуваної мети, заради якої здійснювалася обрана альтернатива;

- ймовірність досягнення бажаного результату;

- відсутність впевненості в досягненні поставленої мети;

- можливість матеріальних, моральних та інших втрат, пов'язаних із здійсненням обраної в умовах невизначеності альтернативи.

До основних рис категорії «ризик» також відносяться: суперечливість, альтернативність та невизначеність.

Суперечливість ризику проявляється в тому, що, з одного боку, він забезпечує здійснення ініціатив, новаторських ідей, експериментів, тобто прискорює суспільний і технічний прогрес. З іншого боку, ризик веде до авантюризму, волюнтаризму, гальмування соціального прогресу в тих випадках, коли альтернатива в умовах ризику вибирається без належного урахування об'єктивних закономірностей розвитку явища. Альтернативність пов'язана з необхідністю вибору з декількох можливих варіантів рішення. Там, де немає вибору, не виникає ризикована ситуація, немає і ризику. Залежно від конкретного змісту ситуації ризику альтернативність дозволяється різними способами. У простих ситуаціях вибір здійснюється на підставі минулого досвіду і інтуїції, у складних ситуаціях необхідне використання спеціальних методів і методик.

Як правило, безризикові рішення одночасно є консервативними та навіть застійними.

Функціонування будь-якого суб'єкта підприємництва на різних етапах та в найрізноманітніших сферах діяльності пов'язане з невизначеністю.

Існування невизначеності в діяльності суб'єктів господарювання є причиною виникнення ризиків, без яких неможливий ефективний розвиток підприємства.

Уникнути невизначеності в підприємництві неможливо, адже вона являє собою елемент об'єктивної дійсності, тому, що завжди існує аспект неоднозначності розвитку, неможливості точного прогнозування певних подій, неповної чи недостовірної інформації.

Першопричиною, необхідною умовою виникнення підприємницьких ризиків виступає невизначеність результатів діяльності. Слід зазначити, що вже понад сто років триває наукова дискусія з приводу взаємовідношення понять «ризик» та «невизначеність». Невизначеність ситуації характеризується тим, що вона залежить від багатьох змінних чинників, контрагентів, дії яких неможливо передбачити з прийнятною точністю. На підвищення ступеня ризику впливає також і відсутність (неоднозначність) чітко визначених цілей та критеріїв їхньої оцінки, зрушення в суспільних потребах і споживчому попиті, непередбачувана поява нових технологій і техніки, зміна кон'юнктури світового ринку, корекція траєкторії руху економіки з політичної необхідності, непередбачуваність природних явищ тощо.

Залежно від засобів визначення ймовірності невизначеність буває статистична та нестатистична. Статистична невизначеність – визначені параметри можуть спостерігатися достатньо для визначення частоти появи події кількість разів за допомогою статистичних даних, імітації, моделювання, експерименту. Імовірність розглядається як об'єктивна ймовірність настання події. Визначається на основі реальних даних через відносну частоту. Нестатистична (апріорна, суб'єктивна) невизначеність – подія повторюється не часто або зовсім не спостерігається, і її реалізація можлива тільки в майбутньому. Імовірність розглядається як ступінь упевненості, що ця подія відбудеться, тобто це – суб'єктивна ймовірність. Визначається на основі опитувань, імовірностей.

За ступенем ймовірності настання подій є повна невизначеність, повна визначеність та часткова невизначеність.

Повна невизначеність – близький до 0 ступінь прогнозованості (ймовірності) настання подій

$$\lim_{t \to n} P_i = 0,$$

де P_i – прогнозованість настання події i; t – час; n – кінцевий час прогнозування події. У даному випадку повністю відсутня можливість будь-яким чином прогнозувати перспективи розвитку і підприємства, і ринку в цілому.

Повна визначеність – близький до 1 ступінь прогнозованості (ймовірності) настання подій

$$\lim_{t \to n} P_i = 1$$

забезпечує можливість зі 100 %-ю ймовірністю прогнозувати не тільки стратегію підприємства на ринку, а й ситуацію, тенденції розвитку тощо.

Часткова невизначеність – ступінь прогнозованості (імовірності) настання події знаходиться в межах від 0 до 1

$$0 < \lim_{t \to n} P_i < 1$$

має конкретний практичний характер порівняно з попередніми видами, що є теоретичними припущеннями про можливості суб'єктів господарювання.

За об'єктом невизначеності виділяють людську, технічну та соціальну невизначеність. Людська невизначеність пов'язана з неможливістю точного передбачення поведінки людини в процесі роботи через відмінності в рівні освіти, емоційно-психологічному настрої, світогляді кожної особи. Технічна невизначеність пов'язана з надійністю обладнання, непередбаченістю виробничих процесів, складністю технології, рівнем автоматизації, темпами оновлення, обсягами виробництва. Соціальна невизначеність зумовлена прагненням людей утворювати соціальні зв'язки та поводитися відповідно до загальноприйнятих норм, традицій, узятих на себе зобов'язань.

Ризик може характеризуватися з об’єктивної і суб’єктивної точок зору. Суб’єктивна сторона ризику проявляється в тому, що люди неоднаково сприймають одну і ту ж величину ризику в силу відмінності психологічних, моральних, ідеологічних, релігійних принципів, установок. Об’єктивна сторона ризику обумовлена тим, що ризик існує незалежно від того, усвідомлюють його наявність чи ні, враховують або ігнорують його. Об’єктивне існування ризику проявляється і в тому, що він відображає реально існуючі явища, процеси, сторони життя. Тому помилково вважати, що ризик породжується тільки дефіцитом інформації і ставленням до нього суб’єкта. Природа його пов’язана з закономірностями розвитку зовнішнього і внутрішнього середовища організації, спонтанністю, випадковістю, недосконалістю, конфліктом інтересів і наявністю суперечливих і навіть антагоністичних тенденцій.

Отже, існування ризику безпосередньо пов’язано з невизначеністю, яка неоднорідна за формою прояву і за змістом. Ризик є одним із способів «зняття» невизначеності, яка є незнання достовірного, відсутність однозначності. Тому необхідно досліджувати джерела ризику.

Таким чином, процес прийняття рішення з точки зору «впевненості» включає в себе такі кроки:

1) визначення альтернативних ліній поведінки;

2) розрахунок витрат по кожному варіанту і їх окупність (покриття);

3) вибір найкращого варіанта з використанням економіко-математичних методів або шляхом перерахування варіантів.

Процес прийняття рішення в ризиковій ситуації з точки зору «невизначеності» повинен містити такі моменти:

1) використання критерію очікуваної величини покриття витрат, беручи до уваги ризик, який ускладнює поняття рішення;

2) очікувана величина покриття є сумою окремих величин, впливають на ймовірність настання випадкової події;

3) інші критерії вибору можуть бути також використані, особливо в ситуаціях, що не повторюються, наприклад, обмеження втрат.

До причин виникнення невизначеності та ризику також відносяться:

- обмеженість і недостатність ресурсів (матеріальних, фінансових, трудових тощо) при прийнятті та реалізації рішень;

- неможливість однозначного пізнання об'єкта при сформованих у даних умовах рівні і методах наукового пізнання;

- відносна обмеженість свідомої діяльності людини, наявність відмінності в людей поводжень, психологічних установок, оцінок тощо.

Оскільки існування ризику пов'язане безпосередньо з наявністю невизначеності, тому і основними причинами невизначеності, тобто джерелами ризику являються:

- спонтанність природних процесів і явищ, стихійні лиха. Землетруси, повені, бурі, урагани, морози, ожеледь, град, гроза, посуха та інші подібні явища можуть негативно вплинути на результати діяльності;

- випадковість, тобто при здійсненні своєї діяльності завжди потрібно враховувати непередбачені випадки, наприклад, різного роду аварії (пожежа, вибух тощо), вихід з ладу обладнання, нещасні випадки, пов'язані з транспортом, виробництвом і багато іншого. Крім цього, це зумовлює неможливість однозначного передбачення настання передбачуваного результату. Наприклад, неможливо точно передбачити число пасажирів, які скористаються транспортом визначеного маршруту;

- наявність протиборчих тенденцій, зіткнення суперечливих інтересів. Наприклад, у результаті військових дій організації можуть зіткнутися із забороною на експорт або імпорт, конфіскацією товарів, обмеженням іноземних інвестицій, заморожуванням активів тощо. Іншим прикладом є застосування недобросовісної конкуренції, тобто один з конкурентів ускладнює іншому здійснення своєї діяльності незаконними і нечесними діями, такими як підкуповування посадовців, паплюження конкурента, спричинення йому прямих збитків;

- імовірнісний характер науково-технічного прогресу, тобто заздалегідь у всій повноті визначити конкретні наслідки тих чи інших наукових відкриттів, технічних винаходів практично неможливо, що і формує невизначеність і ризик.

Існування невизначеності пов'язано також з неповнотою, недостатністю інформації про об'єкт, процес, явище, по відношенню до якого приймається рішення, з обмеженістю людини в зборі та переробці інформації, з постійною мінливістю цієї інформації. І чим нижче якість даних, що застосовуються і враховуються під час прийняття рішень у діяльності, тим вище ризик отримання негативних результатів і наслідків у ній.

Крім названої вище загальної класифікації джерел ризику, можна також їх розділити на три групи:

- внутрішні джерела ризику. Працівник (людина) – найрозвиненіша істота і тому найнепередбачуваніша. Людині властиво помилятися, недобробляти, затримуватись, недбало ставитися до роботи. Люди періодично обманюють і крадуть, шахраюють різними способами. Людина може захворіти та не вийти на роботу. Устаткування – може спричинити збій або вийти з ладу. Неправильно поставлені цілі – наприклад, завдання збільшити частки ринку за будь-яку ціну може призвести до серйозних збитків;

- зовнішні джерела ризику. Конкуренти становлять постійну загрозу. Постачальники можуть недоставити або вимагати невиправдано високу ціну, або надто жорсткі умови контракту, а також можуть давати хабарі працівникам організаціям-замовникам для отримання вигідних замовлень. Клієнти можуть не сплатити за товари (наприклад, використання піратських копій програмного забезпечення), а також можуть не виконувати умови контракту (порушення умов ліцензійної угоди щодо використання придбаного програмного забезпечення). Законодавство (податкове, екологічне, трудове та ін.) – наприклад, митні правила, недотримання яких загрожує штрафами підприємству порушника. Політичні події – наприклад,

війна може змусити згорнути продажі. Суспільна думка – наприклад, споживачі можуть відмовитися від придбання бренду внаслідок негативного ставлення до поточної політики. Стан економіки та фінансів – наприклад, загроза різкої девальвації валюти. Конкуренти, постачальники та клієнти – це персоніфіковані джерела ризику, інші – не персоніфіковані;

- природні фактори. Явища є також джерелами ризику – блискавка може спричинити пожежу будівлі, дощ може протікати через дах та залити сервер, снігопад може завалити в'їзд на склад тощо.

Отже, структура ризику є сукупністю таких елементів, як джерело ризику (події, що становлять загрозу виникнення втрат або шанс отримання додаткових вигод у випадку відмови від ризику), об'єкт ризику (те, на що впливає джерело ризику) та наслідки реалізації ризику (результат втілення загрози або шансу), які перебувають у взаємозв'язку, як наведено на рис. 1.2.

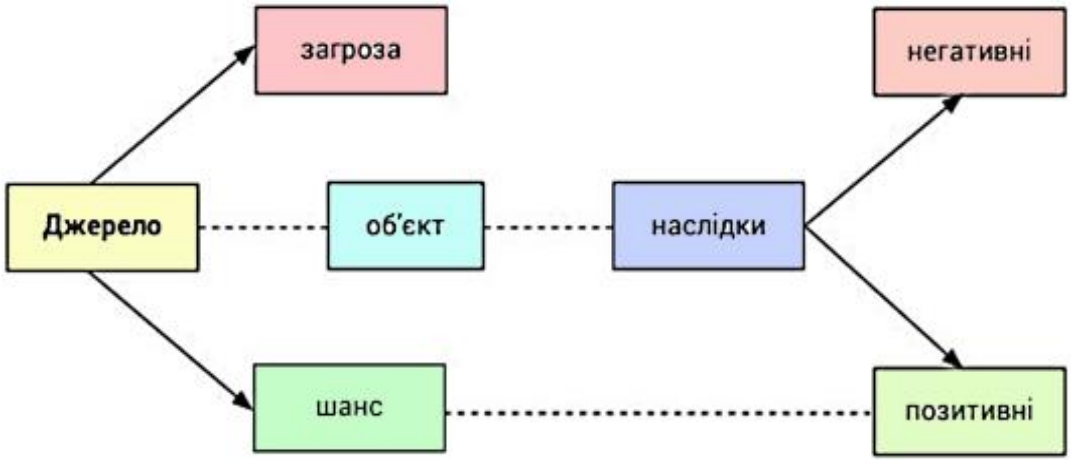


Рисунок 1.2 – Структура ризику

Чинники ризиків можна класифікувати за такими ознаками [11]:

1. За масштабом впливу:

- мегаризики – це ризики, які мають наднаціональний характер, охоплюють кілька країн одночасно та можуть мати тривалий вплив (до 10 років і більше);

- макроризики – схожі за своєю природою з мегаризиками, але їхня дія обмежується межами однієї країни;

- мезоризики – впливають на окремі галузі економіки. Наприклад, галузеві ризики визначають ймовірність коливань фінансових результатів підприємств через зміни в економічному стані конкретної галузі;

- мікроризики – виникають на рівні окремих підприємств і обумовлені дією як суб'єктивних, так і об'єктивних чинників.

2. За можливістю контролю та управління:

- контрольовані фактори – це ті, які можна ідентифікувати за допомогою якісного аналізу та впливати на них через прийняття відповідних рішень;

- неконтрольовані фактори – поділяються на невизначені (оцінити ймовірність їх виникнення складно, а наслідки варіюються у визначених межах) та визначені (ймовірність їх виникнення оцінюється за статистичними даними).

3. За походженням:

- внутрішні фактори – пов'язані з діяльністю конкретного підприємства і охоплюють всі процеси в його виробництві, обігу та управлінні (стратегія, особливості ресурсної бази, рівень впровадження нових технологій тощо). Вони поділяються на об'єктивні (не залежать від людського фактора, як-от раптові зміни у виробничих процесах, впровадження технологій) та суб'єктивні (залежать від людського фактора, наприклад, якості трудових ресурсів);

- зовнішні фактори – обумовлені зовнішнім середовищем, на яке підприємство не може впливати, але має адаптуватися та використовувати можливості, які воно пропонує.

4. За характером впливу:

- фактори прямої дії – це, наприклад, правове та нормативне регулювання, бюджетна та грошово-кредитна політика, дії органів влади, дії контрагентів (постачальників, споживачів, конкурентів), а також загрози від злочинних угруповань;

- фактори опосередкованої дії – включають стабільність політичної, економічної, соціальної, демографічної та екологічної ситуації в країні чи регіоні, форс-мажорні обставини (стихійні лиха), особливості зовнішньоекономічної політики країни, її геополітичне становище та вплив науково-технічного прогресу.

Варто зазначити, що наявність ризиків може мати і позитивний вплив, проявляючись через його функції:

1. Інноваційна функція – полягає в тому, що наявність ризику стимулює застосування новаторських методів ведення бізнесу. Це приносить користь споживачам (інноваційні товари та послуги), конкретному підприємству (зростання прибутку) і країні загалом (посилення конкурентоспроможності на зовнішніх ринках).

2. Захисна функція – виражається в здатності підприємства знаходити і застосовувати різноманітні засоби та методи для запобігання збиткам, як-от правові, політичні, економічні гарантії або соціальний захист.

3. Регулятивна функція – передбачає постійний аналіз ризикових ситуацій, оцінку рівня ризику та коригування прийнятих рішень. При цьому виділяють конструктивну сторону регулятивної функції (позитивний вплив через стимулювання інноваційної діяльності) і деструктивну сторону (негативний вплив у вигляді підвищення ймовірності втрат через необґрунтовані рішення та ігнорування ризиків).

4. Аналітична функція – реалізується через необхідність аналітичного підходу при ухваленні рішень, використовуючи інтуїцію, досвід або методи аналізу для вибору оптимального рішення та уникнення можливих втрат.

Ідентифікація ризиків залежить від сутності та контексту їхніх джерел, подій, причин та наслідків [22].

Джерело ризику – це об’єкт або явище, яке має специфічний потенціал, здатний самостійно або в поєднанні з іншими факторами викликати ризик. Джерела ризику можуть бути як матеріальними, так і нематеріальними.

Подія – це виникнення чи зміна певного явища або комбінації обставин, яка може мати різні прояви та причини.

Наслідки – це результати подій, які можуть впливати на досягнення цілей. Події можуть викликати як позитивні, так і негативні наслідки, що можуть бути чітко визначеними або невизначеними та виражатися кількісно або якісно.

Щоб визначити ризики, необхідно розуміти контекст ризикової діяльності бізнесу, що дозволяє створити повний опис ризиків конкретного виду діяльності організації. Важливо застосовувати комплексний підхід для максимально повного виявлення ризиків у роботі компанії. Одним із способів вирішення цього завдання є класифікація ризиків, яка допомагає систематизувати ризики з урахуванням причинно-наслідкових зв’язків між ключовими елементами ідентифікації.

Ідентифікувати ризики можна, аналізуючи причини ризикових подій та їхні наслідки. Інший підхід полягає в тому, щоб, маючи інформацію про наявні або можливі наслідки чи відмови, визначити причини таких подій на основі вже відомих даних. Ідентифікація ризиків дозволяє окреслити межі для управління ризиками, а також містить уточнення контексту ризику, що охоплює визначення внутрішніх і зовнішніх параметрів, сфери впливу та критеріїв ризиків.

Основний алгоритм дій при ідентифікації ризиків:

1. Визначення джерел і чинників ризику.
2. Визначення можливих наслідків ризикової ситуації:

   а) зміна запланованого результату (збільшення або зменшення);

   б) вплив на ймовірність досягнення запланованих цілей (підвищення чи зниження);

   в) потреба в залученні додаткових дій або ресурсів з боку учасників;

   г) відкриття нових перспективних можливостей.
3. Визначення причин виникнення ризикової ситуації.
4. З’ясування потенційного місця виникнення ризикової ситуації.

5. Визначення можливого часу виникнення ризикової ситуації.

6. Аналіз впливу та наслідків ризикової ситуації.

Під час ідентифікації ризиків доцільно використовувати методи, чия ефективність вже підтверджена практичним досвідом (табл. 1.1).

Таблиця 1.1 – Методи ідентифікації ризиків

Метод	Сфера використання
Мозковий штурм	Прогнозування ситуацій у випадку браку даних або потреби в нестандартних методах для вирішення проблем
Структуровані або частково структуровані інтерв'ю	Збір початкових даних для оцінки ризиків зацікавленими сторонами
Метод Дельфі	Використання експертних оцінок на всіх етапах ризик-менеджменту або життєвого циклу системи, де потрібна додаткова оцінка
Контрольні листи	Створення списків можливих небезпек, ризиків та відмов засобів управління, ґрунтуючись на попередньому досвіді, результатах оцінок ризику або минулих відмовах
Попередній аналіз небезпек (PHA)	Виявлення небезпек, ситуацій та подій, які можуть порушити роботу чи спричинити шкоду для обладнання, систем або діяльності
Дослідження небезпеки та працездатності (HAZOP)	Застосування підказок для виявлення причин, чому проєктні цілі або умови функціонування можуть не досягатися на різних етапах процесу або системи
Аналіз небезпеки і критичних контрольних точок (HACCP)	Структурована ідентифікація небезпек та перевірка засобів управління в усіх етапах процесу, щоб забезпечити надійність продукції, захист від небезпек та мінімізацію ризику
Структурований аналіз сценаріїв (SWIFT)	Використання фраз-підказок для ідентифікації небезпечних ситуацій та розробки сценаріїв їх розвитку групою
Аналіз першопричини (RCA, RCFA)	Дослідження втрат від відмов, оцінка фінансових чи економічних збитків через вплив зовнішніх чинників, пошук корінних причин відмов
Аналіз видів і наслідків відмов (FMEA) або аналіз видів, наслідків та критичності відмов (FMECA	Визначення всіх видів відмов частин і компонентів системи, наслідків відмови, механізмів та способів досягнення безперебійної роботи або пом'якшення наслідків для системи; оцінка значущості кожного виду відмови
Аналіз дерева несправностей (FTA)	Аналіз чинників, що можуть спричинити небажану подію, шляхом створення діаграм у вигляді дерева, яке відображає зв'язки цих факторів із кінцевою подією
Аналіз дерева подій (ETA)	Аналіз послідовностей подій після початкової події, враховуючи роботу або відмову систем, призначених для пом'якшення наслідків небезпечної події
Аналіз причин і наслідків	Аналіз критичної події та її наслідків через логічне поєднання елементів "ТАК/НІ", щоб визначити працездатність або відмову систем, розроблених для зменшення наслідків початкової події.

1.2. Класифікація факторів ризиків

Діяльність у галузі управління ризиком можна визначити як процес підготовки і реалізації заходів, мета яких – зниження небезпеки прийняття помилкового рішення і зменшення можливих негативних наслідків небажаного розвитку подій у ході реалізації прийнятих рішень [4].

До тих пір, поки ризик невизначений, неможливо зробити будь-які заходи щодо його мінімізації. Тому першою стадією тут вважається ідентифікація ризиків. Це може здійснюватися різними способами: від чисто інтуїтивних здогадів до складного імовірнісного аналізу в моделях дослідження операцій.

У табл. 1.2 наведено одну з можливих класифікацій ризиків.

Таблиця 1.2 – Класифікація ризиків за певними ознаками

№	Класифікаційні ознаки	Види ризиків
1	**2**	**3**
1	Зв’язок із підприємницькою діяльністю	- підприємницькі - непідприємницькі
2	Приналежність до країни функціонування суб’єкта господарювання або в сфері їх виникнення	- внутрішні - зовнішні
3	Рівень виникнення	- фірмові (мікрорівень) - галузеві - міжгалузеві - регіональні - державні - глобальний (світовий)
4	Сфера походження	- соціально-політичні - адміністративно-законодавчі - виробничі - комерційні - фінансові - природно-екологічні - демографічні - геополітичні

Продовження таблиці 1.2.

1	2	3
5	Причини виникнення	- ризики, пов’язані з невизначеністю майбутнього - ризики, пов’язані з нестачею інформації - ризики, що виникають через суб’єктивний вплив
6	Ступінь обґрунтованості прийняття ризику	- обґрунтовані - частково обґрунтовані - авантюрні
7	Ступінь системності	- системні - несистемні (унікальні)
8	Відповідність допустимим межам За рівнем небезпеки для діяльності	- допустимі - критичні - катастрофічні
9	Реалізація ризиків	- реалізовані - нереалізовані
10	Тривалість у часі	- постійні - короткочасні
11	Адекватність часу ухвалення рішення реагування на реалізацію ризиків	- попереджувальні - поточні - запізнілі
12	Група, що аналізує ризик та приймає рішення про поведінку у випадку її реалізації	- індивідуальне рішення - колективне рішення
13	Масштаб впливу	- одноособливі - багатоособливі
14	Можливість прогнозування	- прогнозовані - частково не прогнозовані
15	Ступінь впливу на діяльність	- негативні - нульові - позитивні
16	За рівнем правомірності ризику	- виправдані - невиправдані
17	З можливістю страхування	- страховані - нестраховані
18	За масштабом схильності	- загальні - специфічні

Як видно з табл. 1.2, ризики розрізняються між собою за місцем і часом виникнення, сукупністю зовнішніх і внутрішніх факторів, що впливають на їх величину, і, отже, за способами їх аналізу та методами впливу. Відповідно до цього існує безліч підходів до класифікації ризиків, які розрізняються підставами класифікації. Так, в основі найчастіше використовуваних

класифікаційних схем використовуються такі елементи: час, сфера та основні фактори виникнення; характер обліку і наслідків тощо.

Ефективність організації управління ризиком насамперед визначається правильною ідентифікацією ризику по науково розробленій класифікаційній системі. Така система містить категорії, групи, види, підвиди і різновиди ризиків і створює передумови для ефективного застосування відповідних методів і прийомів управління ризиком. Причому кожному ризику відповідає свій прийом управління ризиком.

Перш за все, залежно від можливого результату (ризикової події), ризики можна поділити на дві великі групи: чисті і спекулятивні.

Чисті ризики означають можливість отримання негативного чи нульового результату. До них відносяться ризики природні, екологічні, політичні, транспортні і частина комерційних ризиків (майнові, виробничі, торгові).

Спекулятивні ризики виражаються в можливості отримання як позитивного, так і негативного результату. До них відносяться фінансові ризики, які є частиною комерційних ризиків.

Найчастіше для впорядкування і структуризації процесу прийняття фінансових управлінських рішень виділяються за ступенем їх зниження за допомогою диверсифікації такі види ризиків:

- систематичний, або β-ризик, тобто частина ризику, яка не може бути ліквідована диверсифікацією (не «піддається» диверсифікації);

- несистематичний ризик – ризик, який піддається диверсифікації (на відміну від систематичного ризику).

Залежно від основної причини виникнення (базисна або природна ознака) ризики поділяються на такі категорії: природні, екологічні, політичні, транспортні і комерційні.

Залежно від виду факторів, що обумовлюють настання ризикових подій, виділяють:

- ризики, які залежать від зовнішнього середовища (інфляційні, валютні, кредитні);

- ризики, пов’язані з діяльністю самого підприємства (ризик ліквідності, помилкового способу вкладення капіталу і формування інвестиційного портфеля (інвестиційний портфель – це комбінація з фінансових і нефінансових активів), неефективного управління оборотними засобами, створення оптимальної структури пасивів тощо).

На ризики, які залежать від зовнішнього середовища, впливають такі категорії ризиків зовнішнього середовища, як політичні, природні, макроекономічні (зміна податкового, митного законодавства, правил і норм валютного регулювання тощо). Ризики, що залежать від діяльності самого підприємства, пов’язані з іншими видами ризиків:

- виробничим (неритмічність роботи, збої, зупинка виробництва);

- комерційним (порушення або непередбачена зміна умов договору, зміна постачальника, зміна попиту);

- транспортним (затримка в дорозі, погіршення якості в процесі транспортування) тощо.

До природних відносяться ризики, пов’язані з проявом стихійних сил природи: землетрус, повінь, буря, пожежа, епідемія тощо.

Екологічні ризики – це ризики, пов’язані з забрудненням навколишнього середовища. Під екологічним ризиком розуміється ймовірність настання цивільної відповідальності за нанесення шкоди навколишньому середовищу, а також життю та здоров’ю третіх осіб. Він може виникнути в процесі будівництва і експлуатації виробничих об’єктів і є складовою частиною промислового ризику.

Шкода навколишньому середовищу виражається у вигляді забруднення або знищення лісових, водних, повітряних і земельних ресурсів (наприклад, у результаті пожежі або будівельних робіт), нанесення шкоди біосфері і сільськогосподарським угіддям. Під словами «нанесення шкоди життю та здоров’ю третіх осіб» розуміється результат шкідливого впливу факторів

виробничої діяльності на населення, яке мешкає або знаходиться поблизу промислового об’єкту, що виражається у вигляді збільшення захворюваності та смертності.

Ризики виникнення громадянської відповідальності за нанесення в процесі виробництва шкоди третім особам, в якості яких можуть виступати як юридичні (організації), так і фізичні (населення) особи, реалізуються в результаті аварій, наднормативних викидів і витоку шкідливих речовин на виробничих об’єктах, що впливає на навколишню територію.

Наслідки аварії в даному випадку можна розділити на найближчі і віддалені. Під найближчими наслідками розуміється безпосередній збиток у вигляді руйнування будівель і споруд, забруднення території, травм і загибелі людей тощо. Віддалені наслідки виникають у вигляді довгострокового забруднення ґрунту, водних та інших природних ресурсів і подальшого впливу такого забруднення на здоров’я людей. Вони проявляються у вигляді різних захворювань, причому найчастіше через кілька років після аварії. Крім того, ознаками наявності віддалених наслідків є загальне зниження якості життя на території, порушеній аварією, підвищення рівня смертності та частоти хронічних захворювань, зростання дитячої смертності, збільшення кількості ослаблених дітей тощо.

Характерний приклад наявності прямих і віддалених наслідків – аварія на Чорнобильській АЕС 1985 р., де в результаті аварійно-рятувальних робіт великі дози опромінення отримали групи так званих ліквідаторів. У результаті забруднення значної частини території постраждала велика кількість мирного населення. Прямі втрати в даному випадку виражаються у вигляді випадків захворювань на променеву хворобу і загибелі людей, втрати сільськогосподарських угідь, витрат на відселення населення із заражених областей. Віддалені наслідки проявилися насамперед у погіршенні загального стану здоров’я опромінених груп населення. Відомо, що в осіб, які потрапили в зону радіоактивного зараження, збільшується сприйнятливість до звичайних інфекцій типу грипу або ГРЗ. Основні

віддалені наслідки проявилися через 10 років після аварії у вигляді збільшення частоти ракових захворювань, особливо раку щитовидної залози.

Таким чином, не можна недооцінювати можливість виникнення віддалених наслідків аварій на об'єктах промисловості, тим більше якщо вони надалі виражаються у вигляді збільшення захворюваності або смертності населення. У світовій страховій практиці є випадки, коли позови з приводу віддалених наслідків роботи на небезпечних виробництвах приводили до виплати компенсацій, розмір яких у багато разів перевищував розміри прямих збитків.

Політичні ризики пов'язані з політичною ситуацією в країні і діяльністю держави. Політичні ризики виникають при порушенні умов виробничо-торгового процесу з причин, безпосередньо не залежать від господарюючого суб'єкта.

До політичних ризиків відносяться:

а) неможливість здійснення господарської діяльності внаслідок військових дій, революції, загострення внутрішньополітичної ситуації в країні, націоналізації, конфіскації товарів і підприємств, введення ембарго, через відмову нового уряду виконувати прийняті попередниками зобов'язання тощо;

б) введення відстрочки (мораторію) на зовнішні платежі на певний строк через настання надзвичайних обставин (страйк, війна тощо);

в) несприятлива зміна податкового законодавства;

г) заборона або обмеження конверсії національної валюти у валюту платежу. У цьому випадку зобов'язання перед експортерами може бути виконане в національній валюті, яка має обмежену сферу застосування.

Транспортні ризики – це ризики, пов'язані з перевезеннями вантажів транспортом: автомобільним, морським, річковим, залізничним, літаками тощо.

Комерційні ризики являють собою небезпеку втрат у процесі фінансово-господарської діяльності. Вони означають невизначеність

результату від даної комерційної справи. Комерційні ризики, пов’язані з можливістю недоотримання прибутку або виникнення збитків у процесі проведення торгових операцій, можуть проявлятися у вигляді такиі подій: неплатоспроможність покупця до моменту оплати товару; відмова замовника від оплати продукції; зміна цін на продукцію після укладення контракту; зниження попиту на продукцію.

Збільшення внутрішніх ризиків значно зростає в кризовій ситуації, що може бути викликано різними обставинами:

- виробничими і фінансовими проблемами,

- збільшеною недовірою постачальників і кредиторів, невпевненістю серед менеджерів, розбіжностями серед власників тощо.

По структурній ознаці комерційні ризики поділяються на майнові, виробничі, торгові, фінансові.

Майнові ризики – це ризики, пов’язані з імовірністю втрат майна громадянина (підприємця) з причини крадіжки, диверсії, халатності, перенапруги технічної і технологічної систем тощо.

Виробничі ризики – це ризики, пов’язані зі збитком від зупинки виробництва внаслідок впливу різних чинників, і перш за все – з загибеллю або ушкодженням основних і оборотних фондів (обладнання, сировина, транспорт тощо), а також ризики, пов’язані з впровадженням у виробництво нової техніки і технології. Технічними ризиками супроводжується процес нового будівництва і подальшої експлуатації побудованих об’єктів. Технічні ризики можуть бути складовою частиною промислових, підприємницьких і інвестиційних ризиків.

Технічні ризики поділяються на будівельно-монтажні та експлуатаційні. До будівельно-монтажних відносяться такі ризики:

- втрати або пошкодження будівельних матеріалів і обладнання в результаті стихійних лих, вибуху, пожежі, терористичних актів, дій зловмисників та інших несприятливих подій;

- порушення функціонування об’єкта внаслідок помилок проєктування і монтажу;

- нанесення фізичної шкоди персоналу, зайнятому на будівництві об’єкта.

Після закінчення будівництва об’єкта і здачі замовнику підрядник приймає на себе гарантійні зобов’язання щодо забезпечення його безперебійної експлуатації протягом гарантійного терміну. У випадку виявлення істотних дефектів будівельної частини робіт або встановленого обладнання і необхідності їх усунення підрядник може зазнати великих збитків і опинитися не в змозі виконати взяті на себе раніше зобов’язання. Такий ризик називається ризиком невиконання післяпускових гарантійних зобов’язань.

Під промисловими ризиками розуміється небезпека:

- нанесення шкоди організації і третім особам у результаті порушення нормального ходу виробничого процесу;

- пошкодження або втрати виробничого обладнання та транспортних засобів, руйнування будівель та споруд внаслідок впливу зовнішніх факторів у вигляді стихії або навмисних дій зловмисників.

Для промислового виробництва найбільш серйозним є ризик виникнення відмов машин і обладнання аж до найважчих його проявів у вигляді аварій. Як причини реалізації зазначених ризиків можуть виступати різні події:

- природного характеру – землетрус, повінь, зсув, ураган, смерч, блискавка, шторм, вулканічна активність;

- техногенного характеру – фізичний і моральний знос будинків, споруд, машин і обладнання, помилки проєктування, неточності монтажу, навмисні дії зловмисників, людський фактор, поломки устаткування при будівельних і ремонтних роботах, падіння літальних апаратів або їх частин;

- змішаного характеру – порушення природно-кліматичного балансу внаслідок техногенної діяльності людини, наприклад: виникнення

нафтогазового фонтану при розвідувальному бурінні свердловин, поява зсувів при проведенні будівельних робіт.

Ці події викликають кілька груп несприятливих наслідків:

- вибух може статися через витік газу і виникнення горючої газоповітряної суміші. До вибуху або розриву найчастіше схильні механізми, що володіють значною внутрішньою енергією. Це котли, компресори, насоси, парові турбіни, двигуни внутрішнього згоряння;

- пожежа може виникнути в результаті вибуху або загоряння легкозаймистих речовин;

- поломка механізмів і обладнання містить найбільш широкий клас наслідків – механічна поломка або пошкодження, порушення електричної частини обладнання, руйнування матеріалів у результаті хімічного впливу, корозія. Найбільш часто відбувається руйнування обертових частин обладнання;

- нанесення шкоди навколишньому середовищу може відбуватися в процесі промислового виробництва при витоках і викидах в атмосферу отруйних речовин, пожежах, вибухах, забрудненні акваторії світового океану в результаті аварії суден тощо. Крім того, шкоди навколишньому середовищу завдається при освоєнні природних ресурсів, будівництві промислових об’єктів;

- нанесення шкоди персоналу – це наслідок виникнення аварійної ситуації на підприємстві. Аварія може привести до загибелі людей або до втрати працездатності. Крім того, персонал може понести економічний збиток, пов’язаний з вимушеним безробіттям у результаті зупинки виробництва;

- нанесення шкоди третім особам відбувається в результаті вибуху або поширення отруйних речовин за межі підприємства. При цьому можливий як майновий збиток населенню і організаціям, так і фізичний збиток здоров’ю людей;

- зниження виробництва продукції і зупинка виробництва є наслідками аварії або поломки обладнання. Зниження виробництва призводить до прямих втрат прибутку через зменшення випуску продукції або надання послуг, а також до непрямих втрат через недопоставки продукції споживачам і подачі ними судових позовів на контрагента.

Торговими ризиками є ризики, пов’язані зі збитком через затримку платежів, відмови від платежу в період транспортування товару, непостачання товару тощо.

Підприємницькі ризики класифікуються на внутрішні і зовнішні. Зовнішні пов’язані з нанесенням збитків і неотриманням підприємцем очікуваного прибутку внаслідок порушення своїх зобов’язань контрагентами підприємця або з інших не залежних від нього обставини. Внутрішні залежать від здатності підприємця організувати виробництво і збут продукції. На них впливають такі чинники: рівень менеджменту, собівартість, якість і надійність продукції, умови збуту, реклама, організація післяпродажного сервісу, наявність обігових коштів, клієнтура тощо.

Збиток від підприємницьких ризиків буває прямим і непрямим. Прямий збиток – це втрати основних і оборотних фондів, фізичний збиток персоналу, фізичний і майновий збиток третім особам (населенню і організаціям).

Непрямий збиток – це неотримання доходу (упущена вигода) внаслідок перерви в господарській діяльності з різних причин.

Підприємницькі ризики можуть бути обумовлені такими причинами:

- природними – землетрус, повінь, ураган, смерч, удар блискавки, шторм (на морі), виверження вулкана тощо;

- падінням літальних апаратів та їх частин;

- зносом будинків і споруд, поломками машин і устаткування;

- помилками персоналу;

- зловмисними діями;

- порушенням своїх зобов’язань контрагентами підприємця за угодами;

- непередбаченими витратами.

Якщо підприємницька діяльність пов’язана з проведенням торгових операцій, то вона схильна до комплексу комерційних ризиків, а якщо здійснюється на території зарубіжних країн – комплексу країнових ризиків. Різні види підприємництва можуть бути також схильні до дії окремих видів фінансових ризиків.

Якщо на кризове становище підприємства накладається загальноекономічна криза в країні, то ризик може зрости багаторазово. Наприклад, різке зростання ціни на нафту може розглядатися як приклад систематичного ризику; збільшення ціни може збільшити собівартість продукції в усіх галузях; перемикання активів з однієї компанії на іншу не дозволить знизити збитки для інвестора.

Фінансові ризики пов’язані з імовірністю втрат фінансових ресурсів [3]. Фінансовий ризик являє собою функцію часу. Як правило, ступінь ризику для даного фінансового активу або варіанта вкладення капіталу збільшується в часі. Фінансові ризики підрозділяються на два види:

- ризики, пов’язані з купівельною спроможністю грошей;
- ризики, пов’язані з вкладенням капіталу (інвестиційні ризики).

До ризиків, пов’язаних з купівельною спроможністю грошей, відносяться такі різновиди ризиків: інфляційні і дефляційні ризики, валютні ризики, ризик ліквідності.

Інфляційний ризик – це ризик того, що при зростанні інфляції одержувані грошові доходи знецінюються з погляду реальної купівельної спроможності швидше, ніж ростуть. У таких умовах підприємець несе реальні втрати.

Дефляційний ризик – це ризик того, що при зростанні дефляції відбувається падіння рівня цін, погіршення економічних умов підприємництва і зниження доходів.

Валютні ризики є небезпекою валютних втрат, пов’язаних зі зміною курсу однієї іноземної валюти по відношенню до іншої при проведенні зовнішньоекономічних, кредитних та інших валютних операцій.

Валютні ризики поділяються на операційний, трансляційний та економічний ризики.

Операційний валютний ризик можна визначити як можливість виникнення збитків або недоотримання прибутку в результаті зміни обмінного курсу і впливу його на очікувані доходи від продажу продукції.

Трансляційний валютний ризик (його називають також балансовим) виникає при наявності в головної компанії дочірніх компаній або філій за кордоном. Його джерелом є можлива невідповідність між активами і пасивами компанії, розрахованими у валютах різних країн. Зниження обмінного курсу країни місцезнаходження філії (або дочірньої компанії) по відношенню до валюти країни місцезнаходження материнської компанії викликає удаване зменшення його (або її) прибутку.

Економічний валютний ризик визначається як імовірність несприятливого впливу змін обмінного курсу на економічне становище компанії. Він виникає, наприклад, у результаті зміни обсягу товарообігу в країні або цін на засоби виробництва або на готову продукцію, а також внаслідок зміни конкурентоспроможності компанії в порівнянні з іншими виробниками аналогічних товарів.

Ризики ліквідності – це ризики, пов’язані з можливістю втрат при реалізації цінних паперів або інших товарів через зміну оцінки їхньої якості і споживчої вартості.

Ризик зниження прибутковості містить такі різновиди: кредитні ризики і процентні ризики.

Кредитні ризики пов’язані з можливим неповерненням суми кредиту і відсотків по ньому. Фінансові кошти можуть бути отримані у вигляді кредиту або кредитної лінії. Як правило, умовою видачі кредиту є його цільове призначення, тобто він може бути використаний тільки на потреби конкретного інвестиційного проєкту. Інвестиційний проєкт має техніко-економічне обґрунтування, в якому передбачені терміни освоєння кредиту і очікуваний прибуток.

Ризики прямих фінансових втрат містять такі різновиди: біржовий ризик, селективний ризик, ризик банкрутства, а також кредитний ризик.

Біржові ризики являють собою небезпеку втрат від біржових угод. До цих ризиків відносяться: ризик несплати по комерційних справах, ризик несплати комісійної винагороди брокерської компанії тощо.

Селективні ризики – це ризики неправильного вибору способу вкладення капіталу, виду цінних паперів для інвестування порівняно з іншими видами цінних паперів при формуванні інвестиційного портфеля.

Ризик банкрутства являє собою небезпеку в результаті неправильного вибору способу вкладення капіталу, повної втрати підприємцем власного капіталу і нездатності його розраховуватися за взятими на себе зобов'язаннями. У результаті підприємець стає банкрутом.

Кредитний ризик – компанія, яка видала кредит або має депозит у банку під «плаваючі» відсотки, зазнає збитків у випадку зниження процентних ставок. Компанія, що отримала кредит по «плаваючою» ставкою, навпаки, зазнає збитків у випадку підвищення процентних ставок.

Інвестиційні ризики пов'язані з можливістю недоотримання або втрати прибутку в ході реалізації інвестиційних проєктів. Об'єктом ризику в даному випадку виступають майнові інтереси особи, яка здійснює вкладення своїх коштів, тобто інвестора.

Суть політичних ризиків полягає в можливості недоотримання доходу або втрати власності іноземного підприємця або інвестора внаслідок зміни соціально-політичної ситуації в країні. Вони можуть проявитися у вигляді таких подій:

- введення обмежень до валютного законодавства, що перешкоджають виконанню міжнародних контрактів або репатріації валютної виручки;

- зміна нормативно-правової основи, що ускладнює ведення підприємницької діяльності;

- націоналізація або експропріація підприємств, створених за участю іноземних інвесторів;

- внесення змін до арбітражного права;

- військові дії, громадянські заворушення, масові заворушення, що спричинили за собою заподіяння шкоди майновим інтересам підприємців.

Приклади прояву ризику:

- конфіскація майна або втрата права власності при викупі;

- непередбачені зміни законодавства, що погіршує фінансові показники проєкту (наприклад, збільшення податків);

- зміна персоналу в органах державного управління.

Ризик ненадійності учасників проєкту передбачається в можливості непередбаченого припинення реалізації проєкту, обумовленого, зокрема:

- нецільовим витрачанням коштів, призначених для інвестування в даний проєкт або для створення фінансових резервів;

- фінансовою нестійкістю компанії, що реалізує проєкт (незабезпеченість оборотними засобами, відсутність активів, що забезпечують повернення позикових коштів);

- недобросовісністю, неплатоспроможністю, юридичної недієздатністю інших учасників проєкту (наприклад, будівельних організацій, постачальників, споживачів).

Ризик неотримання доходів обумовлений технічними, технологічними і організаційними рішеннями проєкту, а також випадковими коливаннями обсягів виробництва і цін на продукцію і ресурси. Рекомендована величина конкретних значень поправок на цей вид ризику задається за допомогою табл. 1.3.

Таблиця 1.3 – Поправки на ризики неотримання доходів

Величина ризику	Ціль проєкта	Поправка на ризик, %
Низький	Технічна модернізація виробництва	3–5
Середній	Зростання обсягів продаж продукції	8–10
Високий	Впровадження на ринок нового продукту	13–15
Дуже високий	Інвестиції в інновації	18–20

Наявність ризику і пов’язаних з ним фінансових, моральних та інших втрат створює необхідність у певному механізмі, який дозволив би найбільш ефективним способом визначити і знизити ризик інвестиційних рішень.

Такий механізм зниження ризику являє собою специфічну сферу діяльності, що містить використання сукупності методів і заходів, що дозволяють:

- спрогнозувати появу ризикових подій;

- спланувати заходи щодо оптимізації ризику;

- створити організаційну структуру, здатну реалізувати заходи, спрямовані на зниження ризику.

Очевидно, що реалізація таких заходів потребує глибоких знань в області економічного аналізу, прогнозування, організації праці та виробництва, методів оптимізації рішень, страхової справи, психології тощо.

Серед основних принципів механізму зниження ризику можна виділити такі:

- сумірність. Реалізація цього принципу означає, що перш ніж прийняти рішення в умовах ризику, необхідно визначити максимально можливий розмір втрат у випадку настання ризикової події і потім зіставити його з обсягом вкладених інвестиційних коштів. Іншими словами, «ризикувати» можна на суму, що не перевищує власні кошти;

- відповідальність, тобто необхідність оцінювати наслідки ризикових подій і приймати рішення про передачу ризику на відповідальність іншій особі (випадок страхування ризику) або про відмову від ризику відповідальності, або про покриття можливих втрат власними коштами;

- доцільність. Перш ніж приймати управлінське рішення, що містить ризик, необхідно порівняти очікуваний результат (віддачу) з можливими втратами в разі ризикових подій.

Для того щоб знизити ризик інвестиційного проєкту, застосовують:

- диверсифікацію, під якою розуміється розподіл загальної інвестиційної суми між декількома об’єктами інвестування (інвестиційними

проєктами). Зі збільшенням числа проєктів зменшується загальний розмір ризику;

- скорочення планового періоду прийняття рішень;

- компенсацію ризику за допомогою так званих ризикових премій, які є різного роду надбавками (до ціни, рівня процентної ставки, тарифу, норми дисконту тощо), які виступають у вигляді «плати за ризик»;

- страхування – угоду, згідно з якою страховик за певну винагороду (страхову премію) приймає на себе зобов'язання відшкодувати страхувальникові збитки або їх частину (страхову суму), що виникли внаслідок передбачених у страховому договорі небезпек і (або) випадковостей (страховий випадок), яким піддаються страхувальник або застраховане їм майно. Сутність страхування полягає в передачі ризику (відповідальності за результати негативних наслідків) за певну винагороду іншій особі, тобто в розподілі збитку між учасниками страхування;

- резервування коштів, тобто створення відокремлених фондів відшкодування збитків. Такий спосіб зниження ризику використовується у випадку, коли витрати на резервування коштів менше, ніж вартість страхових внесків при страхуванні;

- лімітування – встановлення системи обмежень, що сприяє зменшенню ступеню ризику, тобто встановлення граничного рівня за ключовими показниками.

За ступенем припустимості ризик буває:

- таким, що можна їм знехтувати;

- прийнятним;

- гранично допустимим;

- надмірним.

Ризик, яким можна знехтувати, характеризується низьким рівнем, який знаходиться в межах допустимих відхилень природного рівня.

Прийнятний ризик – це допустимий рівень ризику, виправданий з точки зору економічних, соціальних і екологічних факторів.

Гранично допустимий ризик характеризується максимальним рівнем ризику, який не повинен збільшуватися, незалежно від очікуваного прибутку.

Надмірний ризик – ризик з високим рівнем, який у переважній більшості випадків призводить до негативних наслідків.

На практиці досягти ризик з нульовим рівнем неможливо. У сучасних умовах ризик, яким можна знехтувати, також не може бути забезпечений через відсутність технічних та економічних передумов для цього.

Наскільки правильно і своєчасно ідентифіковані ризики та проведено їх аналіз, залежить ефективність вжитих заходів, що визначають не тільки отримання прибутку, а й характер зміни всіх показників.

Щодо ризиків в інформаційних системах та ІТ-індустрії – це також вид діяльності, що виконується в інтересах керівництва компанії. Такі дії дають змогу збирати свідоцтва аудиту, оцінювати ступінь їхньої відповідності тим критеріям, які було розроблено під час незалежного оцінювання рівня ІТ-ризиків. Також, це дає можливість скласти рекомендації, пов’язані з їх мінімізацією.

Перелік тут досить широкий. Сюди варто віднести ризик внутрішнього контролю, інформаційної безпеки, операційний бізнес-ризик, персоналу та ІТ проєкту.

Автоматизація діяльності компанії або навіть окремого процесу – це ефективний інструмент, що дає змогу виконувати управління ризиками в ІТ-проєктах. Але, як показує практика, очікування багатьох керівників не виправдовуються.

Основна причина, чому не вдається досягти результатів якісного та ефективного планування, полягає в тому, що успішна реалізація проєктної діяльності слідує лише після грамотного та чіткого планування. Початковий рівень кожного проєкту має показати, наскільки складним має бути поставлене завдання та його реалізація.

Другий важливий фактор – це компетентність і професіоналізм співробітників. Навіть якщо в якійсь сфері співробітник не має високої кваліфікації, він повинен вміти швидко навчатися.

Ризики ІТ-проєктів у сфері виконання – це категорія, яка пов’язана з безпосереднім виконанням проєкту. Такі ризики ІТ-проєктів можуть бути найрізноманітніші, але в будь-якому випадку вони являють собою загальний результат діяльності замовника і виконавця. Також є ще одна класифікація ризиків ІТ-проєкту – це всі питання, які стосуються інформаційної безпеки. Саме тому для управління та ведення всіма категоріями ризиків компанія обирає тільки тих учасників, яким вона дійсно довіряє.

Для кожного проєкту може бути свій перелік ризиків, і зазвичай він містить від 10 до 20 різних факторів. Класифікація зазвичай має п’ять основних ризиків практично для всіх проєктів. Це внутрішні недоліки планування, зміни вимог, постійні зміни в кадрах, невисока продуктивність і порушення специфікації.

Перший варіант можна віднести до того, що виникають недоліки самого процесу планування коштів і часу. Такі помилки зазвичай ґрунтуються на вимогах замовника, які не завжди відповідають реальним витратам часу. Зазвичай перевитрата становить до 80 %.

Зміна вимог дуже часто є тією категорією, коли в процесі реалізації проєкту з’являються нові вимоги замовника. І навіть якщо виконавець відкладає ті проєкти, які вже були виконані, він витрачає час на виконання нових. Для управління ризиками компанія-розробник продумує все, щоб розмір таких змін становив не більше одного відсотка.

Ще один варіант ризиків – це плинність кадрів. Такий ризик передбачає, що щойно найнятому співробітнику доведеться витратити певний період часу на те, щоб досягти необхідної продуктивності. І чим складніший рівень проєкту, то довше доведеться новому співробітнику навчатися.

Порушення специфікацій, являє собою деструктивну складову для проєкту. Це дуже серйозна проблема, яка виникає з вини виконавця. Вона може проявити себе в двох випадках: коли виконавець перевантажує продукт різними непотрібними функціями, або намагається видати бажане за дійсне.

Низька продуктивність – це категорія ризиків, для виникнення якої потрібна поява всього лише одного незначного ризику або фактора, що впливає на його появу. У великих компаніях, де для повноцінного процесу беруть участь одразу кілька спеціалістів або цілих відділів, спад продуктивності роботи одного співробітника може компенсуватися збільшенням ентузіазму іншого фахівця. У невеликих організаціях, що мають одного співробітника, який працює в галузі інформаційних технологій, зниження його активності стає дуже помітним і обмежує інтереси керівництва та компанії загалом.

1.3. Особливості виявлення, аналізу та оцінки ризиків

Ідентифікація та аналіз ризиків – основний етап процесу управління ризиком, від якого більшою мірою залежить ефективність прийнятих рішень і, у кінцевому підсумку, чи вдасться компанії в достатній мірі захиститися від можливих ризиків. У зв’язку з цим моніторинг особливостей області ризик-менеджменту і їх облік у практичній діяльності менеджера по ризиках є ключовим елементом для розуміння всієї системи ризик-менеджменту.

Головна мета ідентифікації та аналізу ризиків – це формування в осіб, що приймають рішення, цілісної картини ризиків, що впливають на ефективність діяльності компанії, майнові інтереси власників, зобов’язання, що виникають у процесі взаємовідносин з клієнтами та іншими контрагентами тощо.

У практичній діяльності важливо не тільки знати перелік ризиків, але й розуміти, який вплив можуть надавати ці ризики на діяльність компанії і наскільки серйозними можуть бути наслідки. У результаті проведеного моніторингу ризиків правильно організована система ризик-менеджменту

забезпечить допустимий рівень захисту компанії від ризиків. Ідентифікація та аналіз ризиків передбачає проведення якісного, а потім і кількісного вивчення ризиків, з якими зустрічається компанія.

Головним завданням просування якісного аналізу є виявлення можливих ризиків, а також факторів, що впливають на ступінь ризику і потенційні області впливу.

Фактори, що впливають на рівень ризику, можна поділити на зовнішні і внутрішні. До зовнішніх факторів належать політична і економічна ситуація в країні та за її межами, законодавчо-правова основа підприємницької діяльності, податкова система, конкуренція, стихійні лиха тощо. Внутрішні чинники – це економічна стратегія компанії, ступінь використання ресурсів у виробничо-господарської діяльності, кваліфікація працівників, якість менеджменту тощо.

Аналіз ризиків в інформаційних системах містить оцінку ризиків і методи зниження ризиків або зменшення пов’язаних з ним несприятливих наслідків. На першому етапі робиться виявлення відповідних чинників і оцінка їх значущості. Призначення аналізу ризиків – дати потенційним партнерам необхідні дані для ухвалення рішень про доцільність участі в проєкті і вироблення заходів по захисту від можливих фінансових втрат.

Загроза – сукупність умов і чинників, які можуть стати причиною порушення цілісності, доступності, конфіденційності інформації.

Вразливість – слабкість у системі захисту, який робить можливою реалізацію загрози.

Ризик порушення інформаційної безпеки – можливість реалізації загрози.

Аналіз ризиків – процес визначення загроз, вразливостей, можливого збитку, а також контрзаходів.

Оцінка ризиків – ідентифікація ризиків, вибір параметрів для їх опису і отримання оцінок за цими параметрами.

Управління ризиками – процес визначення контрзаходів відповідно до оцінки ризиків.

Клас ризиків – безліч загроз інформаційної безпеки, виділених за певною ознакою.

Ризик ускладнює процес прийняття рішення. Для визначення, оцінки та управління ризиком необхідно відповісти на такі питання:

1. Які види ризиків можливі в даній ситуації?

2. Яка ймовірність втрат від них?

3. Як кількісно можна оцінити можливі втрати?

4. Які очікуються втрати в найгіршому випадку?

5. Які альтернативи можна передбачити?

6. Як втрати можуть бути знижені або усунуті?

7. Можлива чи ні при виборі іншої альтернативи поява додаткових або інших ризиків?

Для ефективної реалізації аналізу ризиків компанії важливо цей процес розділити і здійснити за допомогою трьох взаємопов'язаних етапів:

- підготовчий етап – тобто визначаються цілі та завдання дослідження, а також коло фахівців, які будуть здійснювати аналіз, розподіляються роботи і обов'язки між ними, а також здійснюється програмне та технічне забезпечення, обумовлюються терміни проведення аналізу, узгоджуються взаємини між різними підрозділами, які беруть участь у даному процесі тощо;

- аналітичний етап – відповідно до цілей дослідження здійснюється аналіз, тобто фахівець-аналітик повинен вибрати з усього обсягу існуючої інформації саму конкретну і важливу, здійснити класифікацію факторів і розрахунок різних показників. На цьому етапі застосовуються методи і прийоми динамічного, структурного, структурно-динамічного, коефіцієнтного і факторного аналізу;

- заключний етап – результати аналізу оформляються, готуються прогнози та рекомендації щодо оптимізації рівня ризику.

Попереднім кроком стадії кількісної оцінки ризиків є отримання інформації про них, яка повинна містити дані, необхідні для оцінки ступеня передбачуваності ризику: частота (ймовірність) виникнення і розмір збитків. Правильність прийнятих рішень залежить від того, чи вдасться зібрати необхідні якісні дані в потрібному обсязі. Тому визначення ступеня довіри до різних джерел інформації є важливим аспектом цього кроку.

Аналіз ризиків можна розділити на два види, що взаємно доповнюють один одного: якісний і кількісний.

Якісний аналіз. Мета – ідентифікувати чинники, сфери та види ризиків, тобто виявити ризики, властиві конкретній сфері діяльності. Головне завдання даного процесу – не пропустити важливі обставини та докладно описати усі істотні ризики.

Якісний аналіз ризику передбачає:

- виявлення джерел та причин ризику, етапів і робіт, під час яких виникає ризик, тобто встановлення потенційних зон ризику;

- ідентифікація (встановлення) всіх можливих ризиків;

- виявлення практичних вигод та можливих негативних наслідків, які можуть настати при реалізації рішення, що містить ризик.

Результати якісного аналізу є важливою вихідною інформацією для здійснення кількісного аналізу.

Кількісний аналіз. Мета – оцінити ризик. Головне завдання даного процесу – кількісно визначити рівні окремих ризиків та ризику всієї діяльності чи проєкту загалом. У ході цього аналізу визначаються такі характеристики, як ймовірність настання несприятливих подій та розмір можливої шкоди, визначається також допустимий у цій конкретній обстановці рівень ризику. Кількісна оцінка ризиків визначається через:

- ймовірність того, що отриманий результат виявиться меншим за необхідне значення (намічене, плановане, прогнозоване);

- добуток очікуваної шкоди на ймовірність того, що ця шкода відбудеться.

По суті, кількісний аналіз – це оцінка ризиків, він являє собою визначення розмірів окремих ризиків математичними і статистичними методами. Це можуть бути такі методи кількісного аналізу:

- статистичний;
- метод оцінки ймовірності очікуваного збитку;
- метод мінімізації втрат;
- метод використання дерева рішень;
- математичний метод;
- оцінка ризику на основі аналізу фінансових показників діяльності підприємства.

Основний крок стадії кількісної оцінки ризиків – обробка зібраних даних. Вона повинна обслуговувати цілі подальшого процесу прийняття рішень з управління ризиком. Основні критерії кількісної оцінки ризику:

- рішення, прийняте в ситуації ризику, має оцінюватися з точки зору ймовірності досягнення передбачуваного результату і можливого відхилення від нього. Кращим вважається рішення, ризик здійснення якого менший у порівнянні з іншими варіантами:
- ризикове рішення також має оцінюватися з точки зору витрат, необхідних на його здійснення. Кращим буде рішення, яке вимагає менших витрат на своє здійснення.
- ризикове рішення має оцінюватися з точки зору тривалості часу, необхідного на реалізацію рішення. Кращим буде рішення, яке за даних умов вимагає меншого часу на його здійснення.

Для виявлення факторів ризику і ступеня їх впливу можуть бути використані різні методи статистичної обробки даних, у тому числі: кореляційний дисперсійний аналіз, аналіз часових рядів, факторний аналіз і інші методи багатовимірної класифікації, а також математичне моделювання, включаючи імітаційне.

При необхідності статистичний аналіз може бути використаний для підтвердження деяких висновків попередньої стадії, коли якісного аналізу для цього недостатньо.

Пріоритетну роль у процесі управління ризиками відіграє якість отриманої інформації, своєчасне надання якої особі, що приймає рішення, є важливою умовою ефективного ризик-менеджменту. Основні вимоги до якості інформації:

- узгодженість її змісту з організаційною структурою системи ризик-менеджменту;

- оперативність забезпечення інформацією багаторівневої структури системи ризик-менеджменту;

- відповідність інформаційних масивів змісту і особливостям прийнятих управлінських рішень;

- диференційований метод отримання інформації.

З перерахованих вимог випливає, що інформація, необхідна для управління ризиком, різноманітна, її склад і обсяг можуть істотно варіюватись, а доступ до неї повинен бути досить оперативним. Умова – використання інформаційних технологій для отримання і обробки масивів даних. Система, яка використовується, є елементом загальної інформаційної системи організації та будується на основі локальних мереж, дистанційного обміну даними з віддаленими офісами і робочими місцями та баз даних. Підсистема збору та обробки інформації з управління ризиками ґрунтується на принципах загальної інформаційної системи з урахуванням таких факторів:

- специфіки архітектури використовуваної інформаційної технології і її орієнтації на дані, застосунки або клієнтів;

- характеру інформаційного обміну та узгодження форматів баз даних;

- ієрархічної побудови та відповідної обмеженості доступу до інформації з управління ризиком;

- цілей і методів обробки даних.

Система збору та обробки інформації, необхідної для управління ризиком, має такі переваги:

- здатність до швидкої зміни класифікації ризиків і вибудовування пріоритетів у системі завдань ризик-менеджменту;

- зіставлення аналізу ризику з адміністративною, маркетинговою, економічною і фінансовою інформацією і його своєчасне корегування;

- можливість підвищення гнучкості процесу управління ризиком і врахування інтересів різних категорій персоналу на основі оцінки та аналізу ризику, притаманного різним рівням ієрархії, і з застосуванням різних методик;

- інтегрованість різних аспектів системи управління ризиком: кількісна та якісна оцінки; обраний спосіб управління ризиком і його ефективність;

- спрощення процесу аудиту і контролю реалізації програми управління ризиком.

Таким чином, використання інформаційних технологій у порівнянні з інформацією, представленою на паперовому носії, робить систему ризик-менеджменту адаптивної і гнучкою.

При цьому, застосуванню інформаційних технологій властиві й деякі недоліки, серед яких слід відзначити такі:

- уразливість системи управління ризиком (наприклад, неможливість запобігання негативним наслідкам при аварії локальної мережі);

- збільшення вартості збору і обробки інформації за рахунок здійснення додаткових витрат на програмне забезпечення, обладнання, підвищення кваліфікації персоналу;

- необхідність формалізації процесів прийняття рішень в умовах використання інформаційних технологій у ризик-менеджменті вимагає наявності досить формалізованих систем, що ускладнює прийняття і реалізацію ефективних управлінських рішень в умовах форс-мажорних обставин.

Статистичні методи оцінки ризиків.

Статистичні методи ґрунтуються на дослідженні статистики втрат, що мали місце в аналогічних видах діяльності, визначенні частоти появи певних рівнів втрат і прогнозуванні ймовірності втрат. Статистичні методи розглядаються в зв'язку з поняттям зон і меж ризику. Точки, що визначають рівень втрат і ймовірність появи цих втрат, описуються за допомогою статистичного аналізу досить великого масиву даних. Основа цієї групи методів – розрахунок середньоквадратичного відхилення, коефіцієнта варіації і дисперсії.

Багато з основних ідей статистичної теорії рішень були розроблені Нейманом і Пірсоном у 1933 році. Систематична теорія для ситуації, коли немає апріорного розподілу, розвивалася Вальдом, основні ідеї теорії викладені в книзі Вальда, виданій у 1950 році. У цьому виданні викладені відомі статистичні завдання на мові теорії прийняття рішень. У 1951 році Гіршік і Севідж продовжили дослідження Вальда в області теорії прийняття рішень. Фон Нейман і Моргенштерн розвинули аксіоматичний підхід до суб'єктивних корисностям у зв'язку з їх роботами по теорії ігор.

У кінці 1950-х і початку 1960-х років теоретичний інтерес перемістився від ситуації без апріорних розподілів до байєсівської теорії рішення. Авторитетний виклад даного підходу здійснено Ховардом Райффа і Робертом Шлайфером (1961 р.).

Подальший розвиток даної групи методів – розробка широко використовуваного в даний час методу «дерева рішень». Даний метод застосовується для оцінки ризиків тих рішень, які мають доступну для огляду кількість варіантів розвитку. При цьому, для побудови дерева аналітик повинен володіти необхідною і достовірною інформацією з урахуванням ймовірності і часу настання різних сценаріїв проєкту. Послідовність збору даних для побудови «дерева рішень» можна представити таким чином: визначення складу і тривалості фаз життєвого циклу проєкту, ключових подій; формулювання всіх можливих рішень; визначення ймовірності

прийняття кожного рішення і вартості кожного етапу здійснення проєкту. На підставі отриманих даних будується «дерево рішень», до складу якого включаються вузли роботи по реалізації проєкту. Для формулювання різних сценаріїв розвитку проєкту необхідно мати достовірну інформацію з урахуванням ймовірності і часу їх настання.

Імовірнісний підхід до вимірювання ризику запропонували Г. Б. Клейнер, В. Л. Тамбовцев, Р. М. Качалова. Автори пропонують вимірювати ризик на основі теорії вимірювань, яка містить системний аналіз, побудову спеціальної моделі, вибір шкали вимірювання ризику і способу визначення значень показника вимірювання ризику. Також пропонується формувати узагальнену кількісну оцінку ризику проєкту з урахуванням всіх його учасників, для кожного з яких спочатку оцінюються ризики окремих випадків і альтернатив.

Використання статистичних методів у сучасних умовах має ряд обмежень. Дана група методів не враховує взаємозв’язок між змінними проєкту, у силу цього дані методи можуть бути використані для обмеженого кола проєктів. Для ефективного використання цієї групи методів необхідно побудувати розподіл ймовірностей. Розподіл ймовірностей можна визначити або за статистичними даними за минулі періоди, що в умовах нестабільного середовища неможливо, або шляхом імітації поведінки основної випадкової змінної, але необхідним тут елементом є багаторазове повторення процесу, але цей метод теж не дає точних результатів.

Наступна група – **розрахунково-аналітичні методи оцінки ризиків**.

Ця група базується на математичних підходах. При цьому слід зазначити, що прикладні математичні методи розрахунків ризиків виробничо-господарських, фінансових, комерційних недостатньо добре розроблені.

Широке поширення в даній групі отримало імітаційне моделювання. Імітація являє собою методику для проведення експериментів з математичним забезпеченням моделі поведінки системи в певний момент

часу. Виділяють такі види імітації: імовірнісна; залежна і незалежна від тимчасового чинника; явна; ділові ігри; імітація великих систем. Модифіковану модель імітаційного моделювання являє метод Монте-Карло. Процедура імітації Монте-Карло базується на таких етапах:

1) формулювання функціональних залежностей між результуючими і екзогенними змінними моделі;

2) отримання вибірки екзогенних змінних;

3) розрахунок значень результуючих змінних для кожної вибірки за допомогою певних на першому кроці функцій;

4) багаторазове повторення 2-го і 3-го кроків.

Основна відмінність методу Монте-Карло від інших аналітичних методів полягає в охопленні простору рішень. Якщо аналітичні методи охоплюють весь простір, то даний метод тільки частину. Метод дозволяє досить повно врахувати всю невизначеність, а також доступну інформацію. Основний недолік даної моделі полягає в залежності точності результатів від якості створеної прогнозної моделі. Також слід зазначити, що використання даного методу ефективно тільки для великих проєктів, оскільки його реалізація пов’язана з великими витратами.

У 1950-х рр. починає розвиватися досить новий напрямок у статистиці – теорія планування експерименту, засновником даного напрямку прийнято вважати англійського статистика Р. Фішера. Серед всесвітньо відомих вчених, які працювали в даному напрямку, слід зазначити О. М. Колмогорова, Ю. В. Лінніка, Є. В. Маркова, Г. І. Марчука.

Математичні методи планування експерименту дозволяють аналітику вибрати оптимальне число сценаріїв і в рамках кожного з них – оптимальні значення факторів, що дозволяє визначити коефіцієнти багатофакторної регресії при істотно меншому обсязі обчислень. Але розглянутий підхід не набув широкого поширення в силу недостатньої розробленості методики оцінки ризиків.

Подальше вдосконалення та практичне застосування даної групи методів привело до розробки аналізу чутливості (або методу варіації параметрів проєкту) і методу сценаріїв. Метод варіації параметрів проєкту дозволяє досліджувати взаємозв'язки, які існують між пояснюючими і результуючими змінними, шляхом зміни перших. Метод сценаріїв передбачає розробку оптимістичного, песимістичного і найбільш ймовірного варіанту реалізації проєкту з розрахунком всіх результуючих показників по проєкту. Використання аналізу чутливості може бути неефективним у силу того факту, що інформація, яка надається аналітику в результаті проведення аналізу чутливості вкрай недостатня для прийняття обґрунтованого рішення за проєктом. Другий метод також має ряд недоліків, а саме – для використання даного методу необхідно знати найбільш вірогідний сценарій розвитку (песимістичний і оптимістичний), проте, якщо середовище реалізації проєкту дуже рухливе, наприклад, в умовах кризи, то прогнозувати сценарії практично неможливо.

Методи експертних оцінок ризиків. У даний час все частіше застосовуються різні методи експертних оцінок. Вони незамінні при вирішенні складних завдань оцінювання і вибору технічних об'єктів, у тому числі спеціального призначення, при аналізі і прогнозуванні ситуацій з великим числом значущих чинників, коли необхідно залучення знань, інтуїції і досвіду багатьох висококваліфікованих фахівців-експертів.

Проведення експертних досліджень засновано на використанні сучасних методів прикладної математичної статистики, перш за все – статистики об'єктів нечислової природи, і сучасної комп'ютерної техніки.

Метод експертної оцінки являє собою комплекс логічних і математико-статистичних методів і процедур, пов'язаних з діяльністю експерта по переробці необхідної для аналізу і прийняття рішень інформації. Даний метод оцінки ризиків проєктів заснований на використанні здатності експерта знаходити найбільш ефективне рішення на основі досвіду, знань та інтуїції. Використання даного методу є найбільш ефективним у силу тієї

обставини, що тільки експерти мають інформацію для оцінки проєктних ризиків у силу наявності гіпотетичних уявлень про шляхи вирішення локальних і глобальних проблем, апріорних оцінок значущості різних рішень, інтуїтивних здогадок про альтернативи розвитку. Основний недолік даного методу полягає в суб'єктивності оцінки, що може відбитися на якості оцінки, але при використанні науково-обґрунтованої організації проведення всіх етапів експертизи забезпечується ефективність роботи на кожному з етапів. Застосування кількісних методів як при організації експертизи, так і при оцінці суджень експертів і формальній груповій обробці результатів також дозволяє подолати цей недолік.

У літературі зустрічається точка зору, що найбільш пристосованим для аналізу ризиків у ситуації перехідного періоду є системний підхід, тому що він орієнтований на будь-які види залежностей і розподілів, дозволяє використовувати різні показники ефективності та передбачає безпосередній облік ризиків і обчислення сукупного ризику. При цьому необхідно доповнити даний аналіз ситуаційним підходом.

Кожен керівник повинен вибирати для аналізу свого підприємства той метод, ту техніку дослідження ризиків, які найбільше відповідають можливостям даного проєкту і зовнішнім вимогам, враховуючи при цьому як їх переваги, так і недоліки.

Для оцінки ризиків важливим є використання карти ризиків (рис. 1.3), де зіставляються потенційний збиток ризику і ймовірність його настання. Рівні ризику можуть бути незначні (зелена зона, жодні дії не здійснюються), середні (жовта зона, необхідні заходи з контролю ризику), високі і критичні (червона зона, необхідні негайні заходи щодо зниження ризику).

Рисунок 1.3 – Карта ризиків

Після оцінки рівня ризиків необхідно здійснити пріоритизацію ризиків.

Пріоритизація ризиків – це процес вивчення і розгляду всіх виявлених ризиків з метою ранжирування їх, з точки зору ймовірності їх виникнення, негативного впливу і шкоди, тобто виділення певної кількості ризиків, на які маємо сфокусувати увагу і направляти дії з боку керівництва організації. Для здійснення цього процесу допоміжним інструментом є реєстр ризиків, що представляє таблицю, яка включає інформацію про ризики господарюючого суб'єкта.

Приклад фрагменту таблиці реєстру ризиків (тільки один рядок) організації наведено в табл. 1.4.

Таблиця 1.4 – Приклад фрагменту таблиці реєстру ризиків

Опис ризиків	Наслідок реалізації ризиків	Збитки від ризику	Ймовір-ність ризику	Оцінка ризику	Заходи щодо зниження ризику	Відповідальність та терміни
Фінансові ризики - фінансові втрати через банкрутство банків, в яких розміщено існуючі депозити компанії	-розрив ліквід-ності -судові розгляди з банками	висо-кі	се-ред-ня	висо-кий	-диверси-фікація фінансових інструмент-тів - збіль-шення оборотнос-ті коштів	Керівник фінансо-вого відділу

Перші два стовпчики таблиці заповнюються в результаті отриманих даних на етапі ідентифікації або виявлення ризиків, третій, четвертий і п’ятий заповнюються в результаті отриманої інформації з етапу оцінки ризиків, а останні стовпці визначаються на етапі управлінського впливу за всіма ризиками.

При визначенні, оцінці та управлінні ризиком в ІТ-технологіях треба розуміти, що це формує основу для всієї діяльності з інформаційної безпеки та підтримує своєчасне та належне реагування на вимоги ринкових регуляторів. При цьому необхідно виявляти та оперативно реагувати на загрози, вразливості та можливі втрати, розуміти потенційні збитки і наслідки компрометації властивостей інформаційних активів, що служить базою для створення стратегії мінімізації ризиків і допомагає визначати пріоритети під час впровадження захисних заходів.

Ключові завдання:

- виявлення існуючих ризиків;

- оцінка та документування потенційних ризиків і можливих наслідків;

- підготовка фахівців з управління інформаційними ризиками.

Основні підходи до управління ризиками в сфері інформаційних технологій базуються на таких стандартах і рекомендаціях [14]:

- стандарт управління та аудиту інформаційних технологій COBIT 2019 (Control Objectives for Information and related Technology) – методологія управління корпоративною інформацією і технологіями, що охоплює всю організацію;

- рекомендації щодо управління ризиками в інформаційних технологіях NIST 800-30 «Guide for Conducting Risk Assessments» (Посібник з проведення оцінки ризиків) сфокусований на інформаційних технологіях, інформаційній безпеці та операційних ризиках. Він описує підхід до процесів підготовки та проведення оцінки ризиків, обговорення результатів оцінки, а також подальшої підтримки процесу оцінки;

- стандарт управління ризиками ISO 31000:2018 «Risk management – Guidelines» (Менеджмент ризиків. Принципи й керівні вказівки);

- стандарт управління інформаційною безпекою ISO 27005:2022 «Information security, cybersecurity and privacy protection – Guidance on managing information security risks» (Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки);

- стандарт управління ризиками AS/NZS 4360:2004 «Risk management» – стандарт управління ризиками, який описує процес ідентифікації, оцінки та управління ризиками в організації.

Методології, які використовуються в IT-індустрії для оцінки ризиків:

- методологія оцінки ризиків Національного Інституту Стандартів та Технологій США (National Institute of Standards and Technology – NIST);

- FAIR (Factor Analysis of Information Risk) – методологія аналізу факторів ризиків інформаційних технологій від Risk Management Insight;

- методологія пропорційного аналізу ризиків (MESARI) від Crédit Agricole;

- OCTAVE (Operationally critical threats, assets and vulnerability evaluation) – метод оцінки операційно критичних загроз, активів та уразливостей від CERT (Computer Emergency Response Team);

- методологія аналізу інформаційних ризиків Міжнародного Форуму з інформаційної безпеки (Information Risk Analysis Methodology – IRAM).

Методологія оцінки ризиків від Національного Інституту Стандартів та Технологій NIST полягає у виконанні таких кроків:

1. Характеристика системи. На цьому кроці визначаються цілі створення інформаційної системи, її межі, інформаційні ресурси, вимоги до області інформаційної безпеки і компонентів управління інформаційної системи. Опис рекомендується вести відповідно переліку:

- апаратні засоби інформаційної системи, їх конфігурація;

- використовуване програмне забезпечення;

- інтерфейси системи – внутрішні і зовнішні зв’язки з позицій інформаційних технологій;

- типи даних та інформації;

- персонал, який працює в даній інформаційній системі та його обов’язки;

- основні цілі даної інформаційної системи;

- критичні типи даних та інформаційні процеси;

- функціональні вимоги до інформаційної системи;

- категорії користувачів системи та обслуговуючого персоналу;

- формальні вимоги в області інформаційної безпеки, стосовно до даної інформаційної системи (законодавство, відомства тощо);

- архітектура підсистеми інформаційної безпеки;

- топологія локальної мережі;

- програмно-технічні засоби забезпечення інформаційної безпеки;

- вхідні та вихідні потоки даних;

- система управління в даній інформаційній системі (посадові інструкції, система планування в сфері забезпечення інформаційної безпеки);

- існуюча система управління в області інформаційної безпеки (резервне копіювання, процедури реагування на нестандартні ситуації, інструкції з інформаційної безпеки, контроль підтримання режиму інформаційної безпеки тощо);

- організація фізичної безпеки;

- управління і контроль зовнішнього за ставленням до інформаційної системи середовища (кліматичні параметри, електроживлення, захист від затоплень, агресивні середовища тощо).

Для отримання такої інформації рекомендується використовувати:

- різноманітні запитання (чек-листи), які можуть бути адресовані різним групам управлінського й обслуговуючого персоналу;

- інтерв’ю аналітиків, які проводять неформальні бесіди з персоналом і потім готовлять формалізований опис;

- аналіз документів підприємства;

- спеціалізований інструментарій (програмне забезпечення) – сканери, що дають можливість скласти схему інформаційної системи, програми для структурованого опису інформаційних систем, що дозволяють створити необхідні звітні форми.

2. Ідентифікація загроз. На даному етапі здійснюється побудова моделі загрози, де описується, хто може виступати в якості загрози, можливості та мотиви загрози, сценарій реалізації загрози. Результатом є перелік актуальних загроз для системи.

3. Ідентифікація вразливостей – у результаті складається список потенційних вразливостей інформаційної системи. Для існуючої інформаційної системи при складанні списків звертаються до низки джерел: мережеві сканери вразливостей, каталоги вразливостей різних організацій тощо.

4. Аналіз заходів захисту. При оцінці рівня вразливості беруться до уваги існуючі процедури та методи забезпечення режиму інформаційної безпеки, дані внутрішнього аудиту та результати аналізу наявних місць інцидентів.

5. Визначення ймовірності реалізації загроз – вибирають шкали для оцінки параметрів ризику. Найбільшою формою є якісна шкала з кількома градаціями. Оцінка виробляється експертно.

6. Аналіз збитків (втрат). За шкалою оцінюють тяжкість наслідків і ймовірність реалізації загроз.

7. Визначення ризиків. Визначається рівень ризику, поєднуючи ймовірність реалізації загрози та тяжкості її реалізації. Рівень ризику залежить від рівнів загроз, вразливостей і цін можливих наслідків. Ризики повинні бути ранжирувані за ступенем їх небезпеки.

8. Рекомендації щодо заходів безпеки – вироблення рекомендацій щодо управління ризиками: рекомендації по зменшенню ризиків до допустимого рівня необхідні, вони повинні бути комплексними і враховувати можливі заходи різних рівнів.

9. Звітна документація. Результати оцінки ризиків формуються у вигляді звітних документів.

Відповідно до методики FAIR, основним принципом є кількісний аналіз ризиків. Аналізуються фактори, що мають вплив на компоненти, що є складовими ризику. Методологія оцінки ризиків FAIR полягає у виконанні таких кроків [2]:

1. Ідентифікація об’єктів оцінки. Проводиться ідентифікація активів, загрози (з визначенням її групи та типу), оцінюється ефект загрози, що може бути застосований до інформаційної системи підприємства. Дані фіксуються в таблицю.

2. Оцінка частоти виникнення збитків. Частота появи загрози вимірюється з використанням факторів: «мінімальне значення», «найбільш ймовірне значення» та «максимальне значення». Для оцінки найгіршого варіанту необхідно виконати такі пункти:

- визначити дію загрози, яка напевно буде результатом найгіршого випадку;

- оцінити величину кожного виду втрат, пов’язаних з дією загрози;

- підсумувати величини всіх видів втрат.

3. Оцінка величини потенційних збитків – розрахунок величини ризику. При розрахунку використовують метод Монте-Карло.

4. Формалізація та уникнення ризиків. Інтерпретація результатів проводиться відповідно до таблиць методики.

Для розуміння використання методики FAIR для оцінки ризику доцільно розглянути приклад сценарію. Припустимо, що посадова особа з відділу кадрів великого банку записала пароль та логін на нотатку та

приклеїла до монітору. Таким чином, це полегшує цій особі вхід до мережних ресурсів та на сервер для запуску програмного забезпечення відділу кадрів.

Алгоритм оцінки ризику з використанням FAIR:

Етап 1: Визначення компонентів сценарію.

- Визначається актив, на який впливає ризик програмного забезпечення та атрибути.

- Визначаються чинники загрози (прибиральниця, інші співробітники відвідувачі відділу співробітники технічної підтримки наймані особи.

Етап 2: Оцінка частоти випадків втрати (LEF).

- Оцінюється можлива частота виникнення загрози TEF (Threat Event Frequency) (табл. 1.5).

Таблиця 1.5 – Частота виникнення загрози TEF

Рівень	*	Опис
Дуже високий (Very High - VH)		> 100 випадків на рік
Високий (High - H)		Від 10 до 100 випадків на рік
Помірний (Moderate - M)		Від 1 до 10 випадків на рік
Низький (Low - L)	*	Від 0.1 до 1 випадку на рік
Дуже низький (Very Low - VL)		< 0.1 випадку на рік (< 1 випадку кожні 10 років)

- Визначається можливість реалізації загрози (знання та досвід) TCap (Threat Capability) (табл. 1.6).

Таблиця 1.6 – Можливість реалізації загрози TCap

Рівень	*	Опис
Дуже високий (VH)		Найвищі 2 % порівняно із загальною множиною загроз
Високий (H)		Топ-16 % порівняно із загальною множиною загроз
Помірний (M)	*	Середній рівень (між нижніми 16 % і найкращими 16 %)
Низький (L)		Нижні 16 % порівняно із загальною множиною загроз
Дуже низький (VL)		Найнижчі 2 % порівняно із загальною множиною загроз

- Визначається рівень захищеності активу (знання та досвід) CS (Control Strength) (табл. 1.7).

Таблиця 1.7 – Рівень захищеності активу CS

Рівень	*	Опис
Дуже високий (VH)		Захищає від усіх, крім верхніх 2 % значення загрози
Високий (H)		Захищає від усіх, крім верхніх 16% значення загрози
Помірний (M)		Захищає від середньої загрози
Низький (L)		Захищає лише від нижніх 16 % значення загрози
Дуже низький (VL)	*	Захищає лише від нижніх 2 % від значення загрози

- Визначається уразливість активу (зусилля для отримання доступу – рівень захищеності активу) Vuln (Vulnerability) і визначається частота виникнення втрат (втрати конфіденційності активу) LEF (Loss Event Frequency). Рейтинг уразливості визначається як клітинка перетину значення TCap з рівнем захищеності CS (рис. 1.4) у матриці уразливості

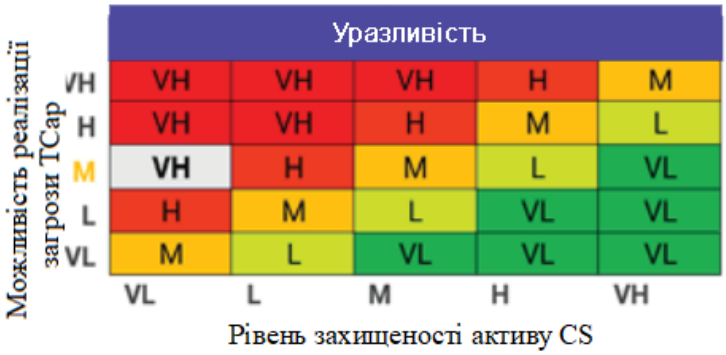


Рисунок 1.4 – Матриця уразливості

У наведеному прикладі рейтинг вразливості Vuln дуже високий (VH).

- Визначення частоти виникнення втрат виконується по відповідній матриці частоти виникнення втрат як клітинка перетину значення TEF зі значенням уразливості (рис. 1.5).

Рисунок 1.5 – Матриця частоти виникнення втрат

Відповідно до отриманої оцінки ймовірність події втрат у сценарії прикладу низька (десь від 0,1 до 1 разів на рік).

Етап 3: Оцінка ймовірної величини втрат PLM (Probable Loss Magnitude).

- аналіз втрат, якщо подія все-таки відбулася (найгірший сценарій). У цьому сценарії виділяються три дії потенційної загрози, які мають значний потенціал втрат – зловживання, розголошення та модифікація. Для цього сценарію обрано «Розголошення» як найгірший варіант.

Оцінка величини втрат у найгіршому випадку для кожної форми втрат (табл. 1.8).

Таблиця 1.8 – Форми втрат

Дія	продуктивність	реагування	заміна	репутація
доступ				
зловживання				
розголошення	High - H	High - H	-	Severe - SV
модифікація				
заборона доступу				

- Обґрунтування оцінок з табл.1.8 вище містить:

а) вплив на продуктивність буде високим (H), оскільки працівники різко реагуватимуть на подію;

б) вартість реагування на подію включатиме розслідування деякий час від юридичного відділу та надання компенсації будь-яким постраждалим (H);

в) вартість заміни спричинить лише зміну пароля відділу кадрів, тому не враховується;

г) вплив на репутацію установи може бути дуже сильним (SV).

Наступним кроком є оцінка найбільш вірогідного розміру збитку внаслідок неправильного використання для кожної форми збитку. Рівні втрат наведено в табл. 1.9.

Таблиця 1.9 – Рівні втрат

Величина	Нижній рівень	Верхній рівень
Сильний (Severe - SV)	10000000 USD	-
Високий (High - H)	1000000 USD	9999999 USD
Значний (Significant – Sg)	100000 USD	999999 USD
Помірний (Moderate - M)	10000 USD	99999 USD
Низький (Low - L)	1000 USD	9999 USD
Дуже низький (Very Low - VL)	0 USD	999 USD

- У прикладі сценарію припускається, що основною мотивацією буде фінансова вигода. Для аналізу, враховуючи тип активу (особиста інформація) і доступні дії щодо загрози, доцільно вибрати «Зловживання» як найбільш імовірну дію – наприклад, крадіжка особистих даних.

Наступним кроком є оцінка найбільш вірогідного розміру збитку внаслідок «Зловживання» для кожної форми збитку (табл. 1.10).

Таблиця 1.10 – Форми втрат

Дія	продуктивність	реагування	заміна	репутація
доступ				
зловживання	Moderate - M	Moderate - M	Very Low -VL	Very Low -VL
розголошення				
модифікація				
заборона доступу				

Так само визначаються за табл. 1.9 рівні втрат внаслідок неправильного використання для кожної форми збитку.

Етап 4: Вимірювання та формалізація ризику.

Ризик визначається на основі частоти втрат LEF і ймовірної величини втрат PLM як клітинка перетину значень LEF та PLM (рис. 1.6). Літера в клітинці позначає: C – Critical (Критичний рівень), H – High (Високий рівень), M – Medium (Середній рівень), L – Low (Низький рівень).

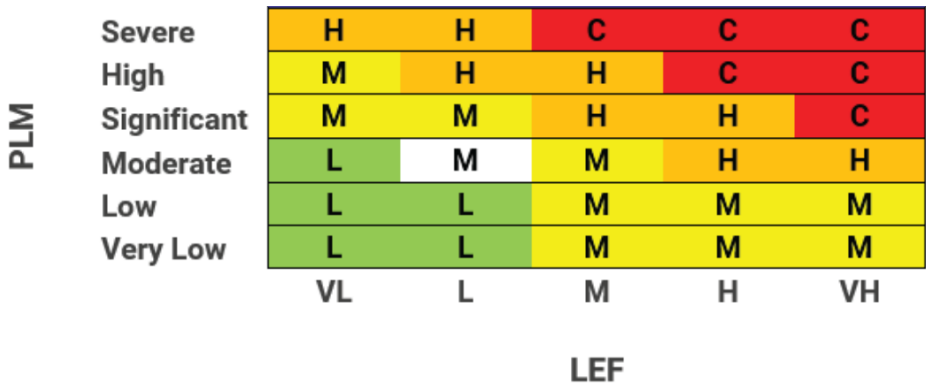


Рисунок 1.6 – Вимірювання рівня ризику

Наступний крок полягає в тому, щоб вирішити, чи сформулювати найбільш вірогідний ризик, чи сформулювати ризик як найгірший випадок.

У даному сценарії, використовуючи наведену на рис. 1.6 матрицю, можна помітити, що найбільш вірогідний ризик є середнім (M) на основі LEF (від 0.1 до 1 разу на рік) і PLM (від 10000 до 100000 доларів США).

Методика оцінки ризиків IT за MESARI складається з трьох основних етапів:

Етап 1. Опис активів або активу та визначення проблемних питань. Виконується аналіз поточного рівня захищеності (існуючі заходи безпеки).

Етап 2. Визначення ризиків та заходів безпеки. Виконується детальний аналіз ризиків (можливі сценарії реалізації ризиків) та покриття ризиків (усунення причин виникнення та перелік можливих заходів безпеки).

Етап 3. Вибір заходів захисту. Виконується вибір адекватних заходів безпеки та прийняття ризиків (ризик усунуто, знижено або залишковий ризик). Наприкінці виконується впровадження заходів та моніторинг ефективності.

Схематично послідовність дій за даною методикою наведено на рис. 1.7.

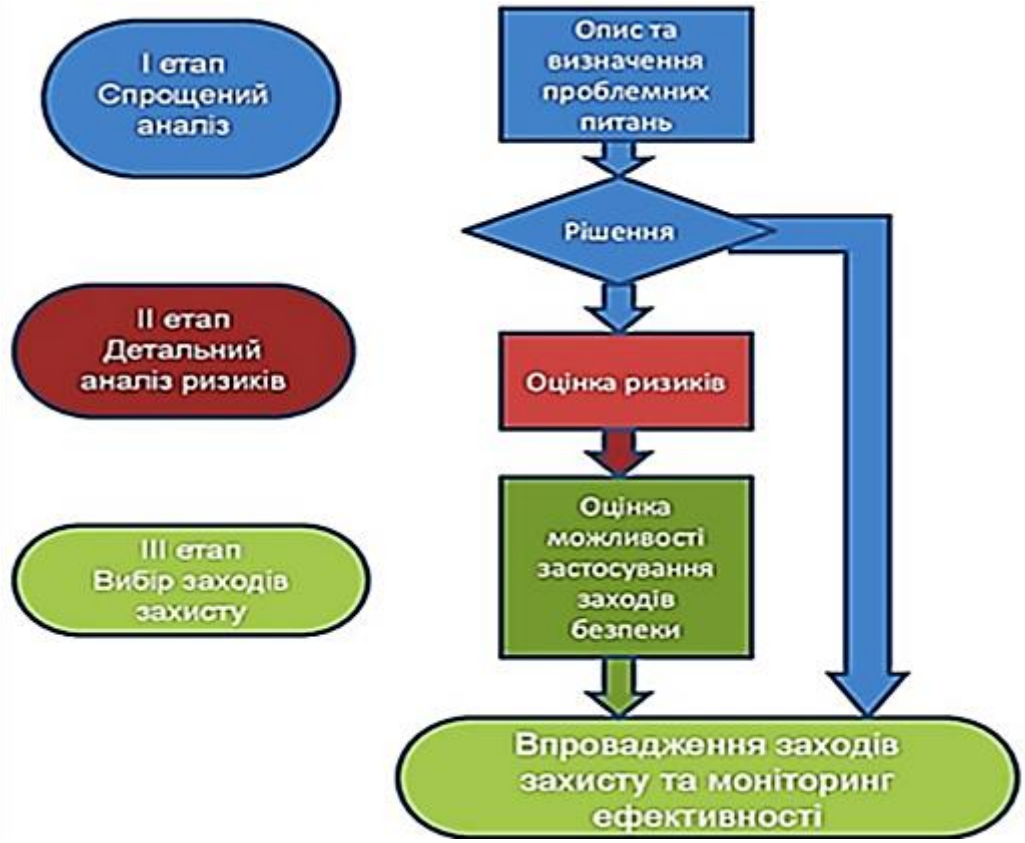


Рисунок 1.7 – Етапи методики MESARI

Методика оцінки ризиків IT за OCTAVE полягає у використанні послідовності відповідно організованих внутрішніх семінарів. Оцінка ризиків здійснюється в три етапи, яким передує набір підготовчих заходів: узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проєктної групи.

Підготовчий етап. Визначення пріоритетів.

Крок 1. Визначення критеріїв вимірювання ризиків. Критерії оцінки ризику є набір якісних параметрів, з допомогою яких проводиться опис ризику. Ці параметри можуть включати ймовірність реалізації ризику, збитки від нього та інші наслідки для організації. Також на даному етапі визначаються найбільш критичні сфери діяльності організації, для яких можуть бути задані різні рівні прийнятного ризику.

Етап 1. Профілювання IT-активів.

Крок 2. Розробка профілів IT-активів. Профіль являє собою опис IT-активу, що містить його унікальні особливості, якості, характеристики,

цінність та вимоги до інформаційної безпеки. Профіль для кожного активу фіксується на одному аркуші, цей документ формує основу для ідентифікації загроз та ризиків на наступних етапах.

Крок 3. Ідентифікація оточення IT-активів. Оточення описує місця, де зберігаються, транспортуються та обробляються IT-активи. Будь-які ризики для оточення IT-активу унаслідуються IT-активом, і це правило має ще більше значення для IT-активів, що надаються організації зовнішніми постачальниками.

Етап 2. Ідентифікація загроз.

Крок 4. Ідентифікація областей для занепокоєння. Цей крок є початком процесу ідентифікації ризиків шляхом мозкового штурму учасників проєктної команди. На даному етапі визначаються високорівневі області та типи ризиків, актуальні для аналізованих IT-активів.

Крок 5. Ідентифікація сценаріїв загроз. Визначається кілька типів загроз: людський фактор та використання технічних засобів, людський фактор з використанням фізичного доступу, технічні та інші проблеми. По кожному типу загроз для кожного IT-активу можуть бути визначені сценарії реалізації загроз, що містить опис їхнього впливу на IT-активи та ймовірність реалізації. При цьому можливість оцінюється як висока, середня або низька. Для спрощення цього процесу використовуються спеціальні опитувальні листи.

Етап 3. Ідентифікація та обробка ризиків.

Крок 6. Ідентифікація ризиків. Використовуючи інформацію про найбільш ймовірні сценарії загроз, на даному етапі проводиться аналіз їхнього впливу на IT-активи організації.

Крок 7. Аналіз ризиків. Використовуючи інформацію, отриману на попередніх етапах, проводиться оцінка впливу загроз на основну діяльність організації та ранжирування виявлених ризиків відповідно до критеріїв, визначених на етапі 1.

Крок 8. Вибір підходу до обробки ризиків. На цьому етапі для кожного ризику визначається стратегія його обробки залежно з його впливу на організацію.

Приклад оцінки ризиків за методикою OCTAVE наведено на рис. 1.8.

Area of Concern	Consequence	Impact Area	Ranking	Impact Value	Score
AC.1	1	Reputation	4	Moderate (2)	8
		Financial	3	Low (1)	3
		Productivity	5	Moderate (2)	10
		Legal Penalties	1	Low (1)	1
		User Defined	2	Low (1)	2
				Total Score	24
Area of Concern	**Consequence**	**Impact Area**	**Ranking**	**Impact Value**	**Score**
AC.2	2	Reputation	4	High (3)	12
		Financial	3	Low (1)	3
		Productivity	5	High (3)	15
		Legal Penalties	1	Low (1)	1
		User Defined	2	Moderat (2)	4
				Total Score	35
Area of Concern	**Consequence**	**Impact Area**	**Ranking**	**Impact Value**	**Score**
AC.3	3	Reputation	4	Moderat (2)	8
		Financial	3	Low (1)	3
		Productivity	5	High (3)	15
		Legal Penalties	1	Low (1)	1
		User Defined	2	Moderat (2)	4
				Total Score	31

Рисунок 1.8 – Розрахунок за методикою OCTAVE

Методика оцінки ризиків IT за IRAM складається з чотирьох етапів (основні дії наведені на рис. 1.9):

Етап 1. Ідентифікація інформаційних активів. Визначаються всі інформаційні активи організації та потенційні загрози, що можуть вплинути на їхню безпеку. Джерелами інформації можуть бути інвентарні дані активів, звіти про кіберінциденти, а також політики інформаційної безпеки організації.

Етап 2. Класифікація інформаційних активів з точки зору безпеки. Аналізуються вразливості активів, щоб оцінити, наскільки вони можуть бути використані загрозами.

Етап 3. Оцінка (моделювання загроз) для інформаційних активів. Оцінюються наслідки, які можуть виникнути у випадку реалізації загрози. Джерелом інформації є бізнес-аналізи, оцінки фінансових ризиків, а також

дані про можливі збитки або порушення роботи організації. Визначаються загальні ризики на основі ймовірності та потенційних наслідків для активів. Ризики класифікуються за ступенем важливості, що допомагає організації зрозуміти, які з них потребують першочергових заходів. Джерела інформації включають попередні звіти з аналізу ризиків та експертні оцінки.

Етап 4. Дія – заходи по зниженню або усуненню загроз. На основі аналізу розробляються стратегії для пом’якшення, уникнення або прийняття ризиків. Тут використовують нормативні вимоги, внутрішні політики безпеки, а також практичні рекомендації з безпеки. Регулярний моніторинг дозволяє підтримувати актуальність аналізу ризиків, враховуючи нові загрози та зміни в середовищі. Джерелами інформації на цьому етапі є системи моніторингу інформаційної безпеки, звіти про інциденти та регулярні внутрішні аудити.

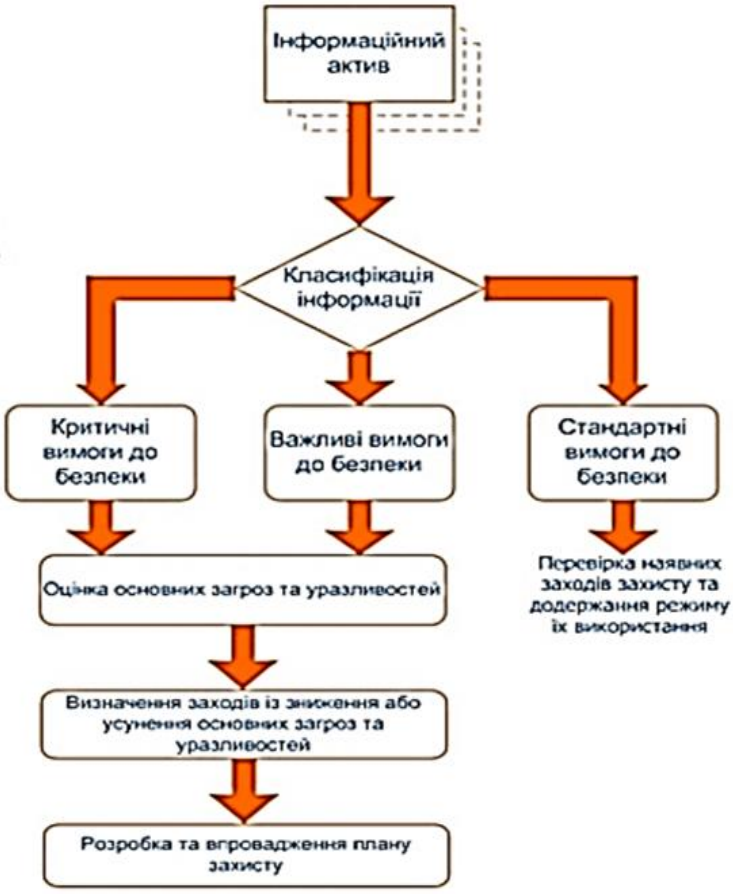


Рисунок 1.9 – Методика оцінки ризиків IRAM

Приклад оцінки ризиків за методикою IRAM наведено на рис. 1.10.

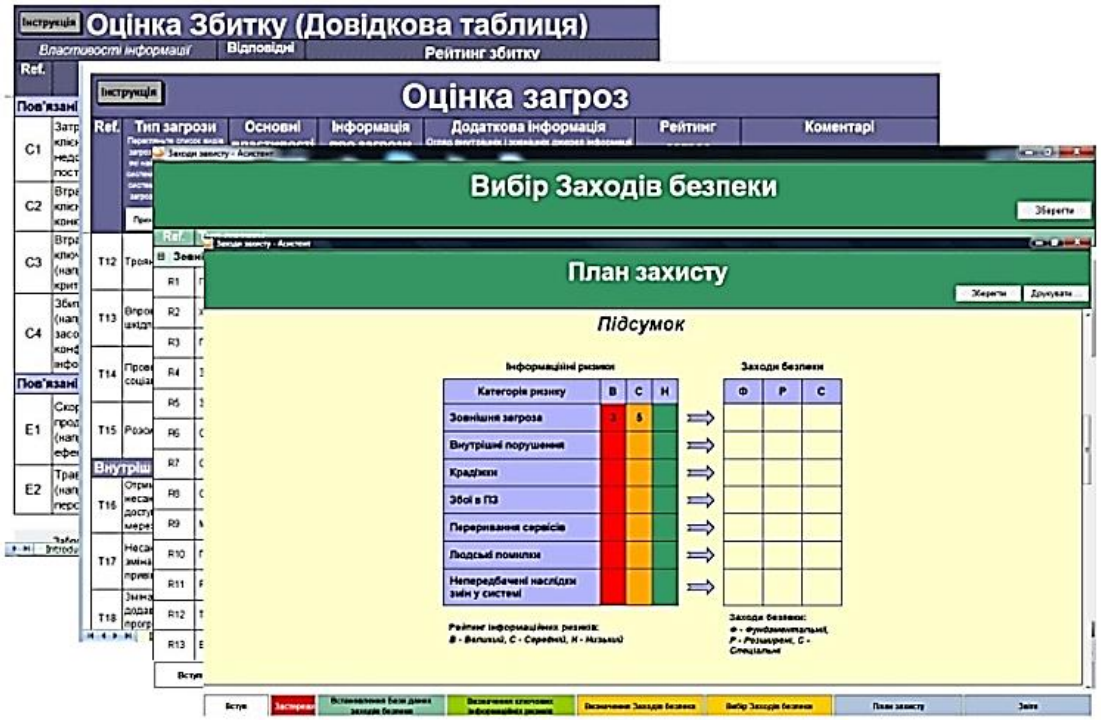


Рисунок 1.10 – Приклад оцінки ризиків IRAM

Методика оцінки ризиків IT за CRAMM. CRAMM (the UK Government Risk Analysis and Management Method) – метод, який розроблено Службою Безпеки Великої Британії та є її Державним стандартом. Він отримав широке поширення в світі, цей стандарт використовується як комерційними, так і державними організаціями Великобританії з 1985 року.

Метод CRAMM був винайдений фірмою Insight Consulting Limited. Базуючись на комплексному підході до оцінки ризиків, метод CRAMM поєднує кількісні і якісні методи аналізу ризиків і може бути застосований як у великих, так і невеликих організаціях (приватних).

Є різні версії CRAMM для різних типів організацій, вони відрізняються базами знань (профілями): існує комерційний профіль і урядовий профіль (за допомогою якого є можливість проводити аудит у відповідність з вимогами американського стандарту ITSEC — так званою «помаранчевою книгою»).

Процес управління ризиками за методикою CRAMM складається з таких етапів:

Етап 1. Ініціювання (Initiation). Проводиться серія інтерв'ю із зацікавленими в процесі аналізу ризиків інформаційної безпеки особами, у тому числі з відповідальними за експлуатацію, адміністрування, забезпечення безпеки та використання ІТ-активів, для яких проводиться аналіз ризиків. У результаті дається формалізований опис області для подальшого дослідження, її меж та визначається склад залучених до аналізу ризиків осіб.

Етап 2. Ідентифікація та оцінка ІТ-активів (Identification and Valuation of Assets). Визначається перелік ІТ-активів, що використовуються організацією у визначеній раніше галузі дослідження. ІТ-активи можуть бути одні з таких типів:

- дані;
- програмне забезпечення;
- фізичні активи.

Для кожного активу визначається його критичність для діяльності організації та, спільно з представниками підрозділів, які використовують ІТ-актив для вирішення прикладних завдань, оцінюються наслідки для діяльності організації від порушення його конфіденційності, цілісності та доступності.

Етап 3. Оцінка загроз та вразливостей (Threat and Vulnerability Assessment). Методологія містить таблиці, що описують відповідність між уразливістю ІТ-активів та загрозами, які можуть впливати на ІТ-активи через ці вразливості. Також існують таблиці, що описують збитки для ІТ-активів у разі реалізації цих загроз. Цей етап виконується лише для найбільш критичних ІТ-активів, для яких недостатньо впровадження базового набору заходів для забезпечення інформаційної безпеки. Визначення актуальних вразливостей та загроз здійснюється шляхом інтерв'ювання осіб, відповідальних за адміністрування та експлуатацію ІТ-активів. Для інших ІТ-активів міститься набір необхідних базових заходів для забезпечення інформаційної безпеки.

Етап 4. Обчислення ризику (Risk Calculation). Обчислення ризику виконується за формулою: Ризик = $Р_{реалізації}$ * Збитки. Ймовірність реалізації ризику обчислюється за такою формулою: $Р_{реалізації} = Р_{загрози} * Р_{вразливості}$. На етапі обчислення ризиків для кожного IT-активу визначаються вимоги до набору заходів щодо забезпечення його інформаційної безпеки за шкалою від 1 до 7, де значенням 1 відповідає мінімальний необхідний набір заходів щодо забезпечення інформаційної безпеки, а значенням 7 – максимальний.

Етап 5. Управління ризиком (Risk Management). На основі результатів обчислення ризику визначається необхідний набір заходів щодо забезпечення інформаційної безпеки. Для цього використовується спеціальний каталог, що включає близько 4 тис. заходів. Набір заходів порівнюється із заходами, які вже вжито організацією. У результаті ідентифікуються області, що вимагають додаткової уваги щодо застосування заходів захисту, і області з надмірними заходами захисту. Ця інформація використовується для формування плану дій щодо зміни складу вживаних в організації заходів захисту – для приведення рівня ризиків до необхідного рівня.

Методика оцінки ризиків IT за RISKWATCH. Розроблений американською компанією RiskWatch Inc. RiskWatch являє собою сімейство програмних продуктів, побудованих на загальному програмному ядрі, які призначені для управління різними видами ризиків з підтримкою різних стандартів. Деякі з них:

- RiscWatch for Physical Security – інструмент для фізичних методів захисту інформаційних систем;
- RiscWatch for Information Systems – інструмент, що застосовується до інформаційних ризиків;
- HIPPAA – WATCH for Healthcare Industry – інструмент для оцінки відповідності стандарту HIPAA;
- RiskWatch RW17799 for ISO17799 – для оцінки вимогам стандарту ISO17799.

Критеріями для оцінки і управління ризиками є очікувані річні втрати ALE (Annual Loss Expectancy) і оцінка повернення інвестицій ROI (Return on Investment). RiskWatch орієнтована на точну кількісну оцінку співвідношення втрат від загроз безпеки і витрат на створення системи захисту. В основі продукту RiskWatch знаходиться методика аналізу ризиків, яка складається з чотирьох етапів.

Етап 1. Визначення предмета дослідження. Описуються такі параметри, як тип організації, склад досліджуваної системи (в загальних рисах), базові вимоги в області безпеки. Зі списків категорій ресурсів, втрат, погроз, вразливостей і заходів захисту необхідно вибрати ті, що реально присутні в організації.

- затримки і відмова в обслуговуванні;
- розкриття інформації;
- прямі втрати (наприклад, від знищення обладнання вогнем);
- життя і здоров'я (персоналу, замовників тощо);
- зміна даних;
- непрямі втрати (наприклад, витрати на відновлення);
- репутація.

Етап 2. Введення даних, що описують конкретні характеристики системи. Дані можуть вводитися вручну або імпортуватися зі звітів, створених інструментальними засобами дослідження уразливості комп'ютерних мереж. Детально описуються ресурси, втрати і класи інцидентів. Задається частота виникнення кожної з виділених загроз, ступінь уразливості і цінність ресурсів.

Етап 3. Кількісна оцінка ризику. На цьому етапі розраховується профіль ризиків, і вибираються заходи забезпечення безпеки. Спочатку встановлюються зв'язки між ресурсами, втратами, загрозами і уразливими, виділеними на попередніх кроках дослідження. Ризик оцінюється за допомогою математичного очікування втрат за рік. Додатково розглядаються сценарії «що якщо:», які дозволяють описати аналогічні ситуації за умови

впровадження засобів захисту. Порівнюючи очікувані втрати за умови впровадження захисних заходів і без них можна оцінити ефект від таких заходів.

Етап 4. Формування звітів. Формується зумовлений набір звітів за результатами оцінки ризиків. Графіки, що використовуються в звітах, надають статистичну інформацію, наприклад, про розподіл уразливостей інформаційної системи по областях контролю. Рекомендовані контрзаходи можуть бути відсортовані в порядку зменшення значення ROI, що є одним з основних показників для прийняття рішення щодо реалізації контрзаходів та відповідних пріоритетів їх реалізації.

Методика оцінки ризиків ІТ за ГРИФ. На відміну від західних систем аналізу ризиків, які є доволі громіздкими і не передбачають самостійного застосування ІТ-менеджерами та системними адміністраторами, система ГРИФ має інтуїтивно-зрозумілий інтерфейс. Але за всієї простоти, у системі ГРИФ реалізовано величезну кількість алгоритмів аналізу ризиків, що враховують понад сто параметрів, і система здатна надати максимально точну оцінку ризиків, які мають місце в інформаційній системі.

Важлива особливість ГРИФ – у наданні можливості самостійного, без залучення експертів, оцінювання ризиків в інформаційній системі, оцінювання поточного стану, та розрахунку інвестицій з метою забезпечення захищеності інформації. Існують випадки, коли немає необхідності або можливості встановлення відповідності цінності інформації в грошових одиницях (наприклад, інформація особистого характеру, військова або політична інформація, оцінка якої в грошовому еквіваленті може бути нерозумною), але при цьому може мати сенс порівняльна оцінка окремих інформаційних компонентів однієї компоненти відносно іншої.

Як приклад можна розглянути ситуацію в державних структурах, де інформація розбивається за грифами секретності. Своєю чергою, грифи

секретності являють собою порядкові шкали цінностей, наприклад: несекретно, для службового користування, секретно, цілком таємно, особливої важливості (НС, ДСП, С, СС, ОВ); за американською системою: unclassified, confidential, secret, top secret (U, Conf, S, TS). Що вищий клас грифа, то більшу цінність має інформація, яку захищають, у зв'язку з чим стосовно неї застосовують вищі вимоги щодо її захисту від несанкціонованого доступу.

У табл. 1.11 наведено порівняння деяких методів оцінки ризиків ІТ.

Таблиця 1.11 – Порівняння деяких методів оцінки ризиків ІТ

Метод	Переваги	Недоліки
NIST	+Детальний опис всіх ризиків для активів +Найбільше підходить для відносно великих організацій.	–Довготривалий процес –Деякі функції не автоматизовані
FAIR	+Надає кількісний аналіз ризиків +Забезпечує симуляційну модель системи	–Занадто "науковий" метод –Тільки для відносно великих банків
MESARI	+Спрямований на банківську діяльність +Підходить для нових (новостворюваних) активів (проєктів)	–Важко запровадити для існуючих активів –Достатня складність –Відсутність автоматизації процесів оцінки
OCTAVE	+Швидко впроваджується +Добре застосовується для будь-якої організації	–Важкість реалізації окремих етапів та відсутність автоматизації –Не спрямований на специфіку банківської сфери
IRAM	+Відносна простота впровадження +Зрозумілість для менеджерів банківських установ +Є приклади успішного застосування	–Відносно дорогий –Краще застосовується до існуючих інформаційних активів.

Також існує ще багато інших методик, серед яких можна назвати [1]: MEHARI, MAGERIT, IT-Grundschutz, EBIOS, SARA, SPRINT, ISO 27005, MIGRA, MAR, ISAMM, GAO/AIMD-00-33, IT System Security Assessment, MG-2 і MG-3, Dutch A&K Analysis, MARION, Austrian IT Security Handbook, Microsoft's Security Risk Management Guide, Risk IT та ін.

У загальному вигляді аналіз ризиків здійснюється так, як наведено на рис. 1.11.

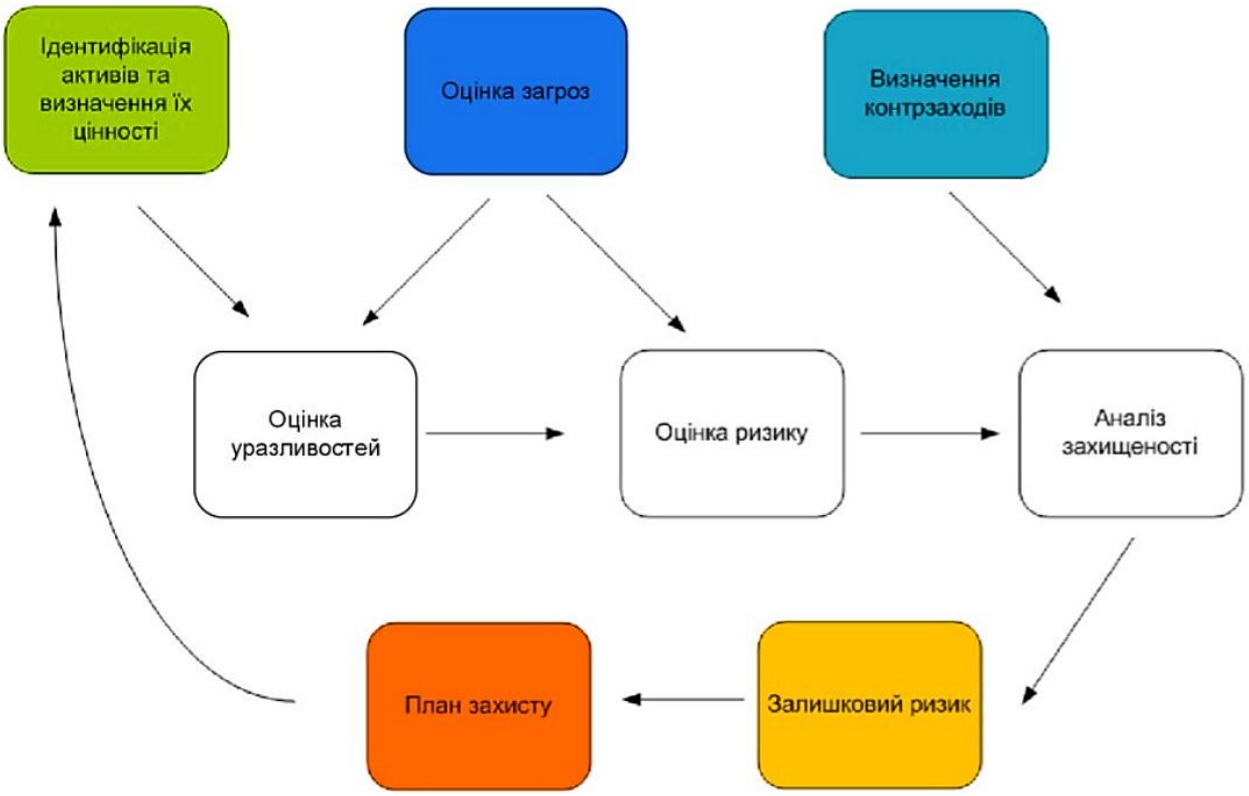


Рисунок 1.11 – Загальна схема процесу аналіза ризиків.

Контрольні питання

1. Що таке ризик?
2. Що таке уразливість?
3. Що таке загроза?
4. Якими методами оцінки ризиків можна скористуватись на практиці?
5. Що є чинниками ризиків в інформаційних технологіях?
6. Які виділяють індикатори ризику?
7. Що таке невизначеність?
8. Які існують причини невизначеності?
9. Чим відрізняється ситуація ризику від ситуації невизначеності?
10. Яким чином задається невизначеність?
11. Які основні категорії «ризик»?

12. Що таке повна та часткова невизначеність?

13. Що є джерелами ризику?

14. За якими ознаками класифікуються чинники ризику?

15. Опишіть основний алгоритм дій при ідентифікації ризиків.

16. Наведіть кілька методів ідентифікації ризиків.

17. Що є комерційними ризиками?

18. Які можливі наслідки ризику відмов машин та обладнання?

19. Що відноситься до підприємницьких ризиків?

20. Назвіть основні принципи механізму зниження ризиків.

21. Які існують рівні ризику?

22. Що таке якісний аналіз ризиків?

23. Що таке кількісний аналіз ризиків?

24. Основні критерії кількісної оцінки ризику.

25. Переваги та недоліки використання інформаційних технологій при зборі та обробці інформації для управління ризиком.

26. Що є основою статистичних методів оцінки ризиків?

27. Основа розрахунково-аналітичних методів оцінки ризиків.

28. Основа методу експертних оцінок ризиків.

29. На яких стандартах та рекомендаціях базуються основні підходи до управління ризиками в сфері інформаційних технологій?

30. Опишіть методологію оцінки ризиків NIST.

31. Опишіть методологію оцінки ризиків FAIR.

32. Опишіть методологію оцінки ризиків MESARI.

33. Опишіть методологію оцінки ризиків OCTAVE.

34. Опишіть методологію оцінки ризиків IRAM.

35. Опишіть методологію оцінки ризиків CRAMM.

36. Опишіть методологію оцінки ризиків RISKWATCH.

37. Опишіть методологію оцінки ризиків ГРИФ.

2. СУТНІСТЬ УПРАВЛІННЯ РИЗИКАМИ

2.1. Управління ризиками в організації

У сучасних умовах оцінка і аналіз ризику набувають самостійне теоретичне і прикладне значення як важлива складова частина теорії і практики управління, оскільки управлінські рішення приймаються в умовах ризику. Щоб вижити в умовах ринкових відносин, потрібно вирішуватися на впровадження технічних нововведень і на сміливі, нетривіальні дії, а це підсилює ризик. Звідси випливає, що треба не уникати ризику, а вміти оцінювати ступінь ризику і керувати ним. Управління ризиком визначає шляхи і можливості забезпечення стійкості підприємства, його здатності протистояти несприятливим ситуаціям.

Управління і ризик є взаємопов'язаними компонентами економічної системи. Перше само може виступати джерелом другого. Досвідчений підприємець при прийнятті ризикового рішення може інтуїтивно користуватися рядом підказаних практикою підходів і прийомів. Однак не можна, зрозуміло, покластися тільки на чисту інтуїцію і наявний господарський досвід. Необхідно спиратися на методологію (теорію) і науково обґрунтовані організаційні алгоритми управління ризиком.

Вивчення світового досвіду, зарубіжних і вітчизняних теоретичних розробок з управління ризиком дозволяє намітити шляхи відповідного пошуку.

Загальний концептуальний підхід до управління господарським ризиком полягає у виявленні можливих наслідків підприємницької діяльності в ризиковій ситуації; розробці заходів, що не допускають, запобігають або зменшують збиток від впливу до кінця не врахованих ризикових факторів, непередбачених обставин; реалізації такої системи адаптування підприємництва до ризиків, за допомогою якої можуть бути не тільки нейтралізовані або компенсовані негативні ймовірні результати, але і

максимально використані шанси на отримання високого підприємницького доходу.

У табл. 2.1 наведені визначення управління ризиками у низці національних і міжнародних стандартів.

Таблиця 2.1 – Визначення поняття управління ризиками

Назва стандарту	Визначення поняття «управління ризиками»
Стандарт Австралії і Нової Зеландії 1995 р.	сукупність культури, процесів та структур, орієнтована на використання потенційних можливостей при одночасному управлінні негативними впливами
Стандарт управління ризиками організацій, інтегрована модель (COSO), США	процес, який здійснюється радою директорів, менеджерами та іншими співробітниками, які можуть вплинути на організацію та управління пов'язаними з цими подіями
Стандарт по управлінню ризиками Федерації європейських асоціацій ризик- менеджерів (FERMA)	центральна частина стратегічного управління організацією, завданням якої є ідентифікація та управління, а також контроль, оцінка ефективності заходів, що проводяться, та система заохочення на всіх рівнях організації
Міжнародний стандарт ISO 31000: 2009	скоординовані дії для того, щоб спрямовувати та контролювати організацію щодо ризиків; архітектура, що складається з принципів, концепції та процесу

Необхідно відзначити, що як на практиці, так і в теорії одночасно застосовуються поняття «управління ризиками» і «ризик-менеджмент». В економічній літературі ці поняття часто мають одну і ту ж сутність, але в міжнародному стандарті ISO 31000:2009 «Ризик-менеджмент – принципи і керівництво» визначення цих двох понять виглядає таким чином: ризик-менеджмент – архітектура (тобто принципи, умови і процес) ефективного управління ризиками, а вираз «управління ризиками» ставиться до застосування даної архітектури щодо певного ризику.

Таким чином, можна сказати, що управління ризиками – сукупність заходів, інструментів і цілеспрямованих дій господарюючого суб'єкта, спрямованих на виявлення, прогнозування їх виникнення і зниження або виключення негативних наслідків від їх реалізації. Це систематичний,

взаємопов’язаний, взаємодоповнюючий і послідовний процес визначення і реалізації заходів щодо усунення або мінімізації негативних наслідків ризиків, а також по використанню потенційних можливостей з метою поліпшення фінансового добробуту та ефективності організації. А ризик-менеджмент – це стратегія і тактика управління всіма ризиками господарюючого суб’єкта.

Термін «управління ризиками» у нормативно-законодавчих актах України має кілька визначень:

- Закон України «Про об’єкти підвищеної небезпеки» від 18.01.2001 р. № 2245-III (в редакції № 1686-IX від 15.07.2021 р. визначення було видалено): «управління ризиком – процес прийняття рішень і здійснення заходів, спрямованих на забезпечення мінімально можливого ризику».

- Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом» від 28.11.2002 р. № 249-IV (втратив чинність 06.02.2015 р., підстава № 1702-VII): «управління ризиками – заходи, які здійснюються суб’єктами первинного фінансового моніторингу, з визначення, оцінки, моніторингу, контролю ризиків, що спрямовані на їх зменшення до прийнятного рівня».

- Наказ Державної Податкової Адміністрації України «Про затвердження Методичних рекомендацій щодо організації проведення перевірок підприємств, які входять до складу фінансово-промислових груп, інших об’єднань та великих платників податків» від 16.07.2007 р. № 432: «управління ризиками – процес вивчення та упередження можливості втрати бюджетних надходжень, а також удосконалення методів виявлення та усунення порушень податкового та валютного законодавства».

- Наказ Міністерства Фінансів України «Про затвердження Термінологічної бази системи внутрішнього контролю та аудиту Державного казначейства України» від 07.10.2008 р. № 417: «управління ризиками – діяльність, пов’язана із ідентифікацією, аналізом ризиків та прийняттям рішень, які мінімізують негативні наслідки настання ризикових подій, метою

якої є найбільш раннє виявлення можливих недоліків, порушень, неефективного використання ресурсів...».

- Постанова Кабінету Міністрів України «Про затвердження Методики виявлення ризиків здійснення державно-приватного партнерства, їх оцінки та визначення форми управління ними» від 16.02.2011 р. № 232 (в редакції № 713-2015-п від 30.09.2015 р.): «управління ризиками – процес, що триває протягом здійснення державно-приватного партнерства і передбачає виявлення, оцінку ризиків, визначення шляхів запобігання їх виникненню, ліквідацію негативних наслідків і передачу ризиків (включаючи страхування), а також прийняття ризиків».

При управлінні ризиками в організації слід зауважити, що:

- не існує діяльності, при реалізації якої можна було б повністю уникнути ризиків;

- не існує ризиків, якими не можна управляти.

Переваги застосування ризик-менеджменту на підприємстві є:

- збільшення прибутковості;

- підвищення економічної вартості підприємства;

- підвищення привабливості підприємства для інвесторів через зниження мінливості рівня доходів;

- удосконалення процесу прийняття рішень;

- формування «правильних» стимулів для менеджерів (система винагород, прив’язана до результатів основної діяльності фірми).

Ризикова ситуація, яка може виникнути, має такий життєвий цикл:

- поява сигналів про можливість виникнення;

- поява ознак виникнення;

- розгортання наслідків у просторі й у часі (безпосередній розвиток ризикової ситуації);

- проявлення результатів прийнятих рішень і вжитих дій по управлінню (вирішення ризикової ситуації) або провал проєкту (у випадку неприйняття

або несвоєчасного прийняття рішень, або неефективності запропонованих заходів, або невиконання або неякісного виконання ухвалених рішень).

Під час реалізації управління ризиками важливо враховувати такі особливості:

- всі ризики мають приховану і відкриту фазу, і з метою подолання ризиків-небезпек необхідно для кожної з цих фаз визначати і реалізовувати їм відповідні заходи і дії;

- різні види ризиків взаємопов'язані і зміна одного з них може спонукати до зміни або появи іншого ризику (ризиків);

- рівень ризику окремої угоди або діяльності однієї і тієї ж організації залежно від постійних змін умов навколишнього середовища господарюючого суб'єкта може змінюватися.

Оптимальний процес управління ризиками складається з таких етапів:

Етап 1. Ідентифікація ризиків:

- встановлення критеріїв ризику;

- розробка методів виявлення ризиків;

- створення системи класифікації ризиків.

Етап 2. Аналіз та оцінка ризиків:

- складання переліку можливих ризикових ситуацій;

- оцінка ступеня та рівня ризику для кожної ситуації;

- визначення пріоритетності ризиків.

Етап 3. Розробка заходів для управління ризиками:

- визначення методів реагування на ризики;

- організація процесу управління ризиками;

- розробка запобіжних заходів для мінімізації ризиків.

Етап 4. Моніторинг і оперативне управління ризиками:

- впровадження методів управління ризиками;

- оцінка ефективності процесу управління ризиками;

- створення системи управління знаннями про ризики.

Комітетом організацій-спонсорів Комісією Тредвея COSO (Committee of Sponsoring Organizations of the Treadway Commission) розроблено основи управління ризиками організацій COSO ERM (COSO Enterprise Risk Management) [15].

Універсальна модель складається з елементів управління ризиками організацій:

1. Система внутрішнього контролю та система управління ризиками будуються із взаємопов'язаних компонентів, які є необхідними інструментами для досягнення цілей та діють у складі єдиного комплексу заходів.

2. Взаємозв'язок цілей, компонентів та організаційних структур внутрішнього контролю та управління ризиками представлений у моделях COSO тривимірною матрицею, що має форму куба (куб IC-COSO – внутрішній контроль, куб ERM-COSO – управління ризиками).

3. Універсальність моделей COSO полягає в можливості їх використання для різних рівнів управління – окремого підрозділу, організації загалом, групи взаємопов'язаних компаній.

Модель визначає основні компоненти управління ризиками установ, що базується на ключових принципах і концепції управління ризиками, пропонує загальну термінологію управління ризиками і передбачає чіткі вказівки і директиви для управління ризиками установ. Модель COSO ERM наведена на рис. 2.1. Кожна вісь куба описує свої функції:

1. На першій, передній осі відображені елементи контролю ризиками:

- реагування на ризики – керівництво обирає метод реагування на ризик – ухилення від ризику, прийняття, скорочення або перерозподіл ризику;

- контрольні заходи – розробка та впровадження заходів щодо управління ризиками;

- інформація та комунікації – необхідна інформація визначається, фіксується та передається в такій формі та в такі терміни, які дозволяють співробітникам виконувати їх функціональні обов'язки;

- моніторинг – весь процес управління ризиками організації відслідковується та за потреби коригується.

2. На другій, бічний стороні куба – рівні управління ризиками: цілі та процеси, що визначені в рамках інших напрямків, повинні виконуватися на всіх рівнях організації.

3. На третій, на маківці куба, розташовуються цілі управління:

- стратегічні;

- операційні;

- у сфері підготовки звітності;

- цілі дотримання законодавства (відповідності вимогам).

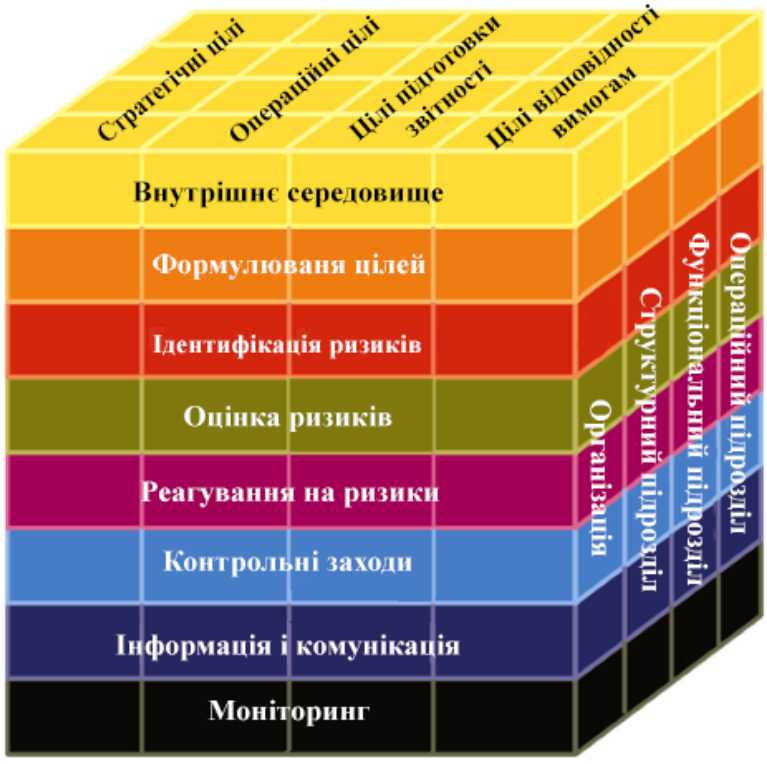


Рисунок 2.1 – Модель COSO ERM

У документі ISO 31000:2018 «Менеджмент ризиків. Принципи й керівні вказівки» (оновлення стандарту ISO 31000:2009) висвітлено

принципи управління ризиками для поліпшення планування і прийняття ефективних рішень. Головну увагу приділено передусім створенню та захисту цінностей як ключовому компоненту управління ризиками, а також особливостям інших суміжних принципів (таких як постійне вдосконалення, залучення зацікавлених сторін), спрямованих на організацію і врахування людських і культурних чинників. Головна мета стандарту – допомогти організаціям у досягненні успіху в довгостроковій перспективі з урахуванням всіх зацікавлених сторін, забезпечуючи належні практики управління ризиками. Схематично процес управління ризиками відповідно до стандарту ISO 31000:2018 наведено на рис. 2.2.

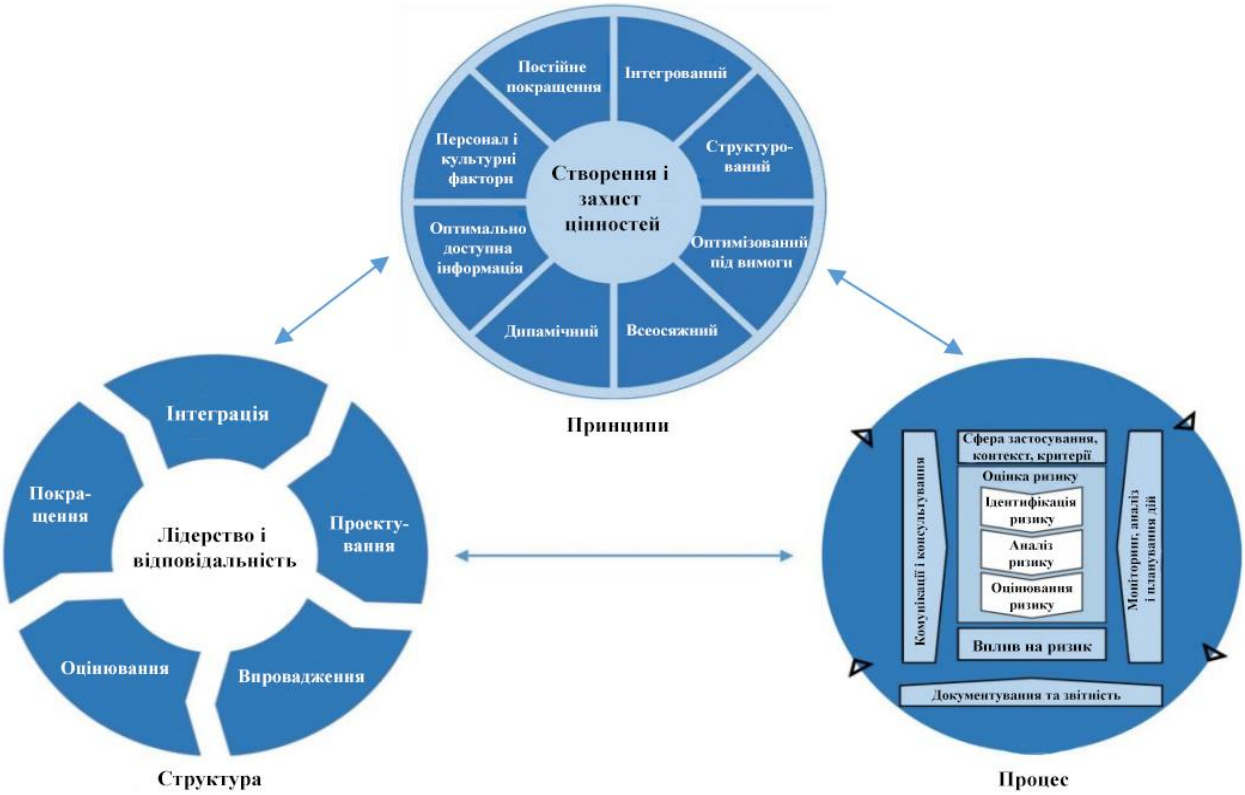


Рисунок 2.2 – Модель ISO 31000:2018

Управління ризиками відіграє важливу роль у загальній системі менеджменту будь-якої організації, це зумовлюють такі аспекти:

- управління ризиками має починатися вже з моменту розробки стратегії організації. Власники компанії при розробці стратегії вже повинні визначити свій ризик-апетит, тобто максимальний рівень сумарного ризику,

на який буде готова йти компанія. Ризик-апетит пов’язаний зі стратегією господарюючого суб’єкта, якщо цей суб’єкт прийняв стратегію завоювання нового сегменту ринку, то він, відповідно, має високий рівень ризик-апетиту. Отже, при розробці стратегії важливо враховувати ризики і дуже часто буває так, що високий рівень ризику є причиною перегляду стратегії організації;

- для ефективної діяльності доцільно залучати всіх робітників і підрозділи в процес виявлення небезпек і можливих збитків, тобто важливо інтегрувати управління ризиками в загальну систему менеджменту організації. Це дає можливість підвищити зацікавленість всіх фахівців у високих результатах господарюючого суб’єкта;

- необхідно централізовано керувати всіма ризиками організації, і тому що всі ризики взаємопов’язані, важливо контролювати сумарні ризики, а також сумарні витрати на управління ризиками;

- застосування інтегрованого підходу до управління ризиками не повинно формувати умову для відсутності окремого підрозділу, що займається питаннями виявлення та управління ризиками. Тобто, даний відділ як спеціалізований центр повинен збирати всю інформацію про ризики та небезпеки від всіх функціональних служб і відповідно до отриманих даних застосовувати певні методи, процедури і способи управління виявлених ризиків. Даний відділ, координуючи і проводячи моніторинг ризиків, контролює весь процес управління організації в цілому, виконуючи функцію внутрішнього контролю. Оскільки контроль є одним з важливих елементів процесу управління організації в цілому, служба ризик-менеджменту разом з іншими функціональними відділами здійснює процес управління даною організацією, ґрунтуючись на критерії «дохідність / ризик».

Ключовими властивостями системи ризик-менеджменту є:

1. Системний характер управління ризиком. Дана властивість системи управління ризиком передбачає комплексне дослідження сукупності можливих ризиків як єдиного цілого, з урахуванням їх взаємозв’язків і очікуваних результатів. Поряд з отриманою загальною картиною про

можливу ризикової ситуації це дозволяє не тільки знайти інструмент управління ризиком, але й визначити взаємодію ризиків залежно від їх місця і зв'язків усередині системи, а також імовірність появи нових ризиків. Дослідження передбачає розгляд таких аспектів ризик-менеджменту:

- цілісність, тобто орієнтація на загальну оцінку сукупності ризиків і виключення негативних результатів з урахуванням характеру їх взаємодії;

- комплексність, тобто вивчення сукупності ризиків, включаючи їх взаємозв'язок, безлічі можливих результатів результату ризикової події і заходів, що вживаються до виключення або зниження ризику;

- здатність системи до інтеграції нових елементів, тобто можливість гнучкого реагування всієї системи на появу нових ризиків, у тому числі і породжених самою системою управління ризиком.

2. Складна структура системи управління ризиком. Дана властивість передбачає аналіз сукупності ризиків, тобто значну неоднорідність природи їх прояви, а також особливості взаємодії і можливість застосування системи управління ризиком для вирішення проблем різного рівня. Крім того, представлена властивість системи управління ризиком досліджує характер і ступінь впливу сукупності факторів на розвиток ризикової події та можливості отримання негативних результатів. Слід враховувати деякі аспекти ризик-менеджменту:

- багатофункціональність і універсальність, тобто здатність виключати ризики з різною природою прояви і можливими їх наслідками;

- модульність, тобто поєднання можливих процедур управління ризиком у різних ситуаціях, що дозволяє врахувати специфіку конкретної ризикової ситуації і при необхідності знайти рішення для індивідуального випадку;

- багаторівневість, тобто знаходження найкращого алгоритму прийняття управлінських рішень, який забезпечує адекватний розподіл повноважень і відповідальності.

3. Висока результативність системи управління ризиком. Ця властивість передбачає здатність сукупності заходів ризик-менеджменту до зниження ймовірності виникнення негативного результату подій і до подолання їх наслідків. Зазначена ієрархічна система управління ризиком повинна оперативно реагувати на зміну зовнішніх і внутрішніх факторів, тобто повинна володіти сформованими контурами зворотного зв'язку, а також генерувати ефективні рішення, спрямовані на отримання бажаного результату і зниження фінансових втрат. Система управління ризиком для забезпечення представлених вимог повинна відповідати таким критеріям:

- гнучкість і адаптивність, тобто значна швидкість реагування, здатність до адаптації до постійно модифікуються умов стрімко справлятися з несприятливими ситуаціями;

- адекватність, тобто відповідність реалізованих заходів управління ризиком, виражається в здатності оперативно виявляти можливі ресурси, необхідні для досягнення очікуваних результатів;

- ефективність, тобто здатність долати вплив негативних результатів ситуацій при мінімальному обсязі можливих ресурсів. Система ризик-менеджменту повинна забезпечувати чистий ефект, тобто витрати на управління ризиком і розмір потенційного збитку в результаті реалізації методів управління повинні бути менше можливого збитку до проведення заходів щодо захисту настання ризикової події.

Представлені властивості системи ризик-менеджменту є загальними і універсальними. Проте система управління ризиком має певну специфіку, яка проявляється в ключових принципах і обумовлена особливостями об'єкта, цілей і методів управління.

З безлічі принципів управління ризиком можна виділити основні:

1) не можна ризикувати більше, ніж це може дозволити власний капітал. Принцип вимагає, щоб підприємець визначив максимальний збиток у результаті негативного відхилення від середньо очікуваного значення та оцінив ймовірність настання катастрофічного ризику;

2) необхідно думати про наслідки ризику. Прийняття рішення про управління ризиком (відмова від ризику; передача ризику, тобто страхування або хеджування; прийняття ризику на свою відповідальність) на основі прогнозних значень максимального збитку в разі настання ризикової ситуації;

3) не можна ризикувати багато чим заради малого. Принцип припускає порівняння прогнозованого доходу з очікуваними втратами.

Загальний процес управління ризиками на підприємстві наведено на рис. 2.3.

Рисунок 2.3 – Процес управління ризиками

На рис. 2.4 наведено типовий життєвий цикл ризикової ситуації при управлінні ризиками (УР) [15].

Рисунок 2.4 – Життєвий цикл ризикової ситуації

Підприємницька діяльність характеризується широким спектром ризиків, тому управління ризиком має являти собою комплексну систему дієвих заходів щодо подолання несприятливих наслідків настання ризикової події.

Ідентифікація ризиків – формування в осіб, що приймають рішення, цілісного бачення ризиків, що загрожують підприємству, його персоналу, майновим інтересам акціонерів, зобов’язанням, що виникають у процесі взаємовідносин з клієнтами та іншими контрагентами. Ідентифікацію ризиків необхідно проводити в два етапи:

1) ідентифікація окремих видів ризиків, що дозволяє ризик-менеджерам визначити специфіку можливої ризикової ситуації і її особливості в результаті песимістичного розвитку подій. Такий аналіз дозволяє знайти вибрати дієві інструменти управління для кожного виду ризику;

2) дослідження сукупності ризиків, що дозволяє визначити комплексний вплив ризиків на об’єкт. Подібний аналіз дозволяє дійти спільної точки зору на сукупність ризиків, притаманних конкретній компанії, отже, виявити дієві заходи з управління ризиком.

Система управління ризиком повинна ґрунтуватися на двох рівнях ідентифікації ризиків і об’єднувати інструменти і методи, характерні для

кожного з них. Недотримання цієї вимоги може привести до несприятливих наслідків ризикової ситуації.

Під час ідентифікації ризику необхідно враховувати глобальні ризики. Фрагменти звіту за 2023-2024 роки про основні глобальні ризики з джерела World Economic Forum Global Risks Perception Survey наведено на рис. 2.5 та рис. 2.6 за останні 2 та 10 років відповідно.

Рисунок 2.5 – Основні глобальні ризики за останні 2 роки

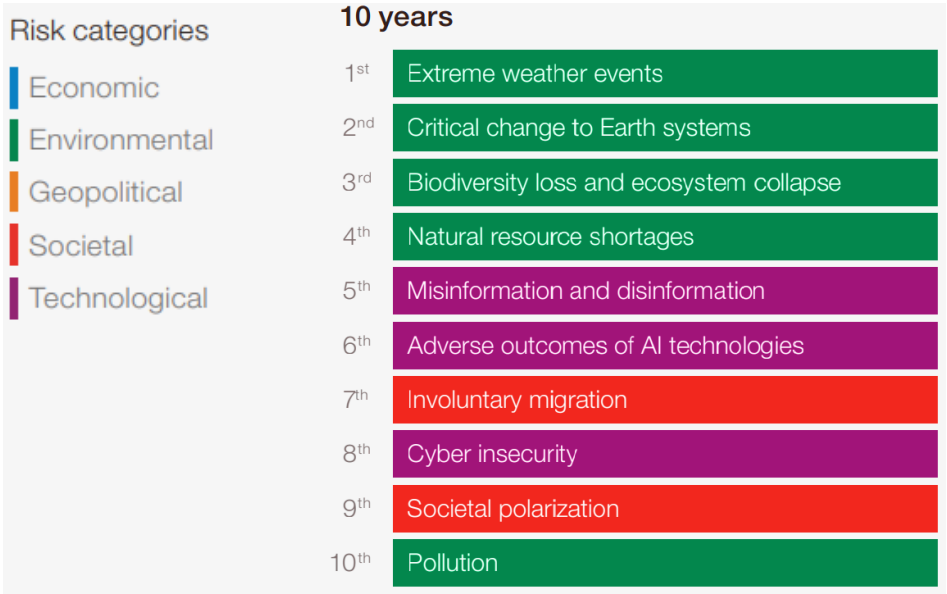


Рисунок 2.6 – Основні глобальні ризики за останні 10 років

За останні 2 роки основними глобальними ризиками є: відсутність інформації та дезінформація, екстремальні погодні явища, поляризація суспільства, кібербезпека, міжнародний збройний конфлікт, відсутність економічних можливостей, інфляція, вимушена міграція, економічний спад, забруднення навколишнього середовища.

За останні 10 років основними глобальними ризиками є: екстремальні погодні явища, критична зміна земних систем, втрата біорізноманіття та колапс екосистеми, дефіцит природних ресурсів, відсутність інформації та дезінформація, несприятливі наслідки технологій штучного інтелекту, вимушена міграція, кібербезпека, поляризація суспільства, забруднення навколишнього середовища. Як можна помітити, ризики з кібербезпеки (Cyber insecurity) займають високі місця.

Аналіз ризиків – систематичне використання інформації про ризик, його вимірювання, оцінка, порівняння з прийнятним ризиком, обґрунтування раціональних заходів захисту.

Дослідження ризику в комплексі з джерелами невизначеності, пов’язаними з проявом окремих ризиків, передбачає ще один аспект – ступінь взаємозв’язку між ризиками. Як правило, спостерігається відсутність повної інформації про такий взаємозв’язок. Даний аспект є важливим джерелом невизначеності.

До того ж природа ризиків різна, тому процес управління ризиків повинен бути комплексним і враховувати особливості внутрішніх зв’язків між ризиками. Таким чином, процес управління ризиком дуже складний, особливо для великих об’єктів.

У зв’язку з цим дослідження ризиків в їх сукупності дає такі переваги:

- результативна організація надходження інформаційних масивів, які дозволять знайти комплексне рішення проблеми;

- забезпечення безпеки прийнятих рішень, у тому числі – відсутність інформаційних витоків, своєчасність прийняття рішень і подолання адміністративних бар’єрів;

- повний облік можливих ресурсних і часових обмежень для прийняття рішень для найбільш ефективного управління ресурсами.

Поєднання всіх вимог з урахуванням особливостей конкретних ризиків на основі індивідуального підходу робить систему управління ризиком адекватною і гнучкою.

Управління ризиком являє собою динамічний процес, оскільки бізнес функціонує в швидко мінливих умовах, тому розглядати управління ризиком як одномоментну дію, навіть якщо вона детально пророблена і обґрунтована, не можна. Збір інформації, оцінка та аналіз ризиків, а також знаходження рішень про реалізацію тих чи інших методів управління ризиками повинні бути постійними в загальному процесі управління бізнесом.

З вищесказаного випливає, що основними прийомами управління ризиком є:

1) усунення ризику – відмова від ризикової ситуації. Однак можливо понести втрати від невикористаних можливостей;

2) зниження ступеня ризику означає зниження ймовірності настання ризикової ситуації і обсягу негативних наслідків. Йдеться про передачу ризику третім особам – страховій компанії, або методу диверсифікації;

3) прийняття ризику передбачає залишення всього або частини ризику за особою, яка приймає рішення покрити можливі збитки за рахунок власних коштів.

Вибір методу управління ризиком повинен здійснюватися на основі таких правил:

- максимум виграшу, максимальний результат при прийнятному ризику;

- оптимальне поєднання виграшу і величини ризику, тобто варіант, в якому співвідношення доходів і втрат найбільше;

- оптимальна ймовірність результату, тобто вибір варіанту, в якому виграш максимальний.

Основна мета управління ризиком – отримання максимального прибутку при оптимальному, прийнятному співвідношенні прибутку і ризику для особи, яка приймає рішення.

Керівництво компанії вибирає обережний варіант управління ризиками, якщо політика ризик-менеджменту спрямована на мінімізацію ризику банкрутства, зниження втрат очікуваного доходу або прибутку, а також на появу додаткових витрат. Проте слід зазначити, що як правило, найбільш ризикована стратегія дозволяє компанії зайняти нову ефективну нішу на ринку і отримати більше прибутку.

Взаємозв'язок між системою ризик-менеджменту компанії і стратегією її розвитку виявляється не тільки в тому, що стратегія обумовлює політику управління ризиком, але і в наявності зворотного зв'язку, тобто вибір варіанту управління ризиком може припускати коригування прийнятої стратегії або попереднього обліку деяких ризиків при формуванні стратегії. Даний факт можна пояснити специфічним впливом ризику на такі цілі компанії:

- продовження операцій. Подія, яка виникає внаслідок реалізації ризикової ситуації, може виявитися з негативним результатом, що призведе до припинення операцій: банкрутство компанії. Таким чином, місія і цілі компанії не будуть реалізовані. У зв'язку з цим стратегія компанії повинна припускати ймовірність виникнення подібних ситуацій;

- стабільність операцій і (або) грошових потоків. Ризики, які безпосередньо впливають на реалізацію даної мети, зустрічаються часто. У цілому компанія зберігає бізнес, але з'являються значні проблеми в досягненні стратегічних цілей при реалізації таких ризиків. У такій ситуації стратегія компанії зазнає значних змін. Слід зазначити, що коштовні заходи, спрямовані на зниження ступеня ризику, можуть зробити негативний вплив на стабільність операцій і (або) грошових потоків;

- прибутковість операцій. Прибутковість операцій – необхідна умова функціонування компанії в довгостроковій перспективі, проте компанія може

собі дозволити для досягнення деяких цілей відносно короткі періоди збиткової роботи. Відзначимо, що зменшення доходу як наслідок негативних подій означає порушення нормального функціонування компанії. Тому стратегія розвитку повинна враховувати ймовірність виникнення подібних ризиків;

- зріст. Стратегія розвитку компанії в сучасних умовах економіки передбачає її зростання. У зв'язку з цим аналіз ризиків, які мають негативний вплив на її зростання, слід розглядати як невід'ємну частину стратегії розвитку. Якщо при формуванні стратегії не враховані подібні ризики, реалізація заходів з управління ризиками може зажадати її перегляду або відмови від неї;

- інші цілі. Стратегія компанії може виключати реалізацію інноваційних цілей. Досягнення подібних цілей може бути ускладнене проявом певних ризиків. Проведений аналіз свідчить про безпосередній зв'язок між стратегією компанії і системою ризик-менеджменту, що свідчить про необхідність виявлення ризику і визначення заходів з управління ними, а також про те, що управління ризиком – невід'ємна частина менеджменту компанії.

Єдність системи ризик-менеджменту та менеджменту компанії є не тільки на етапі координування цілей, але і на етапі прийняття рішень. Це означає, що менеджерам необхідно враховувати особливості організаційної структури компанії і специфіку можливих ризиків і заходів з управління ними.

Таким чином, політика управління ризиком не може бути відокремлена від основної політики компанії, оскільки ризик-менеджмент необхідний для реалізації останньої. Тому заходи з управління ризиком повинні бути ув'язані з рішеннями про ведення бізнесу компанії.

На практиці можливі ситуації, коли вигідніше передати систему управління ризиком або її окремі функції (наприклад, оцінку ризику або управління конкретними ризиками) стороннім організаціям. Такий підхід з

управління ризиком називається аутсорсингом управління ризиком (Risk management outsourcing).

Головна мета системи ризик-менеджменту – забезпечення успішного функціонування компанії в умовах ризику і невизначеності. Таким чином, при настанні ризикової події заходи з управління ризиком повинні забезпечити компанії можливість продовження фінансових операцій, стабільне і стійке надходження відповідних грошових потоків, отримання прибутку і її зростання, а також досягнення інших цілей.

Поряд з головною метою система ризик-менеджменту має такі допоміжні цілі:

- забезпечення результативності операцій. Дана мета передбачає збільшити витрати на реалізацію заходів з управління ризиком для забезпечення обумовленої захисту від надмірно великих втрат, які можуть виникнути з мінімальною ймовірністю;

- знаходження оптимального рівня невизначеності в разі отримання негативного результату. Дана мета означає, що якщо не можна повністю уникнути ризику, то слід мінімізувати його до прийнятного рівня;

- законність дій. Ця мета означає, що реалізація заходів не повинна суперечити основній меті системи управління ризиком;

- інші цілі. Зміст таких цілей залежить від діяльності компанії і заходів з управління ризиками.

Таким чином, ієрархія цілей системи ризик-менеджменту формується залежно від особливості ризикової ситуації і заходів з управління ризиками. Тому при розробці системи цілей ризик-менеджменту слід дотримуватися таких умов:

- визначити необхідність реалізації поставлених додаткових цілей, тобто розподілити їх відповідно до пріоритетністю, виявити їх вплив на фінансову діяльність компанії;

- оцінити необхідність у ресурсах для досягнення цілей. Реалізація одних цілей вимагає великих ресурсів, ніж інших, тому врахування даної

обставини важливо для усвідомлення можливостей системи управління ризиком та її цілей;

- враховувати взаємозв'язок і суперечливість цілей, тобто облік внутрішніх зв'язків між цілями дозволяє підвищити результативність системи управління ризиком у цілому.

Ефективне функціонування системи управління ризиком неможливе без урахування зовнішніх і внутрішніх обмежень середовища, в якому існує бізнес. Ефективність процесу прийняття рішень залежить від розуміння особливостей подібних обмежень. У зв'язку з цим дослідження обмежень системи управління ризиком – важливий етап процесу ризик-менеджменту.

Зовнішні обмеження характеризуються факторами, на які неможливо зробити безпосередній вплив:

- законодавчі обмеження. Подібні обмеження зовнішнього середовища можуть бути представлені законодавчими і нормативними актами;

- обмеження, пов'язані із зобов'язаннями контрагентів та зобов'язаннями перед ними. Контрагенти – це суб'єкти, з якими компанія стикається в своїй діяльності. Контрагентами є партнери по бізнесу, працівники компанії, клієнти. Прикладами таких зобов'язань можуть бути видача або отримання кредитів, борги дочірньої компанії. Подібні зобов'язання роблять різний вплив на можливі ризики компанії. Наприклад, вони можуть знизити ймовірність виникнення втрат, якщо компанія, яка ефективно працює на ринку, виконує свої зобов'язання. Однак чужі зобов'язання перед компанією, навпаки, можуть посилювати ризик збитків, наприклад, якщо боржником є компанія, що працює на ринку неефективно;

- кон'юнктурні обмеження. Такі обмеження пов'язані зі специфікою макроекономічних процесів. Наприклад, ризик втрати фінансової стійкості збільшується в умовах рецесії і спаду, тому в такі періоди бізнес-циклу можливість мінімізації цього ризику знижується. Іншим прикладом можуть бути фінансові ринки, які характеризуються періодичним зростанням

волатильності, що збільшує ймовірність втрати платоспроможності організацій, які купують відповідні фінансові інструменти.

Внутрішні обмеження пов’язані з особливостями функціонування компанії і прийняття управлінських рішень. Моніторинг обмежень цього виду дає можливість менеджеру знайти вузькі місця при управлінні ризиком. До внутрішніх обмежень відносяться:

- інституційні обмеження, тобто обмеження, певні особливостями функціонування різних підрозділів компанії і механізмами їх взаємодії. Такі обмеження безпосередньо впливають на прийняття рішень з управління ризиком;

- бюджетні обмеження, тобто наявність лімітів фінансування заходів з управління ризиком. Ризик-менеджмент є частиною діяльності компанії, тому він повинен підкорятися загальним обмеженням на витрати. Таким чином, компанія може витратити на заходи з управління ризиком тільки виділені бюджетом кошти;

- інформаційні обмеження, тобто неповнота інформації або її відсутність значно впливає на процес управління ризиком, що може привести до неправильних рішень. Тому інформаційне забезпечення надмірно важливе в ризик-менеджменті.

Переваги використання ризик-менеджменту:

1. Зниження рівня невизначеності. Крім контролю над впливом невизначеності на цілі підприємства, розробляється комплекс заходів щодо зниження ймовірності появи негативних наслідків, а також дії щодо мінімізації впливу ризиків, які реалізуються.

2. Пошук перспективних шляхів розвитку. Крім негативних наслідків управління ризиками дозволяє знайти і побачити позитивні можливості шляхом придбання навичок розпізнавання ризиків і пошуку нових перспектив з максимальною вигодою і ефективністю.

3. Підвищення ефективності та оптимізація планування. Ризик-орієнтоване мислення в процесі прийняття рішень дозволяє отримати більш

коректні та точні дані, основні показники, результати протікання процесів та можливі перспективи розвитку, що надає більш об'єктивні можливості для ефективного управління та планування діяльності підприємства.

4. Економія ресурсів. При управлінні ризиками, особлива увага приділяється економічній доцільності проведення заходів різного характеру. Регулярний перегляд і аудит ресурсів дозволяє збільшити ліквідність активів, тим самим уникнувши втрати і збільшивши доходи організації.

5. Положення на ринку та імідж. Впроваджені процеси управління ризиками на підприємстві дають можливість бути більш привабливими для інвесторів, банків, страхових компаній, постачальників і клієнтів, отримувати пільгові кредити, особливі умови страхування, участь у тендерах, участь у міжнародних проєктах, збільшення кількості клієнтів тощо.

6. Виконання вимог зацікавлених сторін. Відповідність очікуванням акціонерів, ради директорів, регуляторів, органів влади, щодо того, що заходи з управління ризиками будуть вжиті. Це дозволяє не тільки економити кошти, але й підвищити конкурентоспроможність на ринках.

Існують випадки, коли впровадження системи ризик-менеджменту є обов'язковим. Сюди можна віднести стани, коли підприємство: знаходиться в пошуках зовнішнього фінансування; має намір поліпшення умов страхування; знаходиться в пошуках стратегічних партнерів в Україні або за кордоном; готується до виходу на фондовий ринок з метою IPO – розміщення акцій на біржі (Initial Public Offering) та коли керівництво підприємства поставило завдання зниження рівня втрат від операційних ризиків.

Система управління ризиками – сукупність необхідних елементів ефективної організації виявлення та управління ризиками підприємства. Вона включає принципи, процес, структуру, культуру і концепцію ризик-менеджменту.

При цьому, окремі стандарти ризик-менеджменту визначають важливість вищевказаних окремих елементів. Наприклад, згідно з австралійського і новозеландського стандарту елементами системи

управління ризиками є процес, структура і культура управління ризиками, в ISO – принципи, концепція і процес управління ризиками.

Принципи управління ризиками – особливі властивості системи управління ризиками, наявність яких формують ефективність останньої. Ними є створення оцінки, систематика, прозорість і інклюзивність, динамічність, прийняття до уваги людських і культурних чинників тощо.

Концепція ризик-менеджменту – набір компонентів, які надають основи і організаційні заходи для проєктування, впровадження, моніторингу, аналізу та постійного поліпшення ризик-менеджменту у всій організації. Мета даної концепції – формування допомоги організації в процесі інтеграції ризик-менеджменту в загальну систему управління компанії. Вона містить розгляд питань, пов’язаних із визначенням доручень і зобов’язань керівництва по ризик-менеджменту, розуміння організації і її контексту, визначення політики управління ризиками організації, особливостей інтеграції ризик-менеджменту в усі процеси діяльності та розгляд необхідних ресурсів для здійснення управління ризиками, встановлення внутрішніх комунікацій і звітного механізму, а також питання організації моніторингу і аналізу даної концепції.

Процес управління ризиками – сукупність етапів управління ризиками господарюючого суб’єкта, процес прийняття і виконання управлінських рішень, спрямованих на зниження ймовірності утворення несприятливих результатів і мінімізацію можливих втрат у діяльності організації.

Управління ризиком – складний і багаторівневий процес, який умовно можна розділити залежно від послідовності дій з управління ризиком на ряд етапів.

У табл. 2.2 наведено визначення складових процесу управління ризиками згідно різних національних і міжнародних стандартів цієї області.

Таблиця 2.2 – Складові процесу управління ризиками

Назва стандарту	Етапи процесу управління ризиками
Стандарт Австралії і Нової Зеландії 1995р.	5 стадій: 1) визначення оточення, 2) ідентифікація ризиків, 3) аналіз ризиків, 4) оцінка, 5) обробка ризиків. 2 процеси: 1) комунікація та консалтинг, 2) моніторинг та аналіз.
Стандарт управління ризиками орг. Інтегрована модель (COSO), США	8 етапів: 1) визначення внутрішнього середовища, 2) постановка цілей, 3) визначення ризикових подій, 4) оцінка ризику, 5) реагування на ризик, 6) засоби контролю, 7) інформація та комунікації, 8) моніторинг.
Стандарт по управлінню ризиками Федерації європейських асоціацій ризик-менеджерів (FERMA)	7 етапів: 1) визначення та розгляд стратегічних цілей організації, 2) оцінка ризиків (аналіз, кількісна та якісна оцінка ризиків), 3) формування звіту про ризики, 4) прийняття рішення, 5) визначення заходів щодо управління ризиками, 6) реалізація повторного звіту про ризики, 7) здійснення моніторингу.
Міжнародний стандарт ISO 31000: 2009	7 етапів: 1) реалізація комунікації та консультацій, 2) встановлення контексту, 3) ідентифікація ризиків, 4) аналіз ризиків, 5) визначення ступеня ризиків, 6) обробка ризиків, 7) моніторинг та аналіз.

Виділення таких етапів умовно, оскільки на практиці вони реалізуються одночасно. Для розуміння процедури управління ризиком слід проаналізувати кожен етап.

Етап 1. Ідентифікація і аналіз ризику. Даний етап необхідний для розуміння особливостей ризикової ситуації. Під ідентифікацією та аналізом

ризиків слід розуміти виявлення ризиків, їх специфіку, обумовлену природою і іншими характерними рисами ризиків, виділення особливостей їх реалізації, включаючи вивчення розміру економічного збитку, а також зміни ризиків у часі, ступінь взаємозв'язку між ними і вивчення факторів, що впливають на них. Без такого моніторингу ризику неможливе ефективне і цілеспрямоване управління.

Особливість першого етапу процедури управління ризиком пов'язана зі специфікою ризик-менеджменту, а також з його інформаційною основою. На даному етапі можливе отримання якісної інформації про наслідки ризикової ситуації і кількісної оцінки потенційного ризику і очікуваних наслідків його реалізації, які необхідні для прийняття управлінських рішень.

Однак, у процесі реалізації наступних етапів ризик-менеджменту інформаційна база про можливі ризикові події може доповнюватися і уточнюватися, тому на даному етапі дії неодноразові і являють собою постійний і безперервний процес збору і обробки інформаційних масивів.

Етап 2. Аналіз альтернативних підходів до управління ризиком. Ключова мета даного етапу міститься в моніторингу інструментів, що перешкоджають виникненню ризикової ситуації і впливу її негативних наслідків діяльність компанії. Дослідження основних методів, спрямованих на мінімізацію негативних подій і фінансових наслідків, дозволяє виявити загальні процедури управління ризиками. На даному етапі за допомогою пріоритизації виділяється вузький спектр потенційних небезпек, на яких керівництво фокусується і, першочергово, направляє свої дії по їх мінімізації або усунення.

Етап 3. Вибір методів управління ризиком. Методи управління ризиками різноманітні. Ними є страхування, різноманітні види диверсифікації, резервування коштів, стрес-тестінг, хеджування тощо. Даний етап необхідний для формування політики системи ризик-менеджменту. Необхідність цієї процедури пояснюється різною ефективністю методів управління ризиком і неоднаковим обсягом ресурсів для їх реалізації. Якщо

керівництво організації вибере неправильну технологію впливу та мінімізації ризику, він може зменшитися, але при цьому може спричинити за собою ще більш серйозні небезпеки в майбутньому.

При виборі методів управління ризиком можуть враховуватись різні критерії, у тому числі фінансово-економічні, спрямовані на забезпечення ефективності. Проте не варто зводити все методи боротьби з ризиком на отримання економічної віддачі. Важливо враховувати і такі критерії, як технічні, що відображають технологічні можливості зниження ризику, або соціальні, спрямовані на зниження ризику до рівня, прийнятного для суспільства. На даному етапі важливим аспектом в ухваленні рішень є те, що на підставі принципу ефективності системи управління ризиком інструменти повинні застосовуватися відповідним ризикам, у тому числі щодо тих ризиків, які тягнуть найбільш негативні наслідки.

Наприклад, в умовах обмеженості бюджету частина ризиків, які за суб'єктивною оцінкою менеджера є незначними, може ігноруватися. У подібній ситуації може виникнути різне ставлення до ризиків – активна або пасивна стратегія, що відображає додаткові особливості процедури ризик-менеджменту.

Програма управління ризиками являє собою сукупність методів, яка містить опис заходів з управління ризиком, а також їх інформаційне та ресурсне забезпечення, критерії результативності їх реалізації, систему розподілу відповідальності за прийняті рішення і ряд інших відомостей, без яких неможлива організація управління ризиковою ситуацією. Подібна програма є початком роботи в сфері ризик-менеджменту.

Після визначення методів складається звітність про ризики, яка містить карту ризиків, опис найбільш значущих ризиків, заходи щодо їх зниження, відповідальних і терміни їх реалізації. Цей документ в основному розробляється раз на півроку.

Етап 4. Виконання обраного методу управління ризиком. Даний етап передбачає виконання прийнятих рішень про реалізацію методів управління.

Це означає, що в рамках цього процесу приймаються і реалізуються приватні управлінські та технічні рішення.

Етап 5. Моніторинг результатів і вдосконалення. Оцінка і аналіз результатів і вдосконалення системи управління ризиком забезпечує зворотний зв'язок у системі ризик-менеджменту. Етап моніторингу результатів є важливим етапом, який забезпечує динамічний характер процесу управління, гнучкість і адаптивність. Важливою умовою оцінки та аналізу ризиків є оновлення та поповнення інформаційних масивів, що, у свою чергу, дає можливість приймати своєчасні та адекватні рішення. На основі цього реалізується оцінка результативності прийнятих заходів. Складність проведення такої оцінки полягає в тому, що за проаналізований період ризики можуть не реалізуватися, але компанія понесе витрати на програму управління ризиками. У зв'язку з цим слід зіставляти гіпотетичні втрати з реальними витратами.

Даному процесу повинні бути піддані: виявлені і розраховані оцінки ймовірності ризику, очікувана величина ризику, складені плани управління ризиками та наявні ресурси для управління ними, інші чинники, які можуть вплинути на значимість ризиків.

Мета оцінки результативності реалізованих заходів – адаптація системи ризик-менеджменту до зміни факторів зовнішнього та внутрішнього підприємницького середовища, які безпосередньо впливають на бізнес.

Алгоритм системи управління представлений на рис. 2.7.

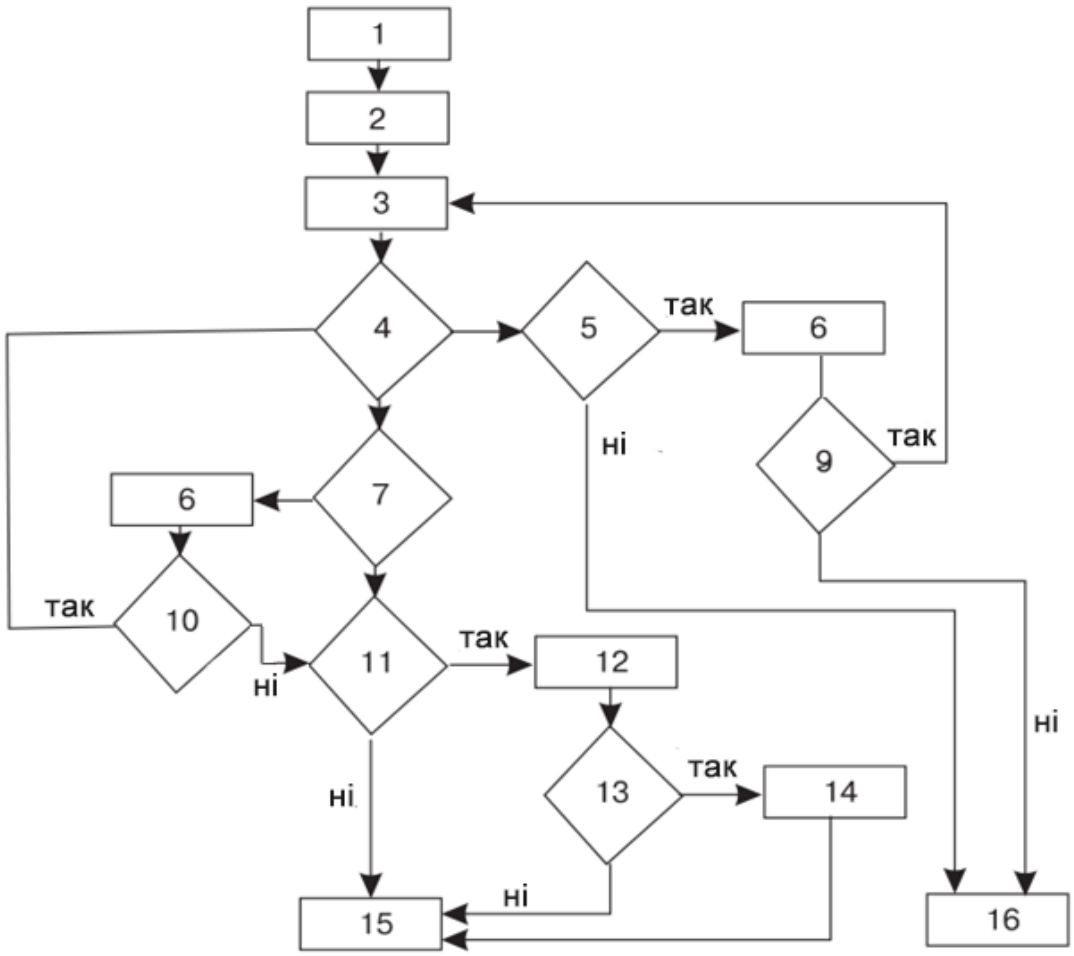


Рисунок 2.7 – Блок-схема процесу управління ризиком:
1 - збір і обробка даних; 2 - якісний аналіз ризику; 3 - кількісна оцінка ризику; 4 - оцінка прийнятності ризику; 5, 11 - оцінка можливості зниження ризику; 6, 12 - вибір методів і формування варіантів зниження ризику; 7 - оцінка можливості збільшення ризику; 8 - формування і вибір варіантів збільшення ризику; 9, 13 - оцінка доцільності зниження ризику; 10 - оцінка доцільності збільшення ризику; 14 - вибір варіанта зниження ризику; 15 - реалізація проєкту (прийняття ризику); 16 - відмова від реалізації проєкту (уникання ризику)

Організаційна структура управління ризиками – це схема організації і реалізації управління ризиками господарюючого суб’єкта, тобто визначення, хто буде здійснювати і відповідати за виявлення, оцінку, управлінський вплив над ризиковими подіями і моніторинг (тобто здійснювати управління ризиками в організації). При цьому, у різних організаціях залежно від цілей, виду діяльності, масштабів і загальної організаційної структури управління вона може бути без формування відділу ризик-менеджменту, з наявністю такого відділу або здійснення аутсорсингу даної функції.

Культура управління ризиками – це формування в організації такого середовища або атмосфери, які сприятимуть виявленню, оцінці і зниження ризиків, а також формуванню відкритої комунікації про ризики. Це середовище, при наявності якого всі співробітники компанії організації бажають брати участь у виявленні та управлінні ризиками і здійснюють у реальності ці заходи.

У системі управління ризиками організації будь-якої сфери діяльності важливу роль відіграє організаційна структура управління ризиками, тобто – хто здійснює і відповідає за цю функцію.

На практиці в сучасній ситуації існують три моделі організаційних структур управління ризиками.

Перша модель – в організації немає окремого підрозділу управління ризиками, тобто ризики виявляються різними функціональними службами, які передаються керівництву для розгляду і застосування різних заходів щодо їх зниження і усунення. Переваги даної моделі в її порівняній дешевизні, простоті реалізації і відсутності вимоги переформування загальної структури організації. Схематично дана модель наведена на рис. 2.8.

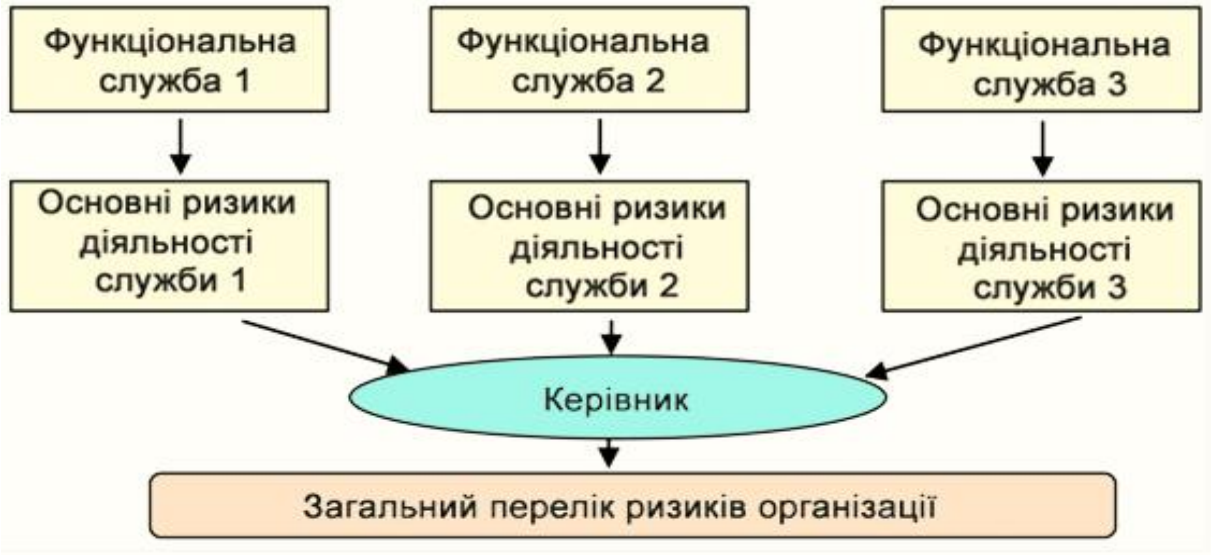


Рисунок 2.8 – Система ризик-менеджменту без формування відділу управління ризиками в організації

Під час розробки проєкту бізнес-плану кожна функціональна служба репрезентує свої ризики і представляє їх керівництву, яке збирає всю цю інформацію. Але оскільки керівництво перевантажене величезною кількістю як робіт, так і ризиків за різними проєктами, воно в реальності їх не аналізує і ними не займається. Для малої і середньої організації дана схема є можливою і зручною, але у великих господарюючих суб'єктах застосування даної структури буде неефективним і може ввести компанію в проблемну ситуацію, аж до її ліквідації.

Друга модель – формування відділу ризик-менеджменту в організації, який буде займатися всіма питаннями виявлення, оцінки та управління ризиками підприємства. Переваги даного варіанту очевидні – в організації питаннями визначення та управління ризиками займаються фахівці цієї сфери, а його недоліками є:

1) для формування нового відділу потрібно наймання додаткових співробітників, певне приміщення для відділу тощо, тобто – необхідне фінансування;

2) якщо це діюча організація, то утворюється необхідність реконструкції її загальної структури, оскільки виникає питання створення функціональної служби ризик-менеджменту.

Тут існують два підходи або моделі організаційних структур: розподільна і концентрована. У першому випадку управління ризиками реалізується підрозділами, в яких вони виникають, а невеликий спеціалізований відділ ризик-менеджменту здійснює моніторинг ризиків, розробляє політику і методику управління ризиками. У другому випадку управління ризиками зосереджено в рамках відокремленого підрозділу ризик-менеджмента.

Служба (відділ) ризик-менеджменту може бути організована таким чином:

- орієнтована на напрямки бізнесу, тобто за кожен напрямок відповідає окремий ризик-менеджер або фахівець з даної сфері;

- орієнтована на різні види ризиків, тобто окремі ризики управляються окремими ризик-менеджерами.

Мета формування даного відділу – виявлення різних ризиків, їх моніторинг і мінімізація наслідків. Для ефективної реалізації своєї функції важливо, щоб структурний підрозділ підпорядковувалося керівництву організації і був самостійним ланкою, а не підвідділом.

Важливим питанням тут також є визначення місця даної функціональної служби в загальній структурі організації, що залежить від сфери діяльності господарюючого суб'єкта та виду нею застосовуваної організаційної структури управління.

Так, залежно від виду структури (функціональна, лінійно-функціональна, дивізіональна, адаптивна тощо) місце даного підрозділу визначається по-різному. Наприклад, у функціональній структурі оптимальним варіантом може бути схема, наведена на рис. 2.9.

Рисунок 2.9 – Формування служби ризик-менеджменту в організації з функціональною структурою управління

Необхідно враховувати також специфіку діяльності організації, оскільки у фінансових, виробничих або венчурних господарюючих суб'єктах організація і реалізація управління ризиками буде відрізнятися.

Після формування і визначення місця даного відділу в загальній структурі необхідно сформулювати права та обов'язки, характер діяльності кожного співробітника даної функціональної служби.

Третя модель організації управління ризиками в господарюючих суб'єктах – аутсорсинг даної функції. Це передача реалізації цієї управлінської діяльності спеціалізованої організації за певну грошову суму. Часто такого роду послуги здійснюють страхові компанії, брокери, банки та інші фінансові організації.

Переваги аутсорсингу управління ризиком:

1) компанія звільняється від реалізації складних заходів ризик-менеджменту і необхідності найму високооплачуваних професіоналів;

2) здійснення певних заходів своїми силами може бути дорожче, тобто компанія економить на можливих витратах;

3) у компанії з'являється можливість сконцентруватися на основній діяльності;

4) придбання переваги від комплексного обслуговування, що містить як систему управління ризиком, так і інші послуги в області аутсорсингу (наприклад, обслуговування локальної мережі);

5) диверсифікація ризику забезпечує прийнятний рівень збитків.

Недоліком аутсорсингу є його зовнішній характер, через що передбачувані заходи будуть сприйматися чужим персоналом організації, що і знизить ефективність системи управління ризиками.

Необхідно також відзначити, що сьогодні актуальні такі структури, в яких об'єднані ризик-менеджмент і антикризове управління, тобто служба антикризового управління, прогнозуючи, виявляючи і визначаючи заходи щодо подолання кризових ситуацій в організації, не може це здійснювати без роботи з ризиками. При цьому, для визначення криз, у першу чергу, даний

відділ повинен виявити і ранжирувати ризики господарюючого суб'єкта. Так, багато сучасних організації саме тому формують інтегровану структуру управління ризиками і кризами.

Для додаткового контролю в організаціях можуть також створюватися комітети з ризик-менеджменту при раді директорів або інших органів вищого керівництва компанії, які здійснюють стратегічну функцію управління ризиками. Це актуально для великих організацій і господарюючих суб'єктів з проєктною системою управління.

2.2. Методи управління ризиками

Ефективність управління факторами ризику підприємства багато в чому залежить від того, які методи використовуються для реалізації намічених цілей.

У реальних ситуаціях, в умовах дії різноманітних чинників ризику можуть використовуватися конкретні способи зниження рівня ризику, що впливають на ті чи інші сторони діяльності суб'єкта господарювання. Різноманіття застосовуваних методів управління господарським ризиком у загальному вигляді можна розділити на чотири типи:

- методи ухилення від ризику:
    - відмова від ненадійних партнерів;
    - відмова від інноваційних проєктів;
    - страхування господарської діяльності;
    - створення регіональних або галузевих структур взаємного страхування і систем перестрахування;
    - пошук «гарантів»;
- методи локалізації ризику:
    - виділення «економічно небезпечних» ділянок у структурно або фінансово самостійні підрозділи (внутрішній венчур);
    - створення венчурних підприємств;

- послідовне розукрупнення підприємств;

- методи дисипації (розсіювання) ризику:
  - інтеграційний розподіл відповідальності між партнерами по виробництву (створення ФПГ – фінансово-промислових груп, акціонерних товариств, обмін акціями тощо);
  - випуск корпоративних облігацій;
  - синдикований кредит;
  - диверсифікація видів діяльності;
  - диверсифікація ринків збуту і зон господарювання (розширення кола партнерів-споживачів)
  - розширення закупівель сировини, матеріалів, комплектуючих тощо;
  - розподіл ризику за етапами роботи (за часом);
  - диверсифікація інвестиційного портфеля підприємства;
- методи компенсації ризику:
  - впровадження стратегічного планування;
  - прогнозування зовнішньої економічної обстановки в країні, регіоні господарювання;
  - моніторинг соціально-економічного та нормативно-правового середовища;
  - створення системи резервів на підприємстві;
  - активний цілеспрямований («агресивний») маркетинг;
  - створення спілок, асоціацій, фондів взаємовиручки і взаємної підтримки тощо;
  - лобіювання законопроєктів, що нейтралізують або компенсують передбачувані чинники ризику;
  - емісія конвертованих привілейованих акцій;
  - боротьба з промислово-економічним шпигунством.

Внутрішнім механізмам управління ризиками належить основна роль у системі ризик-менеджменту. Внутрішні механізми нейтралізації ризиків – це система методів, спрямованих на мінімізацію негативних результатів ризикової ситуації, що реалізуються на підприємстві.

Високий ступінь альтернативності прийнятих управлінських рішень, що не залежать від інших суб'єктів господарювання – основна перевага застосування внутрішніх механізмів нейтралізації ризиків. Внутрішні механізми нейтралізації ризиків ґрунтуються на певних умовах реалізації фінансово-господарської діяльності підприємства, що дозволяє найбільш точно визначити вплив внутрішніх чинників на рівень можливих ризиків у результаті мінімізації негативних наслідків ризикової ситуації.

Серед методів системи внутрішніх механізмів нейтралізації ризиків основними є ухилення від ризику, лімітування концентрації ризику, хеджування, диверсифікація, трансферт ризику, страхування, інші методи.

Методи ухилення від ризику найбільш поширені в господарській практиці. Цими методами користуються підприємці, які віддають перевагу діяти напевно, не ризикуючи. Керівники цього типу відмовляються від послуг ненадійних партнерів, прагнуть працювати тільки з контрагентами (споживачами і постачальниками), що переконливо підтвердили свою надійність – уникають брати участь у комерційних або виробничих проєктах, пов'язаних з необхідністю розширювати коло партнерів. Щоб уникнути ризику зриву виробничої програми через порушення графіків поставок сировини, матеріалів і комплектуючих, підприємства відмовляються від послуг сумнівних або невідомих постачальників. При цьому прагнення уникнути ризику буває настільки сильним, що можуть бути відкинуті навіть консервативні способи отримання більшого прибутку.

Відмова від реалізації нових бізнес-ідей, інноваційних проєктів при ринковій економіці призводить до втрати конкурентоспроможності, застою і банкрутства підприємства. Сучасний керівник повинен бути заповзятливим,

тобто здатним йти на ризик, приймати нові інноваційні проєкти та ідеї. Ухилення від ризику допомагає його уникнути, але не збільшує прибутки і не розвиває підприємство. Керівник підприємства або інвестор, надмірно страхуючи себе від втрат, уникає ризикових вкладень капіталу, випускаючи вигоду.

Рішення про ухилення від ризику може бути прийнято як на попередній стадії прийняття рішення, так і пізніше – шляхом відмови від подальшого здійснення фінансової операції.

Методи ухилення від ризику поширені в господарській практиці. До числа таких заходів відносяться:

- відмова від реалізації фінансових операцій з високим ступенем ризику. Пропонований метод має високу ефективність, але його застосування носить обмежений характер, оскільки фінансові операції пов'язані з виробничо-комерційною діяльністю підприємства, що забезпечує регулярне надходження доходів і формування його прибутку;

- відмова від продовження господарських відносин з партнерами, що систематично порушують контрактні зобов'язання. Розглянутий метод уникнення ризику є одним з поширених і ефективних. Систематичний аналіз стану виконання партнерами своїх зобов'язань, виявлення причин їх невиконання – необхідна умова ухилення від ризикової ситуації на підприємстві;

- відмова від використання у високих обсягах позикового капіталу. Зниження частки позикових коштів дозволить уникнути ризик втрати фінансової стійкості підприємства. Однак подібне ухилення від ризику передбачає упущення можливості отримання додаткового прибутку на вкладений капітал;

- відмова від надмірного використання оборотних активів у низьколіквідних формах. Ухилення від ризику неплатоспроможності підприємства можливо за допомогою підвищення рівня ліквідності оборотних активів. Такий метод позбавляє підприємство додаткових доходів

від розширення обсягів продажу продукції в кредит і породжує нові ризики, пов'язані з порушенням ритмічності операційного процесу через зниження розміру страхових запасів сировини, матеріалів, готової продукції;

- відмова від використання тимчасово вільних грошових активів у короткострокових фінансових інвестиціях. Даний метод дозволяє уникнути депозитний і процентний ризики, проте можливі втрати від інфляційного ризику і ризику упущеної вигоди.

Ухилення від перерахованих ризиків передбачає упущення можливості отримання додаткового прибутку, отже, робить негативний вплив на ефективність використання власного прибутку аж до від'ємних результатів.

Існує й інша можливість ухилення, яка полягає в спробі перенести ризик на будь-яку третю особу. З цією метою вдаються до страхування своїх дій або «пошуку гарантів», повністю перекладаючи на них свій ризик. Страхування ймовірних втрат служить не тільки надійним захистом від невдалих рішень, що само по собі дуже важливо, але також підвищує відповідальність керівників підприємств, примушуючи їх серйозніше ставитися до розробки і прийняття рішень, регулярно проводити превентивні захисні заходи відповідно до страхового контракту. У більш широкому плані підприємство може навіть виступити з ініціативою створення регіональної системи взаємного страхування фінансово-господарських операцій та відповідної системи перестрахування тощо.

Страхування – це угода, згідно з якою страховик (наприклад, будь-яка страхова компанія) за певну обумовлену винагороду (страхову премію) приймає на себе зобов'язання відшкодувати збитки або їх частину (страхову суму) страхувальнику (наприклад, господареві будь-якого об'єкта), що відбулися внаслідок передбачених у страховому договорі небезпек і (або) випадковостей (страховий випадок), яким піддається страхувальник або застраховане їм майно.

Зміст страхування проявляється в тому, щоб уникнути ризику; інвестор відмовляється від частини своїх доходів, таким чином він платить за

зниження рівня ризику і зменшення ймовірності отримання негативного результату. Страхування передбачає виплату страхового внеску чи премії з метою уникнути збитків.

Винятки – це втрати, які на перший погляд задовольняють умовам страхового контракту, але все ж їх відшкодування спеціально виключається. Межі – це кордони, що накладаються на розмір компенсації збитків, передбачених страховим договором. Франшиза – це сума грошей, яку застрахована сторона повинна виплатити з власних коштів, перш ніж отримати від страхової компанії яку б то не було компенсацію.

Страхування як метод управління ризиком забезпечує захист від можливих фінансових втрат, і дає страхувальникові можливість передати ризик втрат страховика на певних умовах. Страховий контракт включає деякі особливості:

- висновок щодо того, що інциденти, які призводять до втрат, відбулися: всі умови обумовлюються в страховому полісі;
- виплата страхового покриття або передача наслідків інциденту відбувається одразу після настання страхової події;
- передача тільки фінансових наслідків втрат. Страхувальник несе збитки в результаті виробничих процесів або втрат іншого капіталу до тих пір, поки фінансова компенсація не буде отримана.

Типовий страховий контракт передбачає виплати страхових сум тільки після того, як всі позови будуть пред’явлені і оформлені відповідним чином. У зв’язку з цим відзначимо, страхування – це короткостроковий механізм передачі ризику. У результаті, витрати на покриття втрат несе страхувальник, а не страховик. Страхування являє собою спосіб «згладжування втрат», який змушує організацію сплачувати свої втрати в довгостроковому масштабі і забезпечує захист при середніх і великих втратах за короткий період від фінансового провалу.

У рамках договору страхування страхові компанії представляють жорсткі вимоги до ризикових подій, які приймають на себе. Таким чином,

страхова компанія прагне піти від збитків і отримати прибуток. Страхова компанія бере на себе тільки частину ризиків, властивих діяльності компанії, яка відповідає таким вимогам:

- випадковий і непередбачуваний характер подій;
- вимірність ризику;
- обмеженість втрат;
- відносно невелика ймовірність настання страхового випадку.

Вимога випадковості і непередбачуваності подій виходить з самої природи ризику. Дотримання цієї умови для страхової компанії необхідно не стільки для самих подій, скільки для розміру збитків. Події, які можна спрогнозувати протягом року, є невигідним об'єктом страхування.

Вимірність ризику – можливість за допомогою теоретичних моделей і статистики розрахувати ймовірні характеристики ризику.

Обмеженість втрат – накладення певних умов на максимальний розмір збитків, що підлягають страхуванню.

Імовірність настання страхового випадку не повинна бути занадто великою з двох причин. По-перше, частота настання страхових випадків схильна флуктуацій щодо середніх величин, тому страхова компанія може понести максимальні збитки. По-друге, висока ймовірність настання страхової події передбачає, що страхувальник повинен сплатити значну частину страхової премії, яка становить 20-30 % страхової суми. Кожен вид страхування передбачає певні ризики, прийняті на страхування. Набір ризиків обмежений і не враховує всі можливі страхові випадки. Наприклад, зі страхування фінансових і інвестиційних ризиків виключаються форс-мажорні обставини.

У результаті страхування страхувальник набуває такі вигоди: відшкодування збитків у випадку настання ризикової події; зниження невизначеності; отримання грошових коштів для більш ефективного використання; отримання консультаційної допомоги ризик-менеджерів, що забезпечується страховою компанією.

Страхування виступає гарантованим джерелом грошових коштів у випадку настання ризикової події. Страхування мінімізує вплив втрат на працездатність компанії. Грошові кошти, що виплачуються страховиком, пом'якшують вплив втрат у період відновлення виробництва на продовження діяльності і прибутковість підприємства.

Основною властивістю страхування є заміна невідомих витрат на певні витрати на страхову премію, оскільки страхування відзначає, що всі ризики інтегруються, що дозволяє страховику обробляти більший масив даних, на відміну від індивідуального страхувальника. Фактично, передбачуваність закону великих чисел знижує сукупний рівень невизначеностей. Виграш окремого страхувальника забезпечується тим, що у випадку страхування для нього ризик несподіваних збитків у будь-якому році не тільки замінюється меншим ризиком, але ще і обмежується сумою страхових внесків.

Однією зі специфічних форм страхування майнових інтересів є хеджування, яке представляє систему заходів, що дозволяють виключити або обмежити ризик фінансових операцій у результаті несприятливих змін курсу валют, цін на товари, процентних ставок у майбутньому. Такими заходами є: валютні застереження, форвардні операції, опціони тощо.

Хеджування – це процес зменшення ризику можливих втрат. Компанія може прийняти рішення хеджувати всі ризики, не хеджувати нічого або хеджувати що-небудь вибірково. Вона також може спекулювати, будь то свідомо чи ні.

Про хеджування ризику говорять у тих випадках, коли дія, яку виконують для зниження ризику зазнати збитків, одночасно призводить і до неможливості отримати дохід.

Відсутність хеджування може мати дві причини. По-перше, компанія може не знати про ризики або можливості зменшення цих ризиків. По-друге, вона може вважати, що обмінні курси або процентні ставки будуть залишатися незмінними або змінюватися в її користь. У результаті компанія буде спекулювати: якщо її очікування виявляться правильними, вона виграє,

якщо ні – вона понесе збитки. Хеджування всіх ризиків – єдиний спосіб їх повністю уникнути. Однак фінансові директори багатьох компаній віддають перевагу вибірковому хеджуванню. Якщо вони вважають, що курси валют або відсоткові ставки зміняться несприятливо для них, то вони хеджують ризик, а якщо рух буде на їхню користь – залишають ризик непокритим. Це і є, по суті, спекуляція.

Одним із недоліків загального хеджування (тобто зменшення всіх ризиків) є досить істотні сумарні витрати на комісійні брокерам і премії опціонів. Вибіркове хеджування можна розглядати як один із способів зниження загальних витрат. Інший спосіб – страхувати ризики тільки після того, як курси або ставки змінилися до визначеного рівня. Можна вважати, що в якійсь мірі компанія може витримати несприятливі зміни, але коли вони досягнуть припустимої межі, позицію слід повністю хеджувати для запобігання подальших збитків. Такий підхід дозволяє уникнути витрат на страхування ризиків у ситуаціях, коли обмінні курси або процентні ставки залишаються стабільними або змінюються в сприятливому напрямку.

Опціони – поширена форма страхового договору. Опціон являє собою право щось купити або продати за фіксованою ціною в майбутньому. Форвардний контракт відрізняється від опціону тим, що він передбачає зобов'язання купити (продати) за фіксованою ціною в майбутньому що-небудь.

Існує стільки ж видів опціонних контрактів, скільки існує предметів купівлі-продажу: товарний опціон, опціон на акції, опціон на процентні ставки, валютний опціон тощо.

Хеджування за допомогою опціонів передбачає право, а не обов'язок страхувальника за опціонну премію купити заздалегідь обумовлену кількість валюти за фіксованим курсом в узгоджений термін. У даному випадку вартість опціону або опціонна премія є аналогом страхового внеску.

Опціон дозволяє його покупцю встановити мінімум або максимум ціни, що його цікавить. Його ризик обмежений сплаченою ним премією, у той час як ризика продавця опціону щодо зміни ціни – потенційно немає.

Опціон несе такі вигоди для покупця: обмежений ризик (сума премії), контроль над великими обсягами товару при обмежених коштах, можливість встановити максимальну ціну в очікуванні покупки або мінімальну в очікуванні продажу, можливість застосування різноманітних стратегій хеджування. Вигоди продавців опціонів – підвищений дохід і збільшення потоків грошових коштів.

Залежно від цілей хеджування застосовують такі коефіцієнти ефективності хеджування.

Мета перша: отримати прогнозований фінансовий результат: більше – краще, менше – гірше. Це властиво багатьом ситуацій з хеджуванням. Кінцевим результатом можуть бути очікувані фінансові надходження або ставка інвестування. Ефективність хеджування розраховується як частка від ділення дійсного фінансового результату на очікуваний.

Мета друга: домогтися прогнозованого фінансового результату: менше – краще, більше – гірше. Тут ризик характеризується протилежною спрямованістю. У цьому випадку ефективність хеджування визначається як частка від ділення очікуваного фінансового результату на дійсний.

Мета третя: отримати очікуваний фінансовий результат з обмеженням на мінімально прийнятний результат. У цьому випадку встановлюється мінімально прийнятний результат.

Мета четверта: отримати прогнозований фінансовий підсумок з обмеженням на максимально прийнятний результат.

Мета п’ята: зберегти статус-кво. У даному випадку будь-яке відхилення від поточної ситуації вважається небажаним.

Варто зазначити, що такий популярний механізм ухилення від ризику, як страхування, незастосовний в багатьох ситуаціях, з якими стикаються промислові підприємства, особливо в сучасній дійсності, де не слабшають

інфляційні процеси і де немає достатньої і надійної страхової статистики. Перш за все, це характерно для підприємств, які освоюють нові види продукції або нові технології, оскільки для таких випадків страхові компанії ще не мають у своєму розпорядженні статистичними даними, необхідними для проведення розрахунків, які обґрунтовують розміри страхових премій і внесків, і тому не страхують ці види ризиків. Тому вибір дій для зниження ризику слід починати зі з'ясування, чи є даний фактор ризику предметом страхування чи ні.

Зниження ймовірності отримання втрат внаслідок настання ризикової ситуації можливе за допомогою резервування коштів, яке передбачає, що підприємець формує відокремлені фонди відшкодування збитків у випадку несприятливого результату за рахунок частини власних оборотних коштів. Внутрішній фонд носить назву «фонд ризику». Резервування коштів на покриття збитків називають самострахуванням, яке необхідно, якщо:

- від його використання в порівнянні з іншими методами управління ризиком очевидна економічна вигода;

- у рамках інших методів управління ризиком немає можливості забезпечити необхідну зниження або покриття ризиків підприємства. Перша ситуація може виникнути, якщо внаслідок аналізу ринка страхування з'ясовується, що розмір страхової премії є занадто великим. Реалізація запобіжних заходів при великих витратах приносить мінімальний ефект.

Друга ситуація можлива, якщо ризики підприємства досить великі і покрити їх повністю в рамках окремої страхової компанії або компаній дуже складно.

Важливою особливістю методу резервування коштів у системі заходів зниження ризику є необхідний у кожному індивідуальному випадку обсяг запасів. У зв'язку з цим важливо встановити оптимальний обсяг запасів для мінімізації ризику.

Однак не виключені непередбачені ризики, наслідки від яких відшкодовуються будь-якими наявними засобами. Для таких випадків формується страховий резервний фонд.

Страховий резервний фонд не приносить прибутку і виключається з обороту. Визначити оптимальний рівень таких фондів видається складним, тому що єдиний загальноприйнятий критерій не встановлено.

Створення резервного фонду обов'язкове для акціонерного товариства, кооперативу, підприємства з іноземними інвестиціями, його розмір повинен бути не менше 10 % і не більше 25 % від статутного капіталу. Джерело відшкодування втрат від настання ризикової ситуації – це прибуток. При створенні фондів – це накопичений прибуток, у випадку відсутності таких фондів і настання ризику – недоотриманий прибуток.

Головною проблемою при формуванні резерву на можливі витрати при непередбачених ситуаціях є оцінка несприятливих наслідків ризиків. Для встановлення початкових сум на покриття непередбачених витрат, їх переоцінки в результаті реалізації проєкту та уточнення сум резерву на основі фактичних даних застосовуються методи якісного і кількісного аналізу ризику.

Формування структури резерву на покриття витрат при непередбачених ситуаціях реалізується на базі одного з двох підходів. При першому – резерв ділиться на дві частини: загальний і спеціальний. Загальний резерв застосовується для покриття змін у кошторисі. Спеціальний резерв містить надбавки на покриття зростання цін, збільшення витрат по окремих позиціях і на оплату позовів по контрактах. Другий підхід заснований на визначенні непередбачених витрат за видами витрат: на заробітну плату, матеріали, субконтракти. Диференціація дозволяє визначити величину ризику, пов'язаного з кожною категорією витрат, які можна розподілити на деякі етапи реалізації проєкту.

Перевагою самострахування є:

- економія на страхових преміях, що дозволяє зменшити витрати і збільшити прибуток;

- отримання додаткового доходу на капітал при відмові від сплати страхових премій за рахунок інвестування збережених засобів;

- економія за рахунок більш ретельного аналізу минулих збитків.

З точки зору ефективності управління самострахування також має певні переваги, які пов'язані з підвищенням гнучкості управління ризиком, збереженням контролю над коштами і за якістю додаткового сервісу.

Недоліком самострахування є додаткові організаційні витрати, неправильне визначення рівня потенційного ризику, вплив інфляції на фонд ризику.

Методи локалізації ризику використовуються в тому випадку, якщо вдається досить чітко і конкретно визначити профіль ризику та ідентифікувати його джерела. Виділивши економічно найбільш небезпечну ділянку або етап діяльності, він стає більш контрольованим і таким чином знижується фінальний рівень ризику підприємства. Для реальних високоризикових проєктів створюються дочірні, венчурні підприємства. Найбільш ризикова частина проєкту локалізується в межах новоствореної і порівняно невеликій автономній компанії. У менш складних випадках замість самостійної юридичної особи утворюються спеціальні підрозділи, наприклад, з виділеним урахуванням по балансу.

Подібні методи набули поширення у великих виробничих компаніях промислово розвинених країн при впровадженні інноваційних проєктів, освоєнні нових видів продукції, комерційний успіх яких викликає великі сумніви.

Методи дисипації ризику – більш гнучкий інструмент управління. У цьому випадку підприємство прагне зменшити рівень власного ризику,

залучаючи до вирішення загальних проблем в якості партнерів інші підприємства та фізичні особи. Для цього можуть створюватися акціонерні товариства, фінансово-промислові групи; підприємства можуть придбавати акції один одного або обмінюватися ними, вступати в різні консорціуми, асоціації, концерни. Інтеграція може бути або вертикальною (діагональною) – об'єднання декількох підприємств одного підпорядкування або однієї галузі для проведення узгодженої цінової політики, поділу зон господарювання тощо, або горизонтальною – по послідовності технологічних переділів, операцій постачання і збуту. При цьому досягається додатковий ефект, який полягає в тому, що на входах і виходах підприємства створюються острівці передбачуваного товарного ринку, надійного довгострокового попиту і таких же постачань виробів, необхідних для виробництва продукції. У деяких випадках буває можливим розподіл загального ризику за часом або по етапах реалізації деякого довгострокового проєкту або стратегічного рішення.

До дисипативних методів управління ризиком відносяться також різні варіанти диверсифікації:

- диверсифікація діяльності – збільшення числа використовуваних або готових до використання технологій, розширення асортименту продукції, що випускається, або спектру послуг, що надаються, орієнтація на різні групи споживачів тощо;

- диверсифікація ринку збуту – робота одночасно на декількох товарних ринках, розподіл поставок між багатьма споживачами, при цьому бажано прагнути до рівномірного розподілу часток кожного контрагента в загальному обсязі випуску, щоб відмова кількох з них не зірвала виробничо-збутову програму в цілому;

- диверсифікація закупівлі сировини і матеріалів припускає взаємодію з багатьма постачальниками, дозволяючи послабити залежність підприємства від окремих ненадійних постачальників сировини, матеріалів і комплектуючих; при порушенні контрагентом графіка поставок по самим

різним, у тому числі і об’єктивним причинам (аварії, банкрутство, форс-мажорні обставини тощо), підприємство зможе безболісно перейти на роботу з іншим постачальником того ж або аналогічного субпродукту.

Природно, такі методи пом’якшення наслідків ризику ускладнюють роботу відділів матеріально-технічного постачання і збуту і, швидше за все, викликатимуть їх явний або прихований опір. Саме тому керівництво підприємства, використовуючи методи дисипації ризику з метою підтримки своєї економічної стійкості, має систематично контролювати такі показники, як кількість партнерів і їх частку в загальному обсязі закупівель і постачань даного підприємства, стимулюючи постійне розширення кола партнерів і рівномірність розподілу обсягів матеріальних потоків між ними і підприємством.

Диверсифікація інвестиційного портфеля підприємства має на увазі віддання переваги програмам реалізації кількох проєктів відносно невеликої капіталомісткості перед програмами, що складаються з єдиного інвестиційного проєкту, який, поглинувши практично всі резерви підприємства, не залишить можливостей для маневру.

Аналогічні диверсифікаційні прийоми зниження ризику можливі і стосовно інших напрямків діяльності або елементів стратегії підприємства.

Таким чином, механізм диверсифікації вибірково впливає на зменшення негативних результатів окремих ризикових ситуацій. Наприклад, отримання інвестором акцій п’яти різних акціонерних товариств замість акцій одного товариства збільшує можливість отримання їм середнього доходу в п’ять разів і, відповідно, у п’ять разів зменшує рівень ризику. Диверсифікація є більш аргументованим і порівняно найменш витратним методом зменшення рівня економічного ризику. Застосування механізму диверсифікації носить обмежений характер, тому що він неефективний у нейтралізації систематичних ризиків, але дає безсумнівний ефект у нейтралізації комплексних фінансових ризиків несистематичної групи.

Методи компенсації ризику використовуються на підприємствах, що здійснюють стратегічне планування. Ефективні в тому випадку, якщо процес розробки стратегії пронизує буквально всі сфери діяльності підприємства. Дозволяють знайти вузькі місця у виробничому циклі, розкрити джерела ослаблення ринкових позицій підприємства в своєму секторі ринку і в підсумку раніше ідентифікувати специфічний профіль факторів ризику даного підприємства в стратегічній перспективі. Розроблений на основі вивчення потенціалу стратегічний план буде, природно, включати комплекс компенсуючих заходів, план використання і підключення резервів тощо.

Різновидом цього методу можна вважати метод прогнозування зовнішньої економічної обстановки. Суть цього методу полягає в періодичній розробці сценаріїв розвитку і оцінки майбутнього стану середовища господарювання підприємства, у прогнозуванні поведінки партнерів і конкурентів, зміни в секторах і сегментах ринку, на яких працює дане підприємство, і, нарешті, у регіональному та загальноекономічному прогнозуванні.

Зрозуміло, ці прогнози немислимі без відстеження поточної інформації про відповідні процеси. Існує ще один важливий і ефективний метод – моніторинг соціально-економічного та нормативно-правового середовища. Реалізується цей метод компенсації ризику шляхом придбання актуалізованих комп’ютерних систем нормативно-довідкової інформації та підключення до мереж комерційної інформації, проведення власних прогнозно-аналітичних досліджень, замовлення відповідних послуг консультаційних компаній і окремих консультантів. Отримані в результаті дані дозволяють уловити нові тенденції у взаєминах господарюючих суб’єктів, завчасно підготуватися до нормативних нововведень, передбачити необхідні заходи для компенсації втрат від зміни правил ведення господарської діяльності, швидко і своєчасно скоригувати тактичні і стратегічні плани підприємства.

Метод створення системи резервів дуже близький до страхування, але зосереджений всередині підприємства. На підприємстві створюються резерви запасів сировини, матеріалів і комплектуючих, резервних фондів грошових коштів, формуються плани їх розгортання в кризових ситуаціях, вільні потужності, які не задіються, встановлюються як би про запас, створюються нові контакти і зв'язки.

Треба відзначити, що при відносно низькому рівні інфляції надається явна перевага фінансовим резервам, які можуть виступати у формі накопичення власних грошових страхових фондів, підготовки «гарячих» кредитних ліній на випадок непередбачених витрат, використання застав тощо. Отже, для підприємства актуальними стають завдання вироблення фінансової стратегії, політики управління своїми активами і пасивами, організація їх оптимальної структури і забезпечення достатньої ліквідності вкладених коштів.

У планах розгортання резервів повинно бути задіяно використання резервів внутрішнього середовища підприємства, можливостей його самовдосконалення – від навчання і тренінгу персоналу відповідно до його схильності до ризику до вироблення специфічної корпоративної культури. Керівники підприємств повинні з'ясувати власний психологічний тип і, якщо він не відповідає вимогам роботи в умовах невизначеності і ризику, постаратися змінити його. Для цього є апробовані методики і підходи, є і компанії, що спеціалізуються на вирішенні такого роду завдань. Якщо керівник змінює ставлення до ризику, то вже одне це може стати фактором вивільнення внутрішніх ресурсів керівного (та й не тільки) персоналу, що підвищує успішність підприємства.

Метод активного цілеспрямованого маркетингу полягає у формуванні інтенсивного споживчого попиту на свою продукцію, використовуючи різні маркетингові прийоми і методи: сегментація ринку, оцінка ємності ринку, організація рекламних компаній, включаючи всебічне інформування потенційних споживачів і інвесторів про найбільш сприятливих властивості

продукції і підприємства в цілому, аналіз поведінки конкурентів, вироблення стратегії конкурентної боротьби, розробка політики і заходів управління витратами тощо.

Одними з прикладів компенсаційної антиризикової поведінки підприємств, що забезпечує захист економічних інтересів шляхом запобігання витоку інформації і роботи з персоналом, є способи боротьби з різними проявами промислово-економічного шпигунства. Як показують дослідження, витік конфіденційної для даного підприємства інформації відбувається в основному через персонал. Тому поширені такі прийоми:

- надання інформації статусу комерційної таємниці;

- ведення спеціального обмежувального діловодства.

Важливим напрямком нейтралізації фінансових ризиків є лімітування їх концентрації. Механізм лімітування концентрації фінансових ризиків використовується зазвичай за тими їх видами, які виходять за межі допустимого їх рівня, тобто за фінансовими операціями, які здійснюються в зоні критичного чи катастрофічного ризику. Таке лімітування реалізується шляхом встановлення на підприємстві відповідних внутрішніх фінансових нормативів у процесі розробки політики здійснення різних аспектів фінансової діяльності.

Система фінансових нормативів, що забезпечують лімітування концентрації ризиків, може містити:

- граничний розмір позикових коштів, що використовуються в господарській діяльності. Цей ліміт встановлюється окремо для операційної та інвестиційної діяльності підприємства, а в ряді випадків – і для окремих фінансових операцій (фінансування реального інвестиційного проєкту; фінансування формування оборотних активів тощо);

- мінімальний розмір активів у високоліквідній формі. Цей ліміт забезпечує формування так званої ліквідної подушки, що характеризує розмір резервування високоліквідних активів з метою майбутнього погашення невідкладних фінансових зобов’язань підприємства;

- максимальний розмір товарного (комерційного) або споживчого кредиту, наданого одному покупцеві. Розмір кредитного ліміту, направлений на зниження концентрації кредитного ризику, встановлюється при формуванні політики надання товарного кредиту покупцям продукції;

- максимальний розмір депозитного вкладу, що розміщується в одному банку. Лімітування концентрації депозитного ризику в цій формі здійснюється в процесі використання даного фінансового інструменту інвестування капіталу підприємства;

- максимальний розмір вкладення коштів у цінні папери одного емітента. Ця форма лімітування направлена на зниження концентрації несистематичного (специфічного) фінансового ризику при формуванні портфеля цінних паперів;

- максимальний період відволікання коштів у дебіторську заборгованість. За рахунок цього фінансового нормативу забезпечується лімітування ризику неплатоспроможності, інфляційного ризику, а також кредитного ризику.

Лімітування концентрації фінансових ризиків є одним з найбільш поширених внутрішніх механізмів ризик-менеджменту, що реалізують фінансову ідеологію підприємства в частині прийняття цих ризиків і не вимагають високих витрат.

Сучасні розвинені організації використовують різноманітні способи і методи управління ризиками, найбільш популярними і вживаними є хеджування за допомогою деривативів, скоринг, математичний метод VaR, стрес-тестінг тощо.

Як було вказано раніше, хеджування – зниження ризику втрат шляхом включення в портфель фінансових інструментів (деривативів), зміна вартості яких протилежно зміни вартості основних активів портфеля. Хеджування використовується для того, щоб обмежити втрати при несприятливому розвитку ситуації. При цьому зниження ризику портфеля досягається за рахунок часткового зниження його очікуваної прибутковості. Деривативи –

це похідні інструменти, що дозволяють відокремити ризик, притаманний конкретному інструменту, і перенести даний ризик від продавця ризику («набувача захисту») до покупця ризику («продавцеві захисту»). Гарантії, синдиковані позики, опціони на активи і страхування ризиків не є деривативами.

Традиційні похідні інструменти зосереджені на ринкових факторах ризику, таких як курси валют, ціни, індекси або процентні ставки. Залежно від типу інструменту вони поділяються на дві великі групи:

- позабалансові інструменти або деривативи: форварди, свопи, опціони і індексні інструменти;

- інструменти, які обліковуються на балансі і є балансовими аналогами і замінниками деривативів: ноти і сек'юрітізовані активи.

Іншим методом оцінки і управління ризиком є автоматизовані системи скорингу, які застосовується в банківській справі для управління кредитними ризиками.

Скоринг – математична або статистична модель, в основі розрахунків якої лежить інформація «минулих» клієнтів банку і на основі цих історичних даних банк визначає ймовірність повернення кредиту певним потенційним позичальником у термін. Основне завдання скорингу – з'ясування можливостей клієнта виплачувати взятий кредит, а також ступеня надійності і обов'язковості клієнта.

У самому спрощеному вигляді скорингова модель – це зважена сума певних параметрів-характеристик потенційного позичальника. Оцінюючи ці параметри-характеристики, формується інтегральний показник (score). При цьому, чим даний показник вище, тим вище вважається кредитоспроможність і надійність потенційного позичальника. У банку також розраховується лінія беззбитковості, яка визначається відношенням середньої кількості позичальників, що платять у термін, за допомогою яких можна покрити або компенсувати збитки від одного проблемного клієнта-боржника. Розрахований інтегральний показник кожного клієнта

порівнюється з цією лінією беззбитковості. Якщо score вище порогової лінії, то кредит даному клієнту видається банком, а якщо нижче – то ні. Для визначення інтегрального показника часто банки використовують такі параметри-характеристики позичальника як: вік, спеціалізація, дохід, кількість дітей, кількість років роботи на даному місці, кількість років перебування клієнтом даного банку тощо.

Сутність скорингу не в пошуку пояснень, чому ця людина не платить свій кредит, а в тому, наскільки даний клієнт надійний.

Стрес-тестінг – наступний важливий сучасний метод управління ризиками, який досліджує, яким чином на вартість торгового портфеля впливають окремі стресові фактори і на їх основі сформовані сценарії розвитку подій, тобто сутність даної методики у визначенні ситуацій та факторів, що призводять до збитків або втрат і негативному впливу на фінансовий стан організації.

Стрес-тестінг більше застосовується в банківському секторі, хоча великі компанії також застосовують даний метод для аналізу своїх ризиків.

Процес стрес-тестінгу можна уявити як сукупність таких заходів:

- виявлення основних можливих факторів ризику;
- створення сценарію, тобто узгодження множини факторів ризику;
- розрахунок потенційних збитків через появу цієї негативної ситуації;
- аналіз проблемних сторін, активів, портфелів тощо.

При цьому, даний інструмент повинен включати всі значущі для організації ризики і напрямки діяльності, а також враховувати ситуації і умови, що призводять до максимальних збитків.

Іншим методом управління ризиком є показник вартості під ризиком (VaR), що відображає максимально можливі збитки від зміни вартості фінансового інструменту, портфеля активів, які можуть статися за цей період часу із заданою ймовірністю його появи. Тобто ризикова вартість – це розмір збитку, який може бути перевищений з імовірністю не більше x % (не буде перевищений з імовірністю (100 - x) %) протягом наступних n днів.

Метод VaR дозволяє виявити розподіл фінансових втрат по портфелю ризиків, на базі якого розрахувати передбачуваний збиток по портфелю при будь-якому заданому рівні довіри (довірчому інтервалі), мінливість обсягу даних втрат і кількості капіталу, потрібного для забезпечення портфеля.

Існує три основні методи розрахунку VaR: метод історичного моделювання, статистичних випробувань Монте-Карло і аналітичний (коваріаційний, дельта-нормальний).

Метод історичного моделювання (historical simulation) заснований на застосуванні історичних даних щодо змін факторів ризику для отримання розподілу майбутніх коливань вартості портфеля. На основі даних щодо змін факторів ризику і їх поточних значень відбувається повне переоцінювання портфеля, і для кожного сценарію обчислюється гіпотетичне значення прибутку або збитку портфеля. Після чого будується емпіричний розподіл ймовірностей прибутковості портфеля і по ньому визначається величина VaR із заданою ймовірністю.

Даний метод у порівнянні з аналітичним простіший під час розрахунків, оскільки в його основі немає теорії ймовірності, і він вимагає невеликої кількості припущень щодо статистичних розподілів для факторів ризику. Цей метод також не найточніший, тому що допускає, що минула ринкова ситуація буде повторюватися і в майбутньому, що в реальності не відповідає дійсності.

Метод статистичних випробувань Монте-Карло (Monte-Carlo simulation) аналогічний методу історичного моделювання. Відмінність полягає в тому, що зміни факторів ризику генеруються псевдовипадковим чином. По заданому розподілу за допомогою генератора випадкових чисел імітуються зміни факторів ризику. При цьому число сценаріїв має бути досить великим. Отримані значення використовуються для обчислення гіпотетичної прибутковості портфеля. За їх розподілом обчислюється величина VaR із заданою ймовірністю.

Метод Монте-Карло є найскладнішим методом визначення VaR, але його точність значно вище, ніж в інших методик розрахунку VaR.

Аналітичний (дельта-нормальний, коваріаційний) метод заснований на припущенні про нормальний розподіл змін факторів ринкового ризику і лінійність залежності прибутковості портфеля від зміни цих чинників. Таким чином, прибутковість портфеля також матиме нормальний розподіл. Виходячи з властивостей нормального розподілу, обчислюється величина VaR із заданою ймовірністю.

Метод сек'юрітізації – це продаж (передача) активів (ризику) організацією зі свого портфеля за допомогою випуску під них цінних паперів, підкріплених очікуваним надходженням готівкових платежів по цим займам.

Таким чином, на практиці існують різноманітні методики управління ризиками різних діяльностей і сфер в організації, і кожна організація повинна сама визначити, який із цих методів більше відповідає її реальності і ризикам, і ефективніше знизить втрати від ризиків.

2.3. Програма управління ризиками в організації

Програма управління ризиками на підприємстві повинна визначати, як здійснюється робота з управління ризиками в превентивної діяльності та постфактум, коли небажана подія вже відбулася, тобто повинні працювати спеціальні ситуаційні програми управління кризами.

Програма управління ризиками повинна відображати різні аспекти управління ризиками:

- види факторів ризиків, у тому числі найбільш актуальні;
- ступінь ризику;
- очікувані втрати або вигоди;
- заходи з управління ризиками;
- бюджети;
- джерела фінансування;

- терміни реалізації;

- відповідальні особи.

Етапи розробки програми управління ризиками:

1) на основі теоретичного узагальненого ризикового спектра підприємництва, галузевих особливостей розробляється класифікація ризиків, проводиться оцінка факторів ризику, здійснюється вибір методів управління факторами ризику, розробляється ризиковий профіль підприємства;

2) виділяються актуальні фактори ризику, які вже призвели до втрат і появі упущеної вигоди;

3) підрахунок підсумків за ризиками, що ввійшли в програму, і їх кількісна оцінка. Підведення підсумків за видами ризиків, побудова загального ризикового профілю організації, розрахунок усередненої напруженості сукупності ризиків. Цей аспект корисний для оцінки ситуації в цілому. Підрахувати усереднені показники напруженості ризиків по підприємству в цілому можна за допомогою методу експертної оцінки або іншими способами;

4) проводяться розрахунки можливих втрат або вигоди;

5) розробляються плани заходів по кожному конкретному фактору ризику. У ці плани слід включати заходи по всіх значущих чинникам ризику, та по іншим чинникам за принципом необхідної достатності, ґрунтуючись на тому, що, з одного боку, ресурси підприємства обмежені, з іншого боку – потрібно забезпечити досить надійну систему управління ризиками. При нестачі фінансових ресурсів саме цю частину програми можна коригувати, виключаючи другорядні заходи. У випадку необхідності, файли з цими іноді досить об’ємними матеріалами підключаються до моделі на гіперпосиланнях;

6) розробляються бюджети, необхідні для здійснення заходів відповідно до розробленого плану. Повні файли бюджетів підключаються до моделі на гіперпосиланнях;

7) формується зведений бюджет шляхом підсумовування конкретних бюджетів по окремих заходах;

8) складається зведений план заходів з управління ризиками. При цьому слід врахувати можливість об'єднання однотипних заходів для різних підрозділів в єдині заходи і компанії для всього підприємства. Після цього етапу будуть зібрані всі необхідні дані для проєктування схеми фінансування зведеного плану заходів;

9) оцінюються можливості фінансування кожного фактора ризику, визначаються джерела фінансування. Вони такі ж, як у будь-якого іншого ділового проєкту. Ризики можуть фінансуватися з власних, додатково інвестованих коштів власників, з позикових джерел, за рахунок продажу фінансових інструментів, акціонерного капіталу, з нерозподіленого прибутку і з потенційною розрахункової економії, яку принесе ефективний ризик-менеджмент як центр прибутку;

10) аналізуються можливості фінансування, проводиться співставлення з розробленим планом і бюджетом. Якщо фінансування значно перевершує доступне, то слід кардинально переглянути прийнятий підхід до управління ризиками. Нижньою межею переліку факторів ризику, які потрібно залишити в програмі, є актуальні, значущі втрати і упущена вигода. Занадто великі витрати, необхідні для їх реалізації, можуть бути симптомом нереалістичної управлінської стратегії. Якщо фінансових ресурсів виявиться істотно менше інтуїтивно очікуваних, то слід проаналізувати ситуацію: або є помилка в оцінці факторів ризику, або є шанс наперед знизити ризики в порівнянні з додатковими витратами на управління ризиками;

11) аналізуються можливості формування інтегральної (загальної для всієї сукупності ризиків) системи захисту від передбачуваних на розглянутий період ризиків. Цей етап знову повертає ризик-менеджера до аналізу взаємозв'язку ризиків між собою, до ранжирування ризиків, до аналізу нелінійної залежності результатів управління ризиками з урахуванням різних стадій життя підприємства;

12) коригується програма фінансування щодо можливості реалізації заходів і необхідності витрат. Після того як чергова спроба призведе до прийнятної конфігурації програми управління ризиками, можна перейти до наступних кроків;

13) готуються декларації, контракти, кредитні угоди, графіки, накази та інші організаційно-розпорядчі, рекламні, агітаційні, наочні, інструктивні документи та інші матеріали, які повинні забезпечити виконання розробленої програми управління ризиками. На цьому етапі визначаються терміни реалізації, відповідальні особи, форми і терміни контролю. Це – організаційна частина прийнятої програми управління ризиками;

14) здійснюється контроль і моніторинг виконання програми управління ризиками, а також проводиться збір інформації, необхідної для розробки такої програми на наступний період планування.

Згідно моделі COSO ERM (рис. 2.1) програма управління ризиками в організації складається з таких елементів:

1. внутрішнє середовище;
2. формулювання цілей;
3. ідентифікація ризиків;
4. оцінка ризиків;
5. реагування на ризики;
6. контрольні заходи;
7. інформація і комунікація;
8. моніторинг.

Внутрішнє середовище (середовище контролю) – це сукупність внутрішніх процесів, операцій, регламентів, організаційної структури, а також розподіл повноважень, правила і принципи управління персоналом, що існують в установі. Усе це спрямоване на забезпечення виконання законодавчо встановлених функцій та завдань установи для досягнення поставлених цілей.

Внутрішнє середовище є базою для всіх інших елементів внутрішнього контролю та охоплює:

а) етичні принципи і чесність керівництва та персоналу, що фіксуються у внутрішніх документах щодо етики та поведінки (кодекси етики) і формують ставлення до управління ризиками;

б) організаційну структуру, закріплену у внутрішніх документах установи, яка містить розподіл обов'язків між керівництвом, посадові інструкції, функції підрозділів, перелік відповідальних осіб та процедури внутрішнього контролю;

в) принципи управління людськими ресурсами, визначені у внутрішніх документах, що регулюють питання навчання, підвищення кваліфікації, оцінки та заохочення персоналу, забезпечення відповідної освіти та досвіду, підтримки професійного рівня.

Кожна організація має свої унікальні процеси та операції, які потребують ідентифікації та опису з визначенням відповідальних осіб, створюючи власне внутрішнє середовище. При аналізі внутрішнього середовища важливо не лише зважати на формальні документи, але й оцінювати практичну реалізацію. Завданням є виявлення сильних і слабких сторін, що впливають на діяльність організації.

Формулювання цілей. Цілі мають бути встановлені ще до того, як керівництво почне аналізувати події, які можуть вплинути на їх досягнення. Процес управління ризиками забезпечує «розумну» впевненість у тому, що керівництво компанії вірно організувало процес вибору й постановки цілей, а також що ці цілі відповідають місії організації.

Цілі організації поділяються на чотири основні категорії:

- стратегічні цілі – це кінцеві результати, на які спрямована діяльність установи, і які визначаються як очікувані показники розвитку сфери діяльності. Зазвичай кількість стратегічних цілей не перевищує п'яти. Вони затверджуються регламентами й мають бути досягнуті в результаті реалізації відповідних процесів;

- операційні цілі – конкретні, вимірювані та обмежені в часі показники, спрямовані на досягнення стратегічних цілей. Операційні цілі визначаються щорічно в плані управління ризиками і є конкретними кроками для реалізації стратегічних цілей установи;

- цілі в сфері звітності – забезпечення достовірності звітної інформації;

- цілі в сфері дотримання законодавства – забезпечення відповідності вимогам законодавства та нормативним актам.

Цілі всіх рівнів повинні бути сформульовані за принципом «SMART»:

1. Конкретність (Specific) – цілі мають чітко відображати кінцевий результат і бути зрозумілими і деталізованими.

2. Вимірюваність (Measurable) – цілі повинні мати критерії, які дозволяють оцінити їх досягнення як за кількісними, так і за якісними показниками.

3. Досяжність (Achievable) – цілі мають бути визначені з урахуванням наявних ресурсів (людських, фінансових, матеріальних тощо) і бути реально здійсненними для установи.

4. Реалістичність (Relevant) – встановлення лише тих цілей, які знаходяться в межах повноважень і відповідальності суб'єктів внутрішнього контролю.

5. Обмеженість у часі (Timely) – визначення чітких термінів досягнення цілей, що підвищує мотивацію і сприяє ефективності виконання завдань.

Ідентифікація ризиків. Ідентифікація ризиків – це визначення ймовірних подій, що можуть негативно вплинути на здатність установи виконувати завдання та функції, встановлені законодавством та внутрішніми документами, для досягнення мети і стратегічних цілей. Ідентифікацію ризиків проводить керівник кожного структурного підрозділу (або відповідальні працівники) для кожного процесу й операції відповідно до своїх повноважень.

Оцінка ризиків включає визначення рівня ризику на основі експертних оцінок, які аналізують ймовірність його виникнення та вплив на

здатність досягати стратегічні цілі. Ризики класифікуються за ймовірністю їх настання та значимістю їхнього впливу.

Реагування на ризики – вибір способу управління ризиками. Керівництво приймає рішення щодо методів реагування на ризик (уникнення, прийняття, зниження або передача ризику) і розробляє заходи, що дозволяють привести ризик до допустимого рівня.

Ефективне управління ризиками охоплює:

1) аналіз діяльності суб'єктів внутрішнього контролю;

2) збір, структурування та аналіз інформації щодо ідентифікації та оцінки ризиків;

3) розробку пропозицій для плану управління ризиками. Залежно від оцінки ризику, керівництво приймає рішення щодо форми реагування:

- зниження ризику – реалізація заходів, що зменшують або усувають ймовірність ризику чи його впливу. Містить низку операційних рішень, що приймаються щоденно;

- прийняття ризику – відсутність додаткових заходів, якщо ризик має мінімальний вплив або витрати на контроль перевищують його потенційну шкоду;

- передача ризику – розподіл ризику з іншими сторонами або передача його частини;

- уникнення ризику – припинення або призупинення діяльності, що підвищує ризик (наприклад, розгляд доцільності нових методів або проєктів).

Контрольні заходи. Заходи контролю – це сукупність управлінських дій, які запроваджені в установі та здійснюються суб'єктами внутрішнього контролю для впливу на ризики й досягнення визначених операційних цілей. Політики та процедури розробляються з метою забезпечення своєчасного і ефективного реагування на ризики. Заходи контролю застосовуються на всіх рівнях діяльності установи та охоплюють усі функції та завдання, зокрема:

1) авторизація та підтвердження – надання дозволів відповідальними особами через процедуру візування, погодження та затвердження операцій;

2) розподіл обов’язків та ротація персоналу – зменшення ризику помилок і неправомірних дій;

3) контроль доступу до ресурсів та облікових записів – обмеження доступу та закріплення відповідальності за використання ресурсів, що запобігає їх втратам чи нецільовому використанню;

4) контроль за достовірністю операцій – перевірка процесів до та після їх виконання для відповідності фактичним обліковим даним;

5) оцінка результатів діяльності – аналіз виконання функцій на предмет ефективності та відповідності нормативам;

6) систематичний перегляд роботи – контроль якості виконання завдань працівниками;

7) інші правила та процедури – наприклад, система контролю за виконанням документів, правила внутрішнього трудового розпорядку тощо.

Інформація та комунікація. Інформаційний та комунікаційний обмін – це система збору, документування, передачі і використання інформації, яка забезпечує можливість керівництву та працівникам якісно виконувати свої завдання. Важлива інформація визначається, фіксується та передається так, щоб допомагати співробітникам у виконанні їхніх обов’язків, із забезпеченням обміну даними як по вертикалі, так і по горизонталі в організації.

Ефективний інформаційний та комунікаційний обмін забезпечує повну, своєчасну та достовірну інформацію для:

- керівництва – про виконання завдань, оцінку ризиків, реалізацію заходів контролю, результати внутрішніх аудитів та вимоги зовнішніх контролюючих органів;

- працівників – для належного виконання покладених на них функцій.

Комунікаційна система містить процедури обміну інформацією, доступ до неї, правила документообігу, налагодження зовнішніх комунікацій та публічне інформування про діяльність установи тощо.

Моніторинг. Увесь процес управління ризиками в організації постійно відстежується і, за необхідності, коригується. Моніторинг може проводитися як у межах щоденної діяльності керівництва, так і через періодичні оцінки.

Заходи моніторингу – це дії, які здійснюють суб'єкти внутрішнього контролю для оцінки якості функціонування системи та відстеження результатів впровадження контрольних заходів.

Моніторинг внутрішнього контролю в установі включає:

- постійний моніторинг – здійснюється в ході щоденної діяльності установи та передбачає управлінські, наглядові й інші дії керівництва та працівників на всіх рівнях. Моніторинг проводиться в реальному часі, що дає змогу оперативно реагувати на зміни. Завдяки цьому проблеми виявляються швидше, а витрати на їхнє усунення зазвичай нижчі, ніж при періодичних оцінках;

- періодична оцінка – виконується на регулярній основі для об'єктивного аналізу роботи системи внутрішнього контролю. Зазвичай оцінку проводять спеціально створені робочі групи або підрозділи внутрішнього аудиту для перевірки результативності та виявлення можливих проблем. Під час періодичних оцінок можуть бути ідентифіковані нові ризики, враховані зміни в операційних цілях та проаналізовані причини потенційної неефективності в системі контролю або її окремих елементах.

Під час реалізації програми управління ризиками в організації можливе виникнення певних проблем, які можуть заважати отриманню результатів. Серед них слід звернути увагу на такі:

- керівник установи перевантажений управлінськими рішеннями та підписанням документів, що призводить до затримок у прийнятті рішень або недостатньої уваги до технічних аспектів. Це демотивує нижчі рівні брати на себе відповідальність;

- надмірна увага керівника до деталей управління обмежує час, необхідний для розробки стратегій і політик;

- державні службовці в структурі з ієрархією уникають участі в прийнятті рішень, не вважаючи це своєю функцією, що знижує їхню мотивацію та уповільнює розвиток професійної служби;

- ієрархічна структура призводить до того, що рішення делегуються на вищі рівні. Навіть залучені до процесу службовці не можуть приймати кінцеві рішення чи нести відповідальність;

- існуюча організаційна структура установи сформована таким чином, що не сприяє досягненню цілей організації;

- адміністративні і правові інструменти, які можуть підвищити ефективність управління, як-от делегування, недостатньо розвинені та лише інколи використовуються на практиці;

- цілі установи не чітко визначені або не передані на нижчі рівні управління;

- обмежена кваліфікація персоналу не сприяє делегуванню відповідальності;

- оцінка ризиків сприймається як додаткова бюрократична обтяженість для нижчого рівня управління та не виконується належним чином;

- відсутність окремих бюджетів для підрозділів означає, що управлінська відповідальність не доповнюється відповідальністю за ресурси;

- деякі керівники не мають впливу на перерозподіл ресурсів для підвищення ефективності надання послуг;

- система звітності та підзвітності слабка і не зосереджена на досягненні результатів;

- механізми відповідальності за неефективну діяльність недостатньо розвинені, і притягнення до відповідальності є складним процесом;

- операційна інформація, потрібна керівнику для ефективного управління, часто недоступна або її значення не усвідомлюється;

- наявна фінансова інформація містить лише порівняння витрат із бюджетом, без аналізу чи прогнозу витрат;

- контрольні заходи спрямовані переважно на бюджетні витрати, а не на досягнення поставлених цілей;

- керівництво не має можливості навчатися визначенню показників ефективності та використанню цієї інформації;

- фінансова оцінка нових інвестицій чи змін не проводиться, що може призвести до прийняття зобов'язань без забезпечення ресурсами та розуміння довгострокових наслідків;

- відсутність стратегічного фінансового планування для оцінки впливу політик на фінансовий стан призводить до короткострокових заходів економії без довготривалого ефекту;

- відсутній аналіз та оцінка прийнятих управлінських рішень;

- оцінка діяльності установ другого рівня не проводиться, і вони функціонують незалежно від установ першого рівня.

Контрольні питання

1. Що спільного в визначенні ризику в стандартах різних країн?

2. Як визначається термін «ризик» у нормативно-законодавчих актах України?

3. Назвіть чотири етапи процесу управлянні ризиками.

4. З яких елементів складається універсальна модель управління ризиками COSO ERM?

5. Як трактується куб COSO ERM?

6. Які складові моделі ризиків відповідно до стандарту ISO 31000:2018?

7. Перерахуйте ключові властивості ризик-менеджменту.

8. У чому полягає сутність ідентифікації ризиків?

9. Які глобальні ризики є актуальними в сучасному суспільстві?

10. Наведіть приклади усунення ризику, зниження ступеню ризику, прийняття ризику.

11. Які існують зовнішні і внутрішні обмеження середовища?

12. Порівняйте складові частини процесу управління ризиками в різних країнах.

13. Назвіть основні етапи процесу управління ризиками.

14. Що таке організаційна структура управління ризиками?

15. Назвіть моделі організаційних структур управління ризиками.

16. Які чотири типи методів управління ризиком існують?

17. У чому полягає сутність методів ухилення від ризику?

18. Що таке хеджування?

19. На чому основані методи локалізації ризику?

20. Що таке дисипація ризику?

21. Назвіть основні ідеї методів компенсації ризику.

22. Які аспекти повинна враховувати програма управління ризиками в організації?

23. Назвіть основні етапи розробки програми управління ризиками.

24. Що таке «внутрішнє середовище» згідно моделі COSO ERM?

25. Як формулюють цілі при управління ризиками згідно моделі COSO ERM? Що таке принцип «SMART»?

26. Які дії виконуються при реагуванні на ризик?

27. Яку роль відіграє інформаційний та комунікаційний обмін при управлінні ризиками?

28. Які дії виконуються під час моніторингу?

3. МЕТОДИ ОЦІНКИ РИЗИКІВ

3.1. Загальні підходи щодо оцінки ризиків на підприємстві

Оцінка ризиків полягає у визначенні ступеня (величини) ризику. Згідно зі стандартами ISO, оцінка ризиків являє собою результат двох процедур – аналізу та вимірювання ризиків. Від якості оцінки залежить не тільки ефективність управління ризиками, але й результат діяльності підприємства.

Поділяють такі види оцінки та аналізу ризиків:

- апріорно-стратегічний;
- оперативно-тактичний;
- апостеріорно-системний.

Апріорно-стратегічний аналіз базується на прогнозуванні виникнення ризиків і містить розробку сценаріїв розвитку ризикових ситуацій, оцінку можливості їх виникнення та важкості наслідків.

Реалізується за відсутності реальної інформації про розвиток ризикової ситуації: основним джерелом для обґрунтування вибору рішення служать прогнозна або експертна інформація, а також база знань організації. Специфіка цих інформаційних джерел полягає в тому, що вони нерідко надають неточну (умовну) інформацію або забезпечують неоднозначний (множинний) вибір рішень. Апріорно-стратегічний аналіз, з одного боку, підвищує роль і значення бази знань суб’єкта господарювання; з іншого боку, некоректні стереотипи і аналогії приводять до росту ризиків прийняття помилкового рішення.

Оперативно-тактичний аналіз реалізується на стадії реалізації заходів щодо управління ризиками, тому його основним завданням є визначення достатності й ефективності прийнятих заходів. На цій стадії аналітичні дослідження містять:

- визначення ступеня відповідності між прогнозними сценаріями розвитку ризикових ситуацій і реальністю;

- виявлення нових факторів ризику, не врахованих при проведенні апріорно-стратегічного аналізу;

- оцінку ефективності реалізованих заходів й обґрунтування додаткових управлінських рішень, якщо буде потреба;

- оперативну оцінку ефективності заходів щодо управління ризиками відповідно до реальної ситуації.

Оперативно-тактичний аналіз реалізується в умовах високої динаміки реальної інформації про розвиток ризикової ситуації: основним джерелом для прийняття рішень є дані, одержані в ході моніторингу проєкту. Але специфіка моніторингової інформації полягає в тому, що нерідко вона неструктурована і неформалізована – тим самим обмежує можливості застосовувати формальні методи обґрунтування прийнятих рішень.

Апостеріорно-системний аналіз є основою для формування системи та бази знань з управління ризиками. Він базується на основі повної і вичерпної інформації про ризикові ситуації, які супроводжували діяльність.

У ході цього аналізу формується база знань в області ризиків, що супроводжують діяльність підприємства:

- перелік можливих ризикових ситуацій;

- структура факторів внутрішнього і зовнішнього середовища та їх комбінація, що викликає виникнення ризиків;

- сценарії розвитку ризикових ситуацій;

- статистичні дані, що характеризують можливість та наслідки ризикових ситуацій;

- статистика ефективності заходів щодо управління ризиком.

Отримана інформація систематизується на основі сформованої системи класифікації ризиків, що дозволяє підвищити ефективність управління ризиками за рахунок скорочення часу підготовки рішень та використання адекватних методів аналізу і рішень.

Під час аналізу ризиків переслідуються такі цілі (отримання відповідей на запитання):

1. Що може відбутися? Визначають можливі сценарії розвитку подій у внутрішньому і зовнішньому середовищі, варіантність реалізації проєктів і відхилення в процесі їх реалізації.

2. Як оцінюється можливість ризику? Визначають імовірність, статистичну частоту можливості виникнення кожної ризикової ситуації (ступінь ризику).

3. Як вплине виникнення ризику на результат? Оцінюють економічні, соціальні, організаційні та інші наслідки виникнення кожної ризикової ситуації (міру ризику).

Порядок оцінки ризиків підприємства можна розглянути у вигляді схеми, наведеній на рис. 3.1.

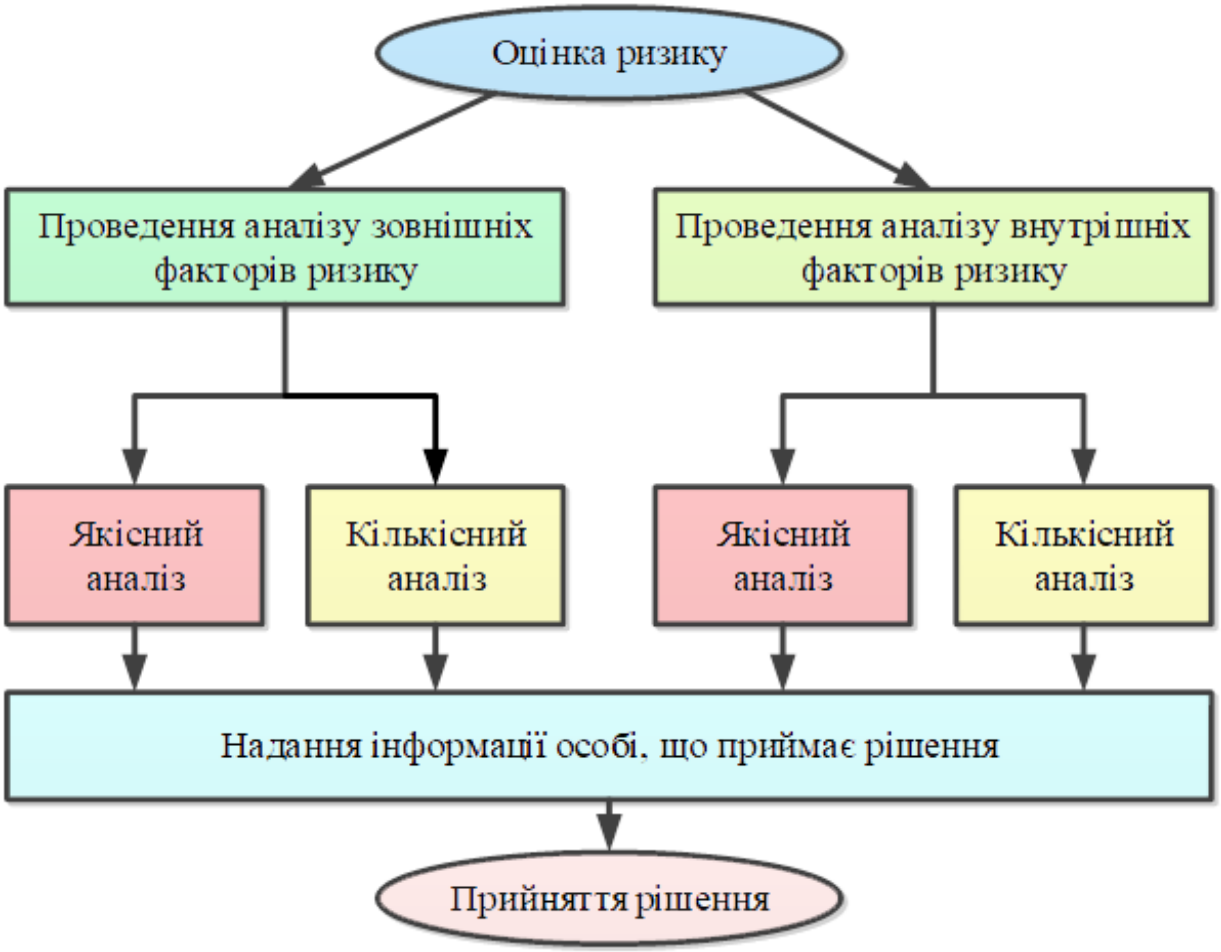


Рисунок 3.1 – Порядок оцінки ризику підприємства

Методи оцінки ризиків діляться на дві групи: якісні та кількісні.

Якісний аналіз носить описовий характер і по суті призводить аналітика до кількісного аналізу ризику. Основне завдання якісного аналізу полягає у виявленні та ідентифікації всіх можливих видів ризиків. Крім того, необхідно описати і дати вартісну оцінку всіх можливих наслідків гіпотетичної реалізації виявлених ризиків. В умовах нестабільного економічного середовища якісний аналіз як перший етап аналізу ризиків, що має метою виявити фактори, всі види ризику і провести можливу вартісну оцінку, набуває особливого значення.

Це пов’язано з наявністю нетрадиційних ризиків і відносно більш високим ступенем звичайних ризиків, поверхнева оцінка яких може призвести до негативних наслідків. Необхідною умовою при цьому є наявність ранжирування і систематизації ризиків, що повністю відображають всю ту їх сукупність, з якої доведеться мати справу при реалізації проєкту.

Друга група методів аналізу ризиків – кількісний аналіз. У літературі виділяється ряд методів, що забезпечують кількісну оцінку ризику.

Кількісний аналіз базується на визначенні чисельних величин окремих ризиків і ризику проєкту в цілому. Основу кількісної оцінки ризику складають теорії ймовірностей, математичної статистики, теорії дослідження операцій. Як правило, кількісному аналізу ризику повинен передувати якісний аналіз, при цьому повинен бути проведений базисний варіант розрахунку проєкту.

Вимірювання ризику пов’язане з оцінюванням для кожної ризикової ситуації таких параметрів:

- ступень ризику,
- міра ризику,
- ціна ризику.

Для оцінки ступеня ризику може використовуватись шкала, наведена в табл. 3.1.

Таблиця 3.1 – Шкала визначення ступеню ризику

Оцінка ймовірності	Величина ймовірності	Індикатори
ВИСОКА (ймовірно)	Ситуація ймовірно настане протягом року або її ймовірність вище, ніж 75 %	Чітка і певна можливість настання ситуації в короткостроковий період при використанні існуючих бізнес-процесів
СЕРЕДНЯ (можливо)	Ймовірність настання ситуації протягом року – 25-75 %	Ситуації можна уникнути при планомірному і чіткому управлінні ризиками
НИЗЬКА (малоймовірно)	Ситуація може настати дуже нескоро або ймовірність її настання протягом року менше, ніж 25 %	Ситуація є малоймовірною при використанні існуючих бізнес-процесів або потребує додаткових досліджень

Ступінь ризику визначає ймовірність того чи іншого сценарію розвитку подій. Ступінь ризику може розраховуватись кількісно або якісно – це оцінка можливості та (або) статистичної частоти виникнення несприятливої ситуації. Фізичний зміст показника – імовірність виникнення ризику.

Розглядаючи ступінь ризику як ймовірність настання випадку втрат, а також розмір можливого збитку від нього, можна говорити про такі градації ступеня ризику (ймовірності настання втрат):

- до 0.1 – мінімальний ризик;

- 0.1-0.3 – малий;

- 0.3-0.4 – середній. Все це – нормальний, розумний, допустимий ризик, коли ймовірні втрати не перевищують прибутки;

- 0.4-0.5 – високий ризик;

- 0.6-0.8 – критичний ризик (втрата повної виручки);

- 0.8-1.0 – катастрофічний ризик (втрата капіталу).

Міра ризику є кількісним показником – це оцінка рівня несприятливості ризикової ситуації у випадку її реалізації, що відображає її можливі негативні наслідки. Фізичний зміст показника – прямий або непрямий збиток, втрачена вигода від настання ризику.

Здійснювана в процесі прийняття управлінських рішень економічна оцінка міри ризику показує можливі втрати або в результаті будь-якої

виробничо-господарської або фінансової діяльності, або внаслідок несприятливої зміни стану зовнішнього середовища.

Залежно від конкретних умов прийняття рішення про міру ризику може оцінюватися або як найбільш очікуваний негативний результат, або як песимістична оцінка можливого результату.

Як інструмент, який використовується в управлінні ризиками для оцінки та визначення пріоритетності ризиків у межах проєкту, бізнесу чи інших контекстах застосовується матриця ймовірності та впливу (матриця оцінки ризику). Ця матриця наочно дозволяє оцінити потенційні наслідки (вплив) ризику та вірогідність (ймовірність) виникнення цього ризику:

1. Шкала ймовірності – відображає ймовірність того, що конкретна подія ризику відбудеться. Її часто виражають у кількісній (відсотки або числові значення від 0 до 1) або якісній (наприклад, низький, середній, високий рівень ризику) оцінці.

2. Шкала впливу – відображає тяжкість наслідків або ефектів у разі виникнення ризикованої події. Вплив можна оцінити за різними параметрами, такими як фінансовий, операційний, репутаційний, безпековий тощо. Часто виражається якісно (наприклад, низький, середній, високий рівень).

3. Матриця – це двовимірна сітка або таблиця, де нанесено ймовірність і вплив кожного ризику. Містить рядки та стовпці з рівнями ймовірності на одній осі і рівнями впливу на іншій осі.

Розмістивши кожен ідентифікований ризик у матриці на основі його оціненої ймовірності та впливу, можна класифікувати ризики за різними зонами ризику.

На рис. 3.2 наведено приклад матриці оцінки ризику. Цифрами 1-4 у колах позначені такі можливі ситуації:

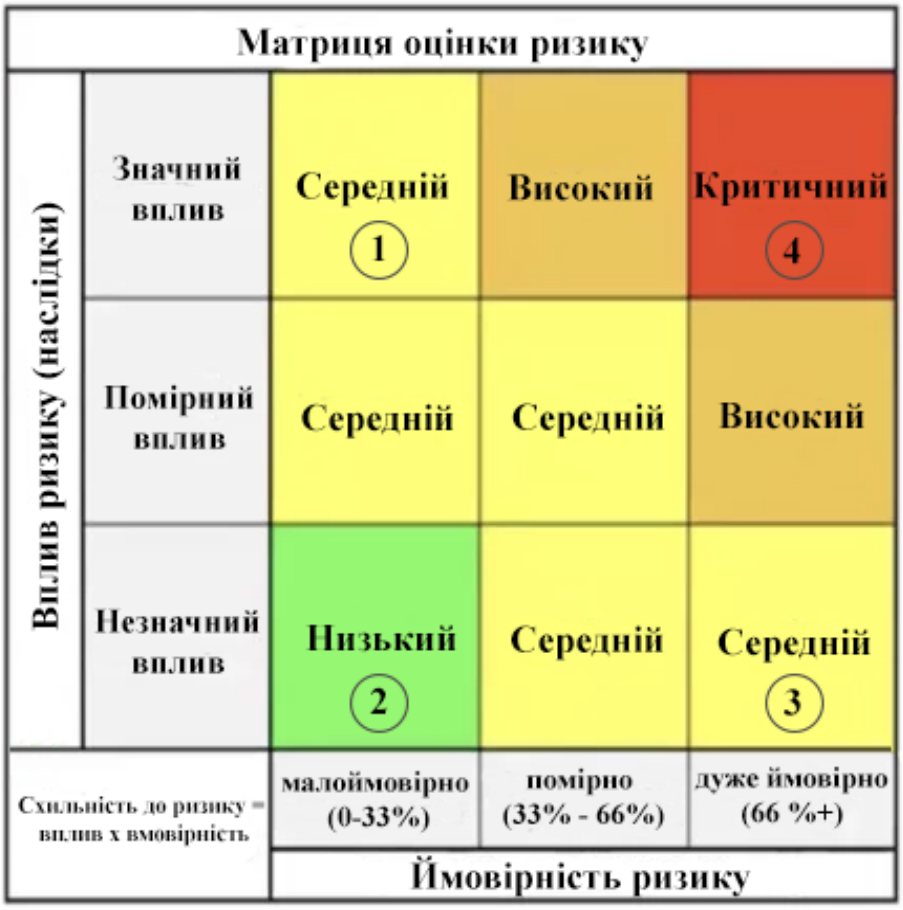


Рисунок 3.2 – Матриця оцінки ризику

1. Низька ймовірність, високий вплив: ці ризики можуть призвести до серйозних наслідків, але малоймовірні. Вони можуть потребувати уваги, особливо якщо їхній вплив може бути катастрофічним.

2. Низька ймовірність і низький вплив. Подія незначна, і ймовірність її появи низька. Ці ризики можуть не вимагати негайної уваги, і їх можна періодично контролювати.

3. Висока ймовірність, низький вплив: ці ризики ймовірно виникнуть, але можуть мати відносно незначні наслідки. Їх все одно слід відстежувати та керувати ними, але вони не такі термінові, як ризики із значними наслідками.

4. Висока ймовірність, високий вплив: Ризики в цьому квадранті є найбільш критичними та вимагають негайної уваги та вирішення, оскільки вони можуть мати значні наслідки.

Матриця ймовірності та впливу є цінним інструментом для оцінки ризиків, прийняття рішень і стратегічного планування.

Ціна ризику – кількісний показник, який відображає відношення максимально можливого результату й міри ризику. Фізичний зміст показника – позитивний результат, що припадає на одиницю негативного.

Головні принципи оцінки ризику, до яких необхідно прагнути:

- розміри втрат від різних видів ризику є незалежними один від одного: якщо один із видів ризику переходить у категорію реалізованого, то втрати внаслідок реалізації інших ризиків не змінюються;

- реалізація певного виду ризику не обов'язково збільшує чи знижує можливість виникнення ризику іншого виду, за винятком форс-мажорних обставин;

- максимально можливі втрати, у випадку реалізації конкретного ризику, не повинні перевищувати фінансових можливостей суб'єкта господарювання (цей принцип ґрунтується на концепції прийнятного ризику, що передбачає можливість прийняття ризику тільки в межах власних активів).

3.2. Оцінювання ризиків кібербезпеки ресурсів інформаційних систем

Безпека інформаційних систем – це їхня захищеність від випадкового чи навмисного втручання в штатний процес їх функціонування. Загалом йдеться про функціональну безпеку інформаційної системи, коли важливим є виконання системою поставлених перед нею завдань. Якщо ж в інформаційній системі міститься інформація, надання та (або) поширення якої обмежене, то в такому випадку йдеться також і про інформаційну безпеку.

Кібербезпека – це стан захищеності інформаційної системи та інформації, що міститься в ній, від зовнішніх і внутрішніх загроз. Стан захищеності порушується у вигляді кібератак. Кібератака – це цілеспрямований вплив програмних та (або) програмно-апаратних засобів на інформаційну систему з метою порушення та (або) припинення її

функціонування та (або) створення загрози безпеці оброблюваній такою системою інформації.

Таким чином, поняття кібербезпеки включає захищеність інформації, яка обробляється інформаційною системою (інформаційна безпека), так і захищеність процесу функціонування самої інформаційної системи (функціональна безпека). У реальному середовищі функціонування будь-якої інформаційної системи незалежно від неї існує безліч загроз її безпеці. Загроза безпеці інформаційної системи – це можливий вплив на неї, який прямо чи опосередковано може завдати шкоди її безпеці. Слід розділяти загрози функціональній та інформаційній безпеці, виходячи з функцій, на які вони націлені. Сукупність всіх загроз, які в тій чи іншій мірі можуть завдати шкоди безпеці інформаційної системи, формують реальне середовище її функціонування. Саме таке функціонування слід розраховувати під час експлуатації інформаційних систем. Будь-яка загроза не може існувати сама по собі в неї має бути джерело.

Джерела загрози в інформаційних системах – це потенційні антропогенні, техногенні або стихійні носії загрози безпеці. Таким чином, джерелом загрози можуть бути:

- суб’єкти, потенційні ненавмисні чи навмисні дії яких можуть завдати шкоди функціональній чи інформаційній безпеці інформаційної системи;

- апаратні, програмні чи апаратно-програмні технічні засоби;

- засоби та комплекси, відмови яких або наявність в їх реалізації логічних помилок може призвести до порушення безпеки інформаційної системи;

- стихійні явища – стихійні лиха, які частково або повністю перешкоджають функціонуванню інформаційної системи.

При виконанні якісного аналізу головне завдання полягає в одержанні інформації про структуру, властивості об’єкта і наявні ризики, а також у визначенні факторів ризику і обставин, що приводять до ризикових ситуацій. Шляхом якісного аналізу виявляються джерела, причини, фактори ризиків,

установлюються потенційні зони ризиків, їх види. До завдань якісного аналізу слід також віднести визначення факторів ризику, етапів роботи, при виконанні яких ризик виникає, тобто встановити потенційні сфери ризику, після чого ідентифікувати всі можливі ризики. Фактори впливу на ступінь ризику [15] наведені на рис. 3.3.

Рисунок 3.3 – Фактори впливу на ступінь ризику

Відповідно до стандарта ISO 31010-2019 фактори ризику поділено на кілька категорій. Наведена на рис. 3.4 діаграма показує ключові ризики, що виникають у силу внутрішніх та зовнішніх факторів. Ризики можуть бути диференційовані за такими категоріями: стратегічні, фінансові, операційні, небезпеки.

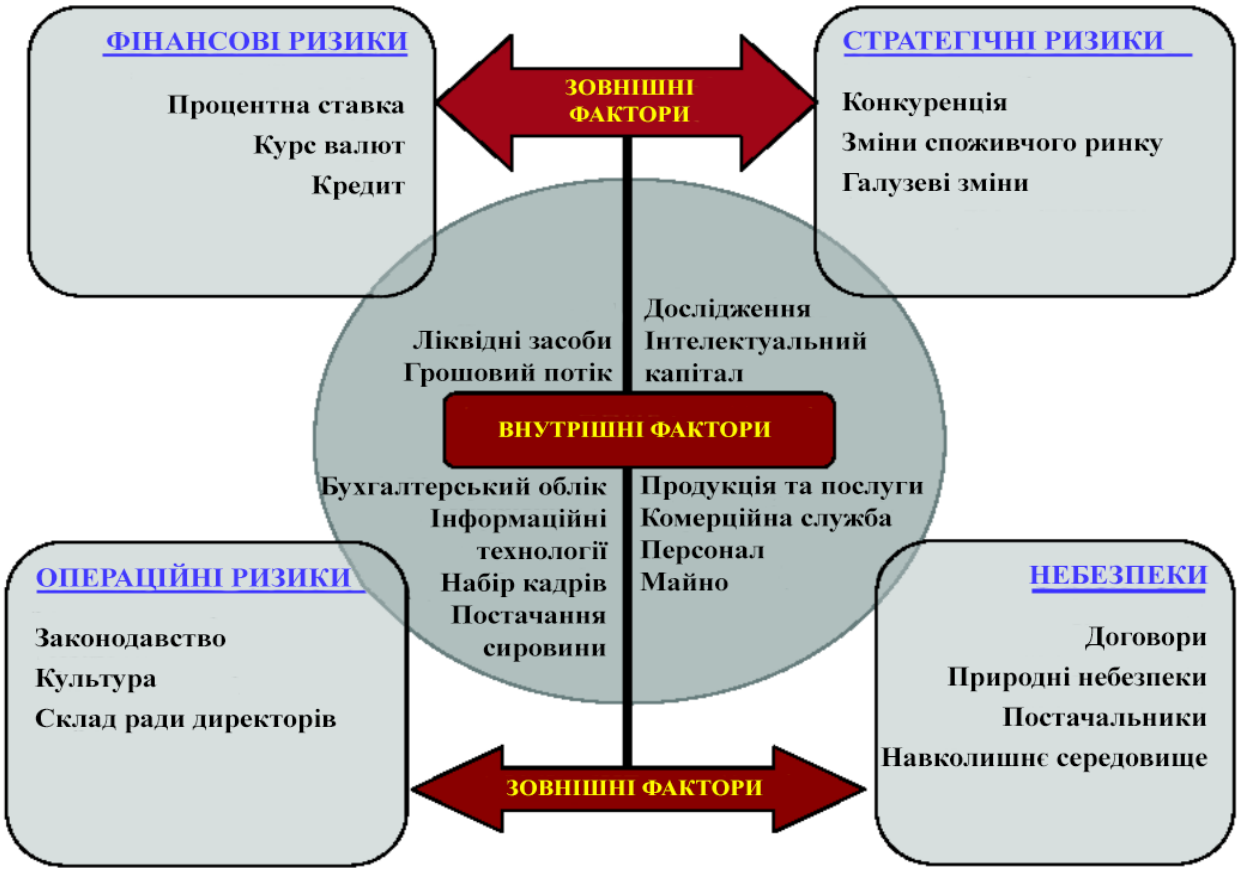


Рисунок 3.4 – Фактори ризику відповідно до стандарта ISO 31010-2019

Якісний аналіз ризику вимагає ґрунтовних знань, досвіду, інтуїції в тій чи іншій сфері економічної діяльності. Його головна мета – визначити чинники і зони ризику, після чого ідентифікувати всі можливі ризики. Характерними для цього аналізу є, зокрема, такі аспекти.

Перший аспект пов'язаний з необхідністю порівнювати очікувані позитивні (сприятливі) результати з можливими економічними, соціальними (як сьогоденними, так і майбутніми) несприятливими наслідками. У зв'язку з цим необхідно ідентифікувати причини виникнення ризику, виявити його чинники, види невизначеності та конфліктності, які зумовлюють ризик. Необхідно також здійснити класифікацію ризику.

Другий аспект якісного аналізу ризику пов'язаний з виявленням впливу рішень, які приймаються в умовах невизначеності та конфліктності, на інтереси суб'єктів господарювання. Без урахування інтересів (зацікавленості) неможливі якісні перетворення в соціально-економічному житті як на

макрорівні, так і на мезо- та мікрорівнях. Коли немає зацікавленості в результатах економічних рішень, то немає й ризику.

Якісний аналіз ризику визначає:

- природу й тип причин і наслідків ризиків, що можуть виникнути;
- метод вимірювання ризиків;
- спосіб визначення їх ймовірності;
- часові рамки ймовірності та (або) наслідків;
- рівень ризиків (зонування);
- погляди зацікавлених сторін;
- рівень, на якому ризик стає припустимим або прийнятним;
- виявлення комбінації множинних ризиків, які повинні бути розглянуті.

Загальний алгоритм якісного аналізу ризику виглядає таким чином:

1. Аналіз та діагностика економічної (управлінської) ситуації, пов'язаної з певним об'єктом (проєктом) і обтяженої ризиком. Визначення головних завдань, основних суперечностей (неузгодженості), домінуючих тенденцій.

2. Виявлення інтересів основних учасників подій, їхнього ставлення до ризику.

3. Виявлення управлінських цілей, методів та засобів їх досягнення.

4. Аналіз основних чинників (параметрів), які впливають на прийняття рішень, розподіл їх на керовані та некеровані параметри ризику.

5. Здобуття інформації про можливі діапазони значень некерованих параметрів (чинників) ризику.

6. Генерація набору альтернативних варіантів проєкта (об'єкта, способу дій).

7. Виявлення пріоритетів (системних критеріїв) суб'єкта ризику щодо різних варіантів проєкту (об'єкта, способу дій).

8. Оцінювання згенерованих альтернативних варіантів. Вибір їх підмножини, що найкраще відповідає вимогам суб'єкта ризику.

9. Розробка відповідного способу дій (програми), яка була б найкращою (найбільш ефективною) з погляду переведення обтяженої ризиком ситуації в більш сприятливу.

Переваги якісного аналізу ризику:

- швидкість;
- прийнятна точність;
- не потребує спеціальної підготовки;
- легкість реалізації;
- ефективність;
- можуть бути залучені всі зацікавлені сторони.

Вхідними даними для проведення якісного аналізу є:

1) фактори зовнішнього середовища;
2) активи організаційного процесу;
3) опис змісту проєкту;
4) план управління ризиками;
5) реєстр ризиків.

Інструменти, які використовуються для якісного аналізу:

1) оцінка ймовірності виникнення і впливу ризиків;
2) матриця ймовірності і впливу;
3) оцінка якості даних про ризики;
4) категоризація ризиків;
5) оцінка терміновості ризиків;
6) експертна оцінка.

Будь-яка оцінна методика оцінки ризиків базується на конкретному методі оцінки або на поєднанні декількох методів. Розрізняють такі основні групи методів, які можуть використовуватися при оцінці рівня, ступеня і кількісного вираження ризику на підприємствах:

- формально-логічні методи;
- експертні методи;
- статистичні методи;

- розрахунково-аналітичні методи.

Найбільш поширеними є такі групи якісних методів оцінки ризиків: формально-логічні та експертні.

Метою **формально-логічних методів** оцінки є виявлення факторів виникнення ризиків та їх сутності. Дані методи використовуються спеціалістами-аналітиками на основі наявної інформації та узагальнюючих даних про виробничо-господарську діяльність. На практиці найбільше використовуються такі методи: морфологічний аналіз, семантичний аналіз, декомпозиція і композиція, методи на основі нечіткої логіки, причинно-наслідковий аналіз, методи сценаріїв, методи співставлення, контекстний аналіз, зворотній інжиніринг тощо.

Експертні методи призначені для одержання широкого переліку кількісних і якісних експертних оцінок практично в усіх напрямках аналізу ризиків діяльності.

Методи експертних оцінок є найпоширенішими методами, що використовуються в процесі якісного аналізу ризиків в інформаційних системах. Їх сутність полягає в отриманні необхідної інформації щодо ризиків, які можуть загрожувати діяльності (або певному проєкту) підприємства, на основі опрацювання думок експертів – співробітників, досвідчених підприємців або інших фахівців.

Особливості експертних оцінок полягають у тому, що вони вимагають наявності в експертів відповідної компетенції, вони засновані на більш складних і трудомістких (в порівнянні з кількісними оцінками) процедурах обробки даних та вони потребують розробки адекватних рейтингових шкал для впорядкування оцінок.

Залежно від чисельності та підготовленості експертів експертні методи поділяються на:

- масові опитування (анкетування, інтерв’ювання, телефонні та інтернет-опитування, статистичні спостереження тощо) – являє собою поверхневу оцінку непрофесійних респондентів;

- вибіркові дослідження (фокус-групи, імітаційні ігри, тренінги тощо) – проводяться при ретельному і послідовному дослідженні індивідуальних думок та мотивів непрофесійних респондентів;

- професійні судження (мозковий штурм, метод Дельфі, попарне порівняння, метод аналогій тощо) – полягають у залучені професіональних експертів для розробки конкретних рекомендацій та оцінок відносно діяльності підприємства на основі життєвого і професійного досвіду експертів; результати даного оцінювання являють собою якісні дані про можливі ризикові ситуації та методи управління ними;

- встановлення переваг (ранжирування, попарне порівняння, різні види голосувань тощо) – здійснюється як професійними так і непрофесійними респондентами з метою встановлення якісних характеристик.

Оскільки методи експертних оцінок передбачають збір і вивчення фахівцями оцінок ймовірностей виникнення різних рівнів втрат і такі оцінки будуються зазвичай на обліку всіх факторів ризику, а також – статистичних даних, то слід прагнути до того, щоб експерти дали свої оцінки рівнів втрат, за якими можна було б знайти середні значення експертних оцінок. Особливе значення представляє питання про точність і надійність рекомендацій, заснованих на експертних оцінках, тому що цим у кінцевому рахунку визначається їх корисність і придатність. Слід критично ставитися до надмірно оптимістичних висловлювань про точність і надійність даних методів. Так само практика не підтверджує і негативне ставлення до можливості використання імовірнісних оцінок експертів у різних областях управління.

Як критерії оцінки небезпеки конкретної загрози слід вибрати можливість виникнення джерела загрози, ступінь його готовності зробити атаку, а також фатальність для інформаційної системи від загрози. Коефіцієнт небезпеки загрози обчислюється на підставі балів.

Аналізуючи коефіцієнти небезпеки сукупності загроз, можна провести їх ранжирування і визначити для конкретної комунікаційної системи перелік найбільш небезпечних з них.

Але самі собою загрози не становлять небезпеку для інформаційних систем. Загрози можуть зовсім не завдавати шкоди їхній безпеці. Небезпеку для інформаційної системи становлять лише ті загрози, для яких вона є вразливою, або, іншими словами, має певні вразливості, через які джерела загроз можуть реалізувати свої загрози та завдати шкоди цьому об’єкту.

Вразливість інформаційної системи – це властиві інформаційній системі причини, що призводять до порушення безпеки її функціонування або безпеки інформації, що в ній обробляється. Сукупність вразливостей інформаційної системи обмежує сферу її експлуатації та режими функціонування. Максимально повне уявлення про уразливості інформаційної системи дозволяє застосувати адекватні заходи щодо їх мінімізації та, тим самим, усунути можливі наслідки від впливу загроз.

Як критерії оцінки небезпеки вразливості пропонуються: фатальність наявності в інформаційній системі вразливості, доступність вразливості для джерел загроз, а також кількість вразливостей обраного роду в інформаційній системі або частота їх появи. Аналогічно з процесом оцінки небезпеки загроз експерти виставляють бали за кожним із критеріїв. Аналізуючи коефіцієнти небезпеки сукупності вразливостей, можна зробити їх ранжирування та визначити ті з них, усуненням яких необхідно зайнятися насамперед.

Для оцінки ризиків кібербезпеки інформаційної системи виділяються її активи – все те, що необхідно для її штатного функціонування і знаходиться в її розпорядженні (апаратні засоби, програмне забезпечення, інформація, що зберігається). Процес оцінки ризиків для кожного з активів повинен враховувати вартість самого активу та ймовірну характеристику можливості порушення його кібербезпеки. При цьому важливо враховувати як всю сукупність загроз, так і всю сукупність вразливостей.

Процес експертної оцінки управління ризику складається з п’яти послідовних етапів:

1. По кожному виявленому ризику визначається граничний рівень (наприклад, який визначається за 100-бальною шкалою), прийнятний для організації і дає можливість реалізовувати певну діяльність або проєкт.

2. За потреби вирішується конфіденційна диференціальна оцінка компетентності експертів (наприклад, оцінка виставляється на десятибальній шкалі).

3. Оцінка ризиків експертами з урахуванням ймовірності настання ризикової події (у частках одиниці) та небезпеки ризиків, що знижують можливість реалізації проєкту або діяльності (наприклад, за стобальною шкалою).

4. Розробник діяльності або проєкту отримує дані-оцінки, вводить їх у певні таблиці (наприклад, у «карту ризиків») та визначає інтегральний рівень по кожному виду ризиків.

5. Порівняння отриманих інтегральних рівнів ризиків та граничних рівнів для цього виду ризику, внаслідок чого виноситься рішення про прийнятність цього виду ризику для розробника діяльності або проєкту.

При цьому, якщо прийнятий граничний рівень одного або декількох видів ризиків нижче за отримані інтегральні значення, визначаються різні методи мінімізації впливу ідентифікованих ризиків на успіх здійснення проєкту або діяльності, і після повторно реалізується аналіз та оцінка ризиків.

Існуючі методи ранжирування загроз та вразливостей в інформаційних системах виконують їхню оцінку незалежно один від одного. Однак, загрози не становлять небезпеки для об’єкта без наявності вразливостей, що їм відповідають. Також і вразливості не підривають рівень кібербезпеки інформаційної системи, якщо немає загроз, які можуть скористатися ними. Отже, оцінку загроз та вразливостей слід проводити сукупно. Загальна

процедура оцінки ризиків кібербезпеки інформаційних систем проводиться з урахуванням наведеного вище процесу експертної оцінки таким чином:

1. Визначається список активів інформаційної системи.

2. Для кожного з активів визначається сукупність загроз його кібербезпеці.

3. Для кожної з загроз визначається сукупність вразливостей, якими вона може реалізуватися.

4. Групою експертів проводиться оцінка коефіцієнта небезпеки кожній із загроз.

5. Здійснюється ранжирування загроз щодо зменшення коефіцієнта їх небезпеки. Таким чином, для кожного активу формується індивідуальний ранжируваний за ступенем небезпеки перелік загроз.

6. Для кожного з активів визначаються ризики кібербезпеки за його вартістю та максимальним для активу значенням коефіцієнта небезпеки загрози.

Переваги експертних методів:

- відсутність необхідності в точних вихідних даних та дорогих програмних засобах;

- можливість проводити оцінку до розрахунку ефективності проєкту;

- простота розрахунків.

Недоліки методів експертних оцінок:

- складність у залученні незалежних експертів;

- суб’єктивність оцінок.

Під час реалізації даних заходів необхідно, щоб фахівці-експерти:

- мали достатній рівень знання певної сфери діяльності і проблеми, що розглядається;

- мали доступ до всіх даних, що стосуються проєкту;

- були креативними особистостями;

- не мали особистих переваг у розглянутому проєкті;

- були здатні оцінювати будь-яку кількість виявлених ризиків.

Таким чином, експертні методи оцінки ризику зручно застосовувати у випадку наявності малої кількості даних, коли реалізація математичної оцінки рівня ризику неможлива.

Експертні методи оцінки часто використовується в поєднанні з експертними системами. Експертні системи засновані на суб'єктивному знанні процесу. Рішення приймається на основі кількісних (цифрових) даних, отриманих у результаті проведеної експертизи на основі:

1) фактів у масштабі проблеми;

2) теорій про проблему;

3) чітких правил і процедур щодо основної лінії проблеми;

4) загальних стратегій для вирішення конкретного виду проблем.

Основні категорії експертних систем:

- інтерпретація – висновок про ситуацію, її опис будується на основі інтуїції;

- передбачення – висновок про ситуацію будується на основі імовірнісних значень параметрів даної ситуації і аналогічних;

- діагноз – висновки про відхилення у функціях системи будуються на основі результатів досліджень;

- припущення – складання суджень про об'єкт дослідження будується на основі порівняння даної ситуації з аналогічною і прив'язки тенденцій аналогічної ситуації до даної;

- планування – розробка планів з чіткою постановкою цілей;

- повчання – вказівка на вразливість окремих сторін плану і повідомлення можливих винятків;

- виправлення – припис коштів для виконання плану реалізації рішення;

- інструктування – постановка діагнозу і коригування виконання;

- контроль – пояснення, пророкування, виправлення і повчання з поведінки системи в ході реалізації рішення.

Кількісний аналіз ризику заснований на використанні числових оцінок і показників, над якими можна виконувати основні математичні дії. Чим досконалішими є методи дослідження та кількісної оцінки ризику, тим меншим стає чинник невизначеності. Застосування кількісних оцінок змінює рівень невизначеності – аж до повної детермінації рішень.

Особливості кількісного аналізу полягають у тому, що він доцільний лише за умови наявності об'єктивних даних для розрахунків та повинен базуватися на репрезентативних даних (хронологічних рядах, статистичних вибірках тощо). Від аналітика при цьому вимагається розуміння формальних розрахунково-аналітичних методів і інструментів.

Методи кількісної оцінки ризику дають змогу виявити чисельне визначення розмірів окремих ризиків і ризику конкретного виду діяльності в цілому. При кількісній оцінці ризиків підприємства застосовують різноманітні методи. Обирання того чи іншого з них буде залежати від виду і джерел ризику, характеристик сфери і виду діяльності, фінансового стану, величини підприємства тощо.

Загалом такі методи поділяються на:

- об'єктивні (ті, що використовують характеристики випадкових процесів, отримані на основі даних, що не залежать від думки конкретно особи);

- суб'єктивні (які ґрунтуються на експертних оцінках ризику).

Методи кількісного аналізу:

1. **Статистичні методи** передбачають формалізовану обробку накопичених статистичних кількісних даних про ризикові ситуації. До даної групи входять стохастичні методи, кореляційно-регресійний аналіз тощо. Перевагами статистичних методів є: можливість одержання найбільш повної кількісної картини про рівень ризику, можливість використання попереднього досвіду робіт. До недоліків таких методів відносять: відсутність аналізу джерел походження ризику (ризик береться як цілісна величина – ігноруються його складові), необхідна наявність достатньо повної

статистичної інформації, невисока точність оцінки, ігнорування фактору постійного розвитку будь-якої діяльності.

Статистичні методи сприяють вивченню статистики втрат, що мали місце в аналогічних видах виробничо-господарської діяльності, встановлення частоти появи певних рівнів втрат, а по частоті – прогнозування ймовірності втрат. Аналізуються всі статистичні дані, що мають відношення до результативності прийнятого рішення. Статистичні методи розглядаються в зв'язку з поняттям зон і меж ризику. Точки, що визначають рівень втрат і ймовірність появи цих втрат, описуються за допомогою статистичного аналізу досить великого масиву даних.

Наявність інформації і правильність її використання в значній мірі зумовлюють раціональність (оптимальність) обраного рішення. Існує досить поширена думка про те, що чисельні дані, що містяться в поточній статистичній звітності, а також у різних планових і технічних документах, і є інформацією. Насправді, крім даних, що складаються із зібраних (числових) величин, інформація містить інші, що не піддаються безпосередньому виміру, величини. Наприклад, припущення про можливі рішення і результати. Практика показує, що основні труднощі, що виникають при пошуку і виборі рішень у ризиковій ситуації, обумовлені перш за все недостатньо високою якістю і неповнотою наявної інформації.

Основні «інформаційні» труднощі у випадку застосування статистичних методів оцінки ризиків можна поділити на такі:

- вихідна статистична інформація найчастіше буває недостатньо достовірною. Однак, якщо присутні достовірні дані про минуле, вони не завжди можуть служити надійною базою для прийняття рішення, спрямованого в майбутнє, оскільки існуючі умови і обставини можуть надалі змінитися (непередбачувані ризики);

- деяка частина інформації має якісний характер і не піддається кількісній оцінці. Так, не можна точно розрахувати ступінь впливу соціальних і політичних факторів на реалізацію планів;

- виникають ситуації, коли необхідну інформацію отримати можна, але в момент прийняття рішення вона відсутня, оскільки це пов’язано з великими витратами часу і коштів;

- істотні труднощі при виборі рішення полягають у тому, що будь-яка ідея містить потенційну можливість різних схем її реалізації, а будь-яка дія може призводити до численних наслідків.

Багатозначність, багатовимірність і якісна відмінність показників у випадку застосування статистичних методів оцінки є серйозною перешкодою для отримання вірного рішення в ризиковій ситуації.

2. **Розрахунково-аналітичні** передбачають обробку кількісних і грошових оцінок ризику. До даної групи методів відносять фундаментальний аналіз витрат, метод прямого і зворотного розрахунку, аналіз стійкості і чутливості, факторний аналіз, розрахунки граничних значень, тощо. Перевагами розрахунково-аналітичних методів є: можливість проведення пофакторного аналізу параметрів, які впливають на ризик, і виявлення подальших напрямів його зниження. До недоліків таких методів відносять: відсутність аналізу джерел походження ризику (ризик береться як цілісна величина) та такі методи недостатньо опрацьовані на теоретичному рівні.

Розрахунково-аналітичні методи базуються на математичних методах. Використання математичних методів і обчислювальної техніки дозволяє приймати рішення, засновані на більш повній і надійній інформації, ніж можна зібрати в сучасних умовах на підприємствах при проведенні процедури оцінки ризикових ситуацій.

3. **Нормативні методи** передбачають визначення меж (діапазонів) ризиків та гранично припустимих значень ризикових параметрів. До цієї групи належать методи фінансових коефіцієнтів, критичних значень і лімітів, рейтингів тощо. Перевагами таких методів вважають легкість розрахунку та оперативність. До недоліків таких методів відносять невисоку точність оцінки та те, що вони не дають можливості врахувати особливості конкретної ситуації.

4. **Методи моделювання** полягають в імітації реальних умов діяльності з метою виявлення вузьких місць, первинних і вторинних центрів ризику, перевірки гіпотез, тощо. Моделювання може бути реалізоване у формі макетування, лабораторних випробувань, економіко-математичних і віртуальних моделей. Перевагами таких методів є можливе застосування в умовах невизначеності інформації про ситуацію прийняття рішення та можливість використання багатьох критеріїв прийняття рішень. Недоліком вважається те, що моделювання суттєво спрощує реальні умови реалізації проєкту. Особливе значення зараз придбали методи оптимізації, засновані на застосуванні математичних моделей, що забезпечують економію часу і коштів при вирішенні практичних завдань. Побудова моделей допомагає привести складні і часом невизначені фактори, пов'язані з проблемою прийняття рішення, у логічну схему, визначити, які дані необхідні для оцінки і вибору альтернатив. Але ці методи застосовні на етапі регулювання ризику (ризиковий менеджмент) при визначенні впливу рівня ризику на результати виробничо-господарської і фінансової діяльності підприємства.

Імітація використовується як метод аналізу ситуації. Згідно визначення – це процес наслідування або симулювання дійсності, це методика для проведення експериментів з математичним забезпеченням моделі поведінки системи в певний період часу.

Існують такі види імітації:

- імовірнісна;
- залежна і незалежна від часового чинника;
- явна (видима);
- ділові ігри;
- імітація великих систем.

Імітаційне експериментування повинно враховувати обставини можливого ризику ситуації.

Основними методами кількісної оцінки ступеню ризику є: статистичний метод, метод експертних оцінок, метод використання аналогів,

метод критичних значень, метод оцінки ризику за допомогою «дерева рішень», аналіз чутливості, аналіз сценаріїв, імітаційне моделювання.

Кожен із методів оцінки ризику має свої переваги та недоліки, які необхідно враховувати при оцінюванні, оскільки інколи це може призвести до помилкових висновків. Не існує єдиного методу, який би дозволив здійснити повний аналіз та дати точну оцінку ризику, оскільки ризик немає сталого, абсолютного значення, він постійно змінює свої характеристики залежно від факторів дії зовнішнього та внутрішнього середовища. Тому, на практиці при оцінюванні ризиків, як правило, використовують комбінацію якісного та кількісного підходу, що дає змогу визначити не лише очікуваний рівень відповідних показників, але й встановити ймовірність їх досягнення.

Стандарт ISO 31010-2019 є одним з основоположних документів з практики управління ризиками. У ньому визначаються підходи, засновані на застосуванні методів, перевірених багаторічною практикою. Їх застосування дозволяє:

- зрозуміти, які небезпеки загрожують підприємству і яким чином вони вплинуть на досягнення цільових показників діяльності;
- структурувати інформацію, необхідну для прийняття рішень;
- ідентифікувати внутрішні та зовнішні фактори ризику;
- порівняти рівень ризику із середньоринковими значеннями та з показниками альтернативних методів організації діяльності;
- налагодити обмін інформацією про невизначеності і ризики;
- ранжирувати ризики на підставі показників їх суттєвості і ймовірності;
- визначити найбільш ефективні способи впливу на ризик;
- систематизувати інформацію про факти реалізації ризику;
- забезпечити комплаенс-контроль в організації (контроль відповідності нормативно-правовим вимогам);
- налагодити постійну систему оцінки ризику;

- забезпечити обґрунтування рішень про прийняття ризику (ризик-апетит).

У стандарті ISO 31010-2019 визначено понад 30 методів оцінки ризику (українські назви методів взяті зі стандарту ДСТУ IEC/ISO 31010) [4]:

- **мозкова атака** або мозковий штурм (Brainstorming) – обговорення проблеми групою фахівців, метою якого є ідентифікація можливих видів відмов і відповідних небезпек, ризику, критеріїв прийняття рішень та/або способів обробки ризику;

- **структуроване чи напівструктуроване опитування** або структуровані або частково структуровані інтерв'ю (Structured or semi-structured interviews) – запитання із заздалегідь підготовленого переліку, що заохочують всебічний аналіз ситуації і, таким чином, більш повну ідентифікацію небезпек і ризику;

- **метод Дельфі** (Delphi method) – отримання узагальненої думки групи експертів;

- **переліки контрольних запитань** або контрольні листи (Checklist) – переліки небезпек, ризику або відмов засобів управління, які зазвичай розробляють на основі отриманого раніше досвіду, результатів попередньої оцінки ризику або результатів відмов, що сталися в минулому;

- **попереднє аналізування небезпечних чинників** або попередній аналіз небезпек PHA (Preliminary Hazard Analysis) – ідентифікація небезпек, небезпечних ситуацій і подій, які можуть порушити роботу або завдати шкоди цьому виду діяльності, обладнанню або системі;

- **дослідження небезпечних чинників і працездатності** HAZOP (HAZard & Operability) – заснований на використанні керуючих слів, які допомагають зрозуміти, чому мета проєктування або умови функціонування не можуть бути досягнуті на кожному етапі проєкту, процесу, процедури або системи;

- **аналізування небезпечних чинників і критичні точки контролю** або аналіз ризиків і критичних контрольних точок HACCP (Hazard Analysis

and Critical Control Points) – мінімізація ризику шляхом застосування засобів управління в процесі виробництва продукції, а не тільки при контролі кінцевої продукції;

- **загальне оцінювання екологічного ризику** (Toxicity assessment) – визначення схильності рослин, тварин і людей впливу екологічних небезпек;

- **структурований метод «Що, якщо?»** SWIFT (Structured What-If Technique) – метод дослідження сценаріїв, заснований на командній роботі, в якому використовують набір слів або фраз–підказок, що допомагають у процесі наради учасникам групи ідентифікувати небезпечні ситуації і створити сценарій їх розвитку;

- **аналізування сценаріїв** (Scenario analysis) – процес розробки описових моделей розвитку подій для ідентифікації ризику шляхом розгляду можливих подій у майбутньому і дослідження їх значущості та наслідків;

- **аналізування впливу на діяльність** або оцінка впливу на бізнес BIA (Business Impact Analysis) – дослідження ключових видів відмов/порушень/руйнувань, які можуть вплинути на ключові види діяльності і процеси організації, ідентифікація і визначення необхідних можливостей для управління організацією в цих умовах;

- **аналізування першопричини** RCA (Root Cause Analysis) – дослідження втрат внаслідок різних видів відмов без розгляду їх зовнішніх проявів;

- **аналізування видів і наслідків відмов** FMEA (Failure Mode and Effects Analysis) – ідентифікація способів відмови компонентів, систем або процесів, які можуть призвести до невиконання їх функцій;

- **аналізування дерева відмов** або аналіз дерева несправностей FTA (Fault Tree Analysis) – ідентифікація та аналіз факторів за допомогою дедукції, які можуть сприяти виникненню небажаної події, що досліджується;

- **аналізування дерева подій** ETA (Event Tree Analysis) – графічний метод подання взаємовиключних послідовностей подій, що наступають за

появою вихідної події, відповідно до функціонування і нефункціонування систем, розроблений для пом'якшення наслідків небезпечної події;

- **аналізування причин і наслідків** (Cause and consequence analysis) – поєднання методів дерева відмов і дерева подій;

- **аналізування причинно-наслідкових зв'язків** або аналіз причин та наслідків (Cause-and-effect analysis) – структурований метод ідентифікації можливих причин небажаної події чи проблем шляхом компонування можливих причин та факторів в узагальнені категорії так, щоб можна було дослідити всі можливі гіпотези;

- **аналізування рівнів захисту** LOPA (Layers of Protection Analysis) – змішана оцінка ризику, пов'язаного з небажаною подією або сценарієм, аналіз достатності заходів з управління або зниження ризику;

- **дерево рішень** (Decision tree) – подання альтернативних варіантів рішень з їх вихідними даними і відповідною невизначеністю для управління ризиком проєктних рішень та в інших випадках, коли необхідно вибрати найкращий спосіб дій у ситуації невизначеності;

- **загальне оцінювання надійності людини** або аналіз впливу людського фактора HRA (Human Reliability Assessment) – оцінка впливу дій людини, у тому числі помилок оператора, на роботу системи;

- **аналізування за схемою «краватка-метелик»** BTA (Bow-Tie Analysis) – схематичний спосіб опису та аналізу шляху розвитку небезпечної події від причин до наслідків;

- **технічне обслуговування, зорієнтоване на забезпечення надійності** RCM (Reliability-Centered Maintenance) – визначення політики проведення технічного обслуговування, спрямованої на попередження відмов і способів її впровадження для досягнення необхідного рівня безпеки, експлуатаційної готовності та економічності функціонування для всіх типів устаткування;

- **аналізування паразитних схем** SCA (Sneak Circuit Analysis) – ідентифікація помилок проєктування (неявні дефекти комп'ютерного обладнання, програмного забезпечення або їх поєднання, що можуть

спричинити подію або перешкоджати реалізації очікуваної події і не є наслідком відмови компонентів);

- **Марковське аналізування** (Markov analysis) – метод, заснований на понятті «станів» (наприклад, працездатний і непрацездатний стан) і переходів між ними в часі в припущенні постійної ймовірності переходу (використовується для аналізу ремонтопридатності систем і в ситуаціях, коли застосування аналізу надійності окремих блоків системи є недоцільним);

- **імітаційне моделювання за методом Монте-Карло** (Monte Carlo simulation) – статистичний метод дослідження впливу невизначеності для оцінки діапазону зміни результатів і відносної частоти значень у цьому діапазоні для кількісних величин, таких, як вартість, тривалість, продуктивність, попит тощо;

- **Байєсова статистика і мережі Байєса** (Bayesian statistics and Bayes nets) – статистичний метод з використанням даних апріорного розподілу для оцінювання ймовірності результату, мережа Байєса є графічною моделлю, що являє собою змінні та їх імовірнісні взаємозв’язки;

- **криві FN** (FN curve, накопичені частоти) – графічне подання ймовірності подій, що викликають певний рівень небезпечних впливів для встановленої групи населення (відображають кількість жертв);

- **показники ризику** (Risk index) – підхід, що застосовується для ранжирування та порівняння ризиків на основі мір ризику, отриманих із застосуванням балових оцінок на основі порядкових шкал;

- **матриця «наслідок-імовірність»** або матриця наслідків і ймовірностей (Consequence/probability matrix) – засіб поєднання якісних або змішаних оцінок наслідків та ймовірностей, застосовується для визначення або ранжирування рівня ризику;

- **аналіз витрат і вигод** або аналіз ефективності витрат CBA (Cost/benefit analysis) – оцінка ризику в ситуації, коли необхідно порівняти очікувані витрати із загальними очікуваними вигодами і вибрати кращий або найбільш вигідний варіант рішення;

- **багатокритеріальне аналізування рішень** MCDA (Multiple criteria decision analysis) – ранжирування критеріїв для об'єктивної та прозорої оцінки різних варіантів рішень.

У табл. 3.2 наведені лише деякі основні методи оцінки ризиків зі вказівкою їх переваг та недоліків.

Таблиця 3.2 – Кількісні методи оцінки ризику

Метод	Переваги	Недоліки
Статистичний	Можливість моделювання сценаріїв, висока точність розрахунків, часткова стандартизація, нескладність математичних розрахунків	Необхідність великої кількості спостережень; ризик відповідності обраної моделі; високі витрати на інформатизацію та аналіз інформації
Розрахунково-аналітичний	Широке застосування, можливість об'єктивної оцінки за невисоких витрат	Суб'єктивізм оцінок, відсутність стандартів
Метод експертних оцінок	Невисока вартість; відсутність необхідності в точних початкових даних і дорогих програмних засобах, можливість здійснювати оцінку до розрахунку ефективності проєкту, простота розрахунку	Складність з отриманням фінансової оцінки ризику, висока залежність від суб'єктивної думки експертів; складність залучення незалежних експертів
«Дерево рішень»	Висока точність оцінки; детальний облік факторів ризику; можливість різних сценаріїв розвитку подій	Потребує багато часу на дослідження; високі витрати при великій кількості варіантів
Аналіз чутливості	Можливість за його допомогою вирішити проблему зіставлення впливу різних (натуральних, вартісних) характеристик проєкту, що варіюються.	Врахування одного чинника проєкту, що приводить до нестачі можливостей зв'язків між окремими чинниками або недообліку їхньої кореляції.
Аналіз сценаріїв	Можливий для різноманітних варіантів реалізації проєкту; застосування програмних засобів (можливість збільшити кількість можливих сценаріїв і таким чином значно підвищиться ефективність оцінки ризику)	Для високої цінності сценарію з метою прогнозування необхідний великий об'єм вихідної інформації; низька можливість реалізації точного прогнозування при кожному сценарію; потребує масштабних підготовчих робіт
Метод Монте-Карло	Дозволяє реалізувати моделі складних систем; можливість використання будь-яких розподілів; моделювання складної поведінки ринку.	Складність методу; необхідна велика кількість експериментальних даних необхідність потужних розрахунків; складність презентації.
Метод аналогій	Невисока вартість; простота розрахунку.	Невисока точність; проблематичність підбору аналогів; не враховується розвиток певного виду діяльності.

Метод оцінки ризику «краватка-метелик» BTA – один з найбільш наочних методів аналізу, що дозволяє показати зв'язок джерел ризику та наслідків його реалізації. Він полягає в тому, щоб на одній діаграмі відобразити ризик (як подію) та всі його джерела, можливі наслідки і інші пов'язані аспекти.

Основна перевага методу – наочність. Візуалізація причинно-наслідкових зв'язків ризикових подій дозволяє швидко пояснити будь-кому, що представляють собою ризики підприємства. У центрі діаграми розміщують небезпечну подію, яку вибирають для аналізу. Ліва частина діаграми слугує для визначення причин ризиків, права – для аналізу можливих наслідків, до яких вони можуть призвести. Таке розташування формує вигляд «метелика».

Це дуже потужний інструмент, коли керівник бере один з істотних ризиків і починає розкладати його в ліву сторону на можливі причини його настання, а в праву – на можливі наслідки (рис. 3.5). Після цього як причини, так і наслідки декомпозуються на такі рівні: підпричини і піднаслідки.

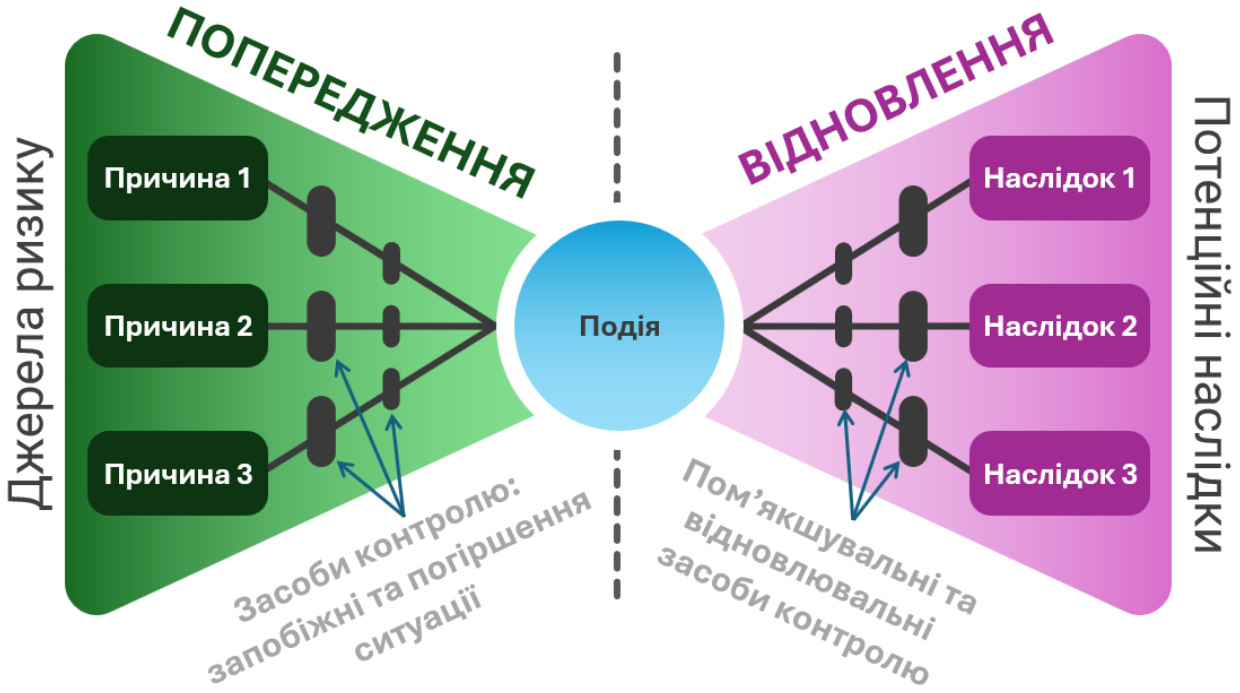


Рисунок 3.5 – Метод «краватка-метелик»

Даний метод частіше застосовують після експертної оцінки, і він зазвичай використовується тільки для тих ризиків, які потрапили в червону зону на карті ризиків.

Таким чином, метод «краватка-метелик» наочно представляє всі причини виникнення певного ризику і наслідки від його реалізації, що дає можливість визначити найбільш відповідну технологію управління їм.

Метод «краватка-метелик» слід будувати згідно з таким планом:

1. Визначення небезпечної події, обраної для аналізу, і відображення її в центральному елементі «краватки-метелика».

2. Складання переліку причин події за допомогою дослідження джерел ризику (або небезпеки).

3. Ідентифікація механізму розвитку небезпеки до критичної події.

4. Проведення ліній, які відокремлюють причини від події, що дозволяє сформувати лівий бік метелика. Додатково можуть бути ідентифіковані і включені в діаграму фактори, які можуть призвести до ескалації небезпечної події та її наслідків.

5. Нанесення поперек ліній перешкод, відповідних бар'єрам, які запобігають небажаним наслідкам. Якщо визначено фактори, які можуть спричиняти ескалацію небезпечної події, то додатково можуть бути подані бар'єри, що відвертають подібну ескалацію. Цей підхід може бути використаний для позитивних наслідків, коли перепони відображають засоби управління, що стимулюють появу і розвиток події.

6. Ідентифікація в правому боці метелика різних наслідків небезпечної події і проведення ліній, що з'єднують центральну подію з кожним можливим наслідком.

7. Зображення бар'єрів перешкод у напрямку до наслідку. Цей підхід може бути використаний для позитивних наслідків, коли перепони відображають засоби управління, що забезпечують появу сприятливих наслідків.

8. Відображення під діаграмою допоміжних функцій управління, що належать до засобів управління (таких, як навчання і перевірка), і поєднання їх із відповідним засобом управління.

Кількісну оцінку для аналізу «краватка-метелик» часто виконують за допомогою методів аналізу дерева несправностей FTA та аналізу дерева подій ETA.

Метод оцінки ризику «краватка-метелик» використовують у критичних для безпеки галузях, таких як авіація, хімічна промисловість, нафта і газ. Вони візуалізують потенційні причини та наслідки небезпечних подій і дозволяють висвітлити засоби запобігання та відновлення.

Професіонали з кібербезпеки можуть використовувати спрощені діаграми «краватки-метелика», щоб повідомити про ризики безпеки нетехнічну аудиторію, оскільки вони стисло відображають бізнес-наслідки та їхні причини на одному зображенні.

Наприклад, розглянемо спрощений сценарій розкриття конфіденційних даних, що може статися або через спробу фішингу (один з різновидів шахрайства в мережі Інтернет з метою отримання незаконного доступу до конфіденційних даних користувачів), або через атаку підміни облікових даних (наприклад, через шкідливе програмне забезпечення), що призводить до різноманітних бізнес-наслідків, починаючи від втрати коштів і закінчуючи репутаційною шкодою.

На рис. 3.6 наведено вигляд діаграми «краватки-метелика», додатково підписані потенційні запобіжні бар’єри та засоби контролю відновлення, які застосовуються до і після інциденту відповідно. До запобіжних засобів можна віднести дії з посилення безпеки, використання багатофакторної аутентифікації, підвищення рівня обізнаності користувачів за допомогою підготовчих курсів. Засоби контролю відновлення можуть містити дії по виявленню та реагуванню на випадки несанкціонованого доступу, його локалізації та відновленню після виявлення, аналіз причин виникнення ризикової ситуації та врахування їх у подальшій роботі.

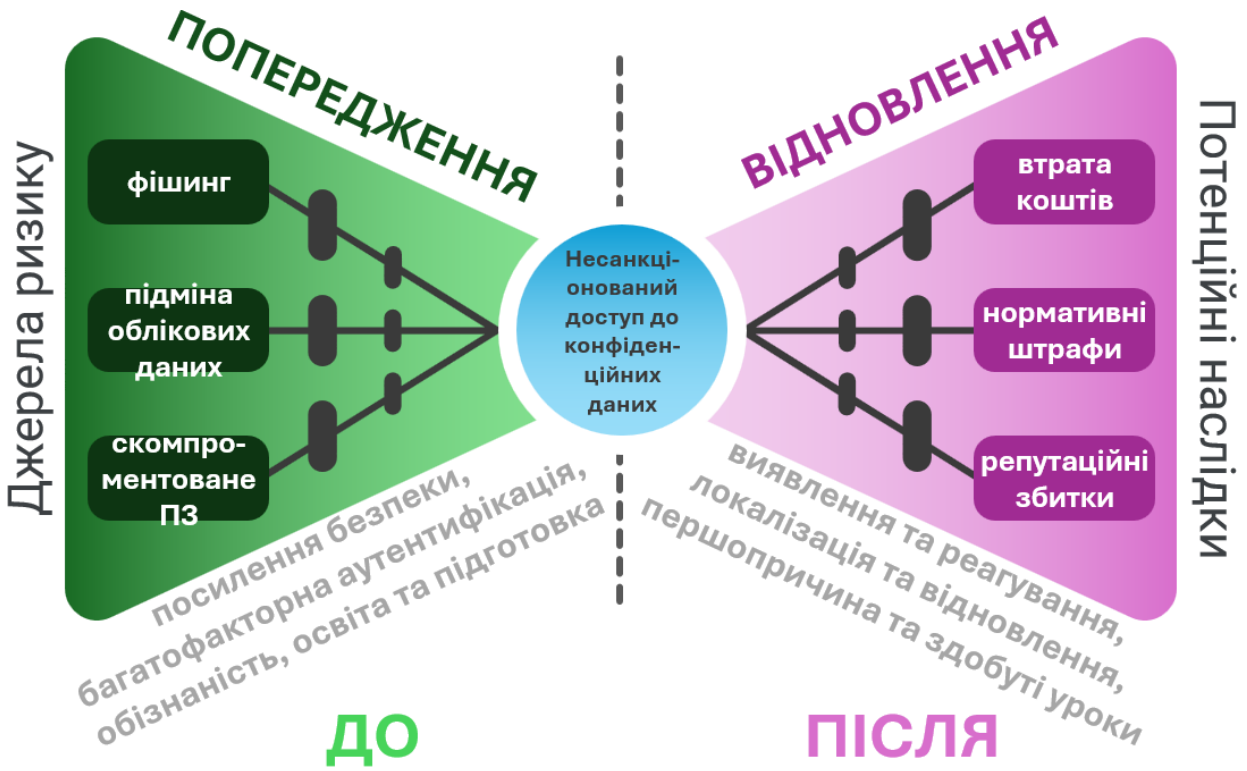


Рисунок. 3.6 – Аналіз ризику несанкціонованого доступу

Метод оцінки ризику «краватка-метелик» має ряд плюсів та мінусів у використанні.

Плюсами є:

- наочне, просте і ясне графічне подання ризику та його наслідків;

- орієнтація на засоби управління, спрямовані на попередження і/або зменшення наслідків небезпечних подій, і оцінку їхньої ефективності;

- може бути застосований щодо оцінки сприятливих наслідків;

- застосування не вимагає залучення висококваліфікованих експертів.

Мінусами є:

- не дозволяє відобразити сукупність причин, що виникають одночасно і мають особливі наслідки;

- може представити складні ситуації в надмірно спрощеному вигляді, особливо при застосуванні кількісної оцінки.

Аналіз причин і наслідків (діаграма Ісікава (Ishikawa) «риб'ячий скелет») – це графічний метод дослідження і визначення найбільш істотних та важливих причинно-наслідкових взаємозв'язків між факторами і наслідками ризикових подій.

Діаграма Ісікава являє собою графічне упорядкування факторів, що впливають на об'єкт аналізу. Вона дозволяє виявити взаємозв'язки між різними факторами і більш точно зрозуміти досліджуваний процес. Сприяє визначенню головних факторів, що мають найбільший вплив на розвиток проблеми, а також описує попередження або усунення дії таких факторів.

Проблема, яка досліджується, на діаграмі – це «голова риб'ячого скелету». «Хребет» на діаграмі умовно відображається у вигляді прямої горизонтальної стрілки. Причини і фактори, прямо і опосередковано впливають на проблему, зображуються похилими стрілками – це «кістки».

На діаграму Ісікава за направленням вліво наносять основні «кістки» (категорії), які мають відношення до проблеми. Для початку команда експертів може розглянути загальні категорії. Усі можливі причини зазвичай розподіляють за категоріями за принципом «5М»:

- Man (Людина) – причини, пов'язані з людським фактором;
- Machines (Машини, обладнання) – причини, пов'язані з обладнанням;
- Materials (Матеріали) – причини, пов'язані з матеріалами;
- Methods (Методи, технологія) – причини, пов'язані з технологією роботи, з організацією процесів;
- Measurements (Вимірювання) – причини, пов'язані з методами вимірювання.

Інші деякі можливі варіанти діаграм Ісікава, що найчастіше використовуються, будуються за принципами «5М & 1Е», «4S», «8Р» тощо.

Принцип «5М & 1Е» використовується в промисловості, яка займається виробництвом. Перші п'ять категорій співпадають з вищевказаними, додаткова категорія:

- Environment (Навколишнє середовище) – причини, пов’язані з впливом навколишнього середовища (температура, тиск, вологість тощо).

Принцип «4S» підходить для вирішення проблем у сфері послуг.

- Suppliers (Постачальники) – аналізується якість, надійність та ефективність постачальників, а також їхній вплив на якість обслуговування та задоволеність клієнтів;

- Scale (Масштаб) – враховується операційна ефективність, розподіл ресурсів і здатність підтримувати якість обслуговування на різних рівнях попиту;

- Surrounding (Середовище) – все, що може вплинути на надання послуг (місцезнаходження, демографічні дані клієнтів, економічні фактори тощо);

- Skill (Навички) – відсутність навичок може призвести до збоїв в обслуговуванні.

Принцип «8P» підходить для вирішення проблем у сфері маркетингу продукції:

- Price of the Product (ціна товару);

- Product specification (специфікація товару);

- Promotion or marketing strategy (просування або маркетингова стратегія);

- Place market (ринок збуту);

- Process (процес);

- People (personnel, trained manpower, stakeholders) (люди);

- Physical evidence (речові докази);

- Performance (виконання).

Основні категорії розподіляються в упорядкованому вигляді, починаючи з тієї категорії, яка має найбільшу ймовірність того, що її причини викликають проблему.

Для кожної категорії будуються додаткові «кістки», що представляють окремі причини, у них, у свою чергу, додаються свої підпричини. Продовжуючи таким чином, можна отримати розгалужене дерево, яке зв’язує

причини виникнення невідповідності, що знаходяться на різному рівні деталізації. Таким чином, можна досягти первинних причин, усунення яких найбільш сильно вплине на усунення всієї невідповідності. Загальний вигляд діаграми наведено на рис. 3.7.

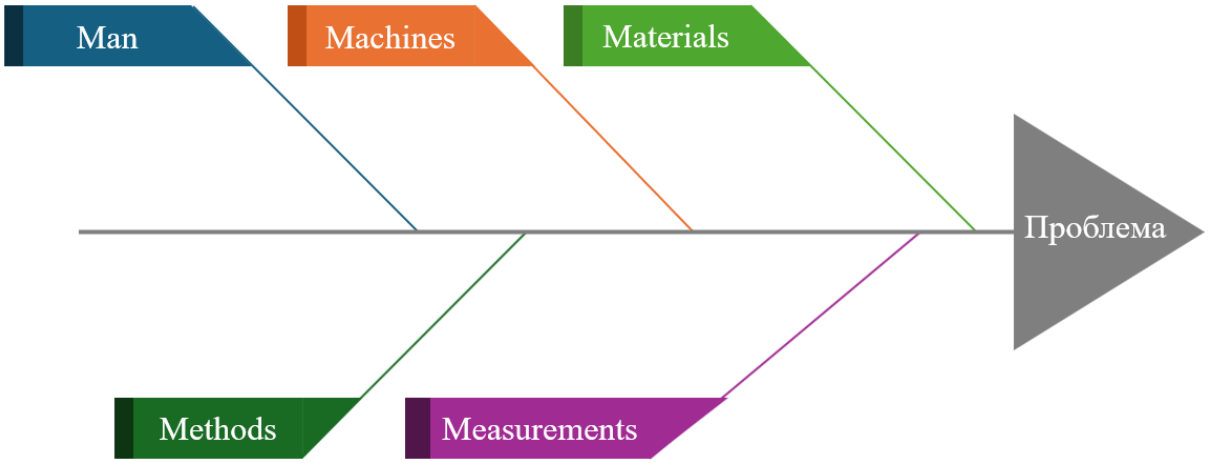


Рисунок 3.7. – Діаграма Ісікава 5М

Основними етапами аналізу причин та наслідків є:

- встановлення висновку, який необхідно проаналізувати, і розміщення його праворуч у відповідному блоці діаграми. Висновок може бути позитивним (мета) або негативним (проблема) залежно від обставин;

- визначення основних (головних) категорій причин і зазначення їх у відповідних блоках діаграми «риб'ячого скелета». Категорії визначають згідно з об'єктом дослідження;

- зазначення можливих причин для кожної основної (головної) категорії на гілках і відгалуженнях для опису взаємозв'язків між ними;

- продовження дослідження шляхом альтернативної постановки запитань «чому?» або «що це викликало?» для встановлення зв'язків між причинами;

- встановлення всіх гілок і відгалужень для перевірки послідовності і повноти виявлених причин, і визначення їх відношення до основного висновку;

- ідентифікація найбільш імовірних причин цього висновку на основі узгодженої думки робочої групи експертів і доступних об’єктивних свідчень.

Робота з самою діаграмою проводиться в кілька етапів:

1. Виявлення та збір всіх факторів і причин, що будь-яким чином впливають на досліджуваний результат.

2. Групування факторів за критеріями та причинно-наслідковими блоками.

3. Ранжирування факторів всередині кожного блоку.

4. Аналіз отриманої ситуації.

5. Виключення факторів, на які не можна впливати.

6. Ігнорування малозначущих і непринципових факторів.

Встановити всі виявлені причини неможливо, або невигідно.

Ключове завдання полягає в тому, щоб мати від трьох до шести основних критеріїв, які охоплюють всі можливі впливи ризику. Для цього експерти повинні виділити першопричини з маси можливих і ті наслідки невідповідності, яким потрібно виділити найбільшу увагу. Для ранжирування причин і оцінки тяжкості в подальшому зручно використовувати аналіз видів і наслідків відмов FMEA. Максимальна глибина такого дерева досягає 4-5 рівнів. Діаграма Ісікава використовується як аналітичний інструмент для перегляду дії можливих факторів і виділення найбільш важливих причин, дія яких породжує наслідки та піддається управлінню.

Наприклад, розглянемо спрощений аналіз ризику атаки програм-вимагачів з точки зору кібербезпеки.

Програми-вимагачі – це шкідливе програмне забезпечення, яке блокує комп’ютери або особисті файли користувачів, вимагаючи викуп за відновлення доступу. Головні категорії причин виникнення такого ризику – зовнішні загрози, проблеми управління, проблеми контролю/моніторингу доступу та проблеми людини/користувача. Для кожної головної причини формуються підпричини:

- зовнішні загрози – спамні та фішингові електронні листи, зловмисні вебсайти та рекламні оголошення, клікбейт-заголовки на вебсайтах;

- проблеми управління – ігнорування засобів безпеки обслуговуючим персоналом та обмеження фінансування питань безпеки;

- проблеми контролю/моніторингу доступу – використання слабких паролів, неналежне настроювання керування доступом, використання відкритого віддаленого доступу до робочих станцій за допомогою RDP (Remote Desktop Manager);

- проблеми людини/користувача – відсутність підготовки з питань кібербезпеки, слабкі навички у використанні комп'ютерної техніки та довірливість користувачів, неналежне зберігання паролів, що веде до втрати або викрадення облікових даних.

Діаграма Ісікава для такого випадку наведена на рис. 3.8.

Рисунок 3.8 – Приклад діаграми Ісікава для аналізу ризику атаки програм-вимагачів

Перевагами методу аналізу причин і наслідків є:

- залучення компетентних експертів до роботи групи;

- застосування структурованого аналізу;

- розгляд усіх ймовірних припущень і гіпотез;

- графічне відображення результатів у простій для сприйняття формі;

- визначення сфер, в яких потрібні додаткові дані;

- можливість встановлення факторів, які можуть викликати події, що розглядаються як для сприятливих, так і для небажаних результатів. Позитивний погляд на проблему може стимулювати більшу відповідальність і залучення учасників.

Метод має такі недоліки:

- група експертів може не мати необхідної компетентності;

- для розробки рекомендацій метод необхідно застосовувати тільки як частину аналізу першопричини;

- метод призначений для проведення мозкового штурму, а не самостійного аналізу;

- поділ причинних факторів на основні категорії на початку аналізу означає, що взаємозв'язки між категоріями причин можуть бути не розглянуті належно, наприклад, відмова обладнання, спричинена помилкою оператора, або помилки оператора через недоліки конструкції системи.

Аналіз впливу на бізнес BIA – це метод, що дозволяє вивчити, як різні види негативних подій можуть вплинути на основні напрямки діяльності і ключові бізнес-процеси підприємства. Він також дозволяє оцінити можливості підприємства щодо зменшення імовірності ризику.

Метод аналізу впливу на бізнес використовують при визначенні критичності процесів організації, часу їх відновлення і необхідних ресурсів (активи, персонал, навички, технології, виробничі площі та інформація) для забезпечення досягнення встановлених цілей, цей метод допомагає при визначенні взаємозв'язків між процесами.

Для цілей первинного збору інформації використовується анкетування та інтерв'ювання ключових співробітників підприємства. Для цього необхідні:

- група експертів – група аналізу та розробки плану безперервності бізнесу;

- цільові показники організації – інформація про цілі, навколишнє середовище, види діяльності та взаємозв'язки організації;

- детальний опис бізнес процесів – докладний опис видів діяльності та функціонування організації, що містять процеси, допоміжні ресурси, взаємозв'язки з іншими організаціями, угоди про аутсорсинг, причетні сторони;

- інформація про реалізацію ризиків – перелік можливих економічних та виробничих наслідків, що можуть бути спричинені порушенням критичних процесів;

- анкети – заздалегідь підготовлені анкети;

- список інтерв'юйованих – список опитуваних осіб у відповідних сферах діяльності організації та/або причетних сторін.

Етапи методу аналізу впливу на бізнес:

- ідентифікація критичних бізнес-процесів і ключових продуктів – визначення критичності ключових процесів та ключових видів продукції, робіт, послуг організації на основі оцінки для них небезпек, загроз і вразливостей;

- ідентифікація наслідків реалізації ризиків – визначення економічних і виробничих наслідків відмов/порушень/руйнувань ідентифікованих критичних процесів за певні періоди часу;

- визначення взаємозв'язків між внутрішніми і зовнішніми агентами – ідентифікація взаємозв'язків із ключовими внутрішніми і зовнішніми причетними сторонами. На цьому етапі може бути корисним складання карт взаємозв'язків у системі і в ланцюзі постачань;

- виявлення ресурсів забезпечення неперервності бізнесу – визначення наявних необхідних ресурсів для забезпечення безперервності робіт після відмов/порушень/руйнувань на мінімальному допустимому для організації рівні;

- розробка альтернативних способів діяльності – ідентифікація альтернативних способів виконання робіт і процесів, що існують, або запланованих до розробки. Альтернативні способи виконання робіт та процесів можуть бути застосовані в ситуації нестачі або відсутності необхідних ресурсів або можливостей під час відмов/порушень/руйнувань;

- визначення максимально допустимого періоду простою MTD (Maximum Tolerable Downtime) – визначається період часу, після закінчення якого існує загроза остаточної втрати життєздатності організації, якщо поставка продукції та/або надання послуг не будуть відновлені при відмовах/порушеннях/руйнуваннях. Визначення виконується для кожного процесу, заснованого на ідентифікованих наслідках і критичних факторах виконуваних видів діяльності;

- визначення цільового часу відновлення RTO (Recovery Time Objective) – це час, запланований для відновлення виробництва продукції та надання послуг після відмов/порушень/руйнування, відновлення діяльності організації і відновлення спеціалізованого обладнання, інформаційних технологій або інших активів. Визначення виконується для будь–якого спеціалізованого обладнання, інформаційних технологій та інших активів організації;

- визначення вимог щодо резервування процесів – встановлення рівня підготовленості критичних процесів для управління в умовах порушень, яке може містити оцінку рівня резервування процесу (наприклад, наявності запасного обладнання) або існування альтернативних постачальників.

У даному методі аналізу враховується кілька показників часу у випадку застосування резервного копіювання даних в інформаційних технологіях.

RTO – показник часу відновлення. Це час, необхідний відновлення даних після аварії. На цей показник впливає багато параметрів: кількість віртуальних машин або фізичних хостів, для яких створюються бекапи, програмне забезпечення, розмір дискових масивів та тип дисків, що використовуються для зберігання даних, майданчик зберігання бекапів.

А також місце точки оновлення в ланцюзі резервних копій. RTO враховує кроки, які IT-команда має зробити для повернення функціонування сервісів та даних. Якщо бізнес використовує сучасні системи, обладнання та резервує його, можна визначити цей показник у секундах.

WRT (Work Recovery Time) – час, протягом якого відбувається перевірка коректності відновлення, цілісності даних та підтверджується повне відновлення.

MTD (RTO+WRT) загальний період часу, протягом якого порушення роботи бізнес-процесу не призведуть до критичних для компанії наслідків.

RPO (Recovery Point Objective) – показник точки відновлення, проміжок часу між збереженими резервними копіями. Це максимальний час, протягом якого можуть бути втрачені дані в обсязі, не критичному для функціонування бізнесу. Наприклад, якщо цей параметр становить одну годину, то в разі аварії компанія відновить дані, створені лише за годину до її виникнення. Якщо створюється бекап кожні 24 години, то в найгіршому випадку буде втрачено всю нову інформацію за цей період. Слід враховувати цей момент при побудові бекап-плану. Сучасне програмне забезпечення дозволяє робити резервні копії з мінімальними проміжками часу, такі як п’ять хвилин.

Графічне подання показників часу наведено на рис. 3.9.

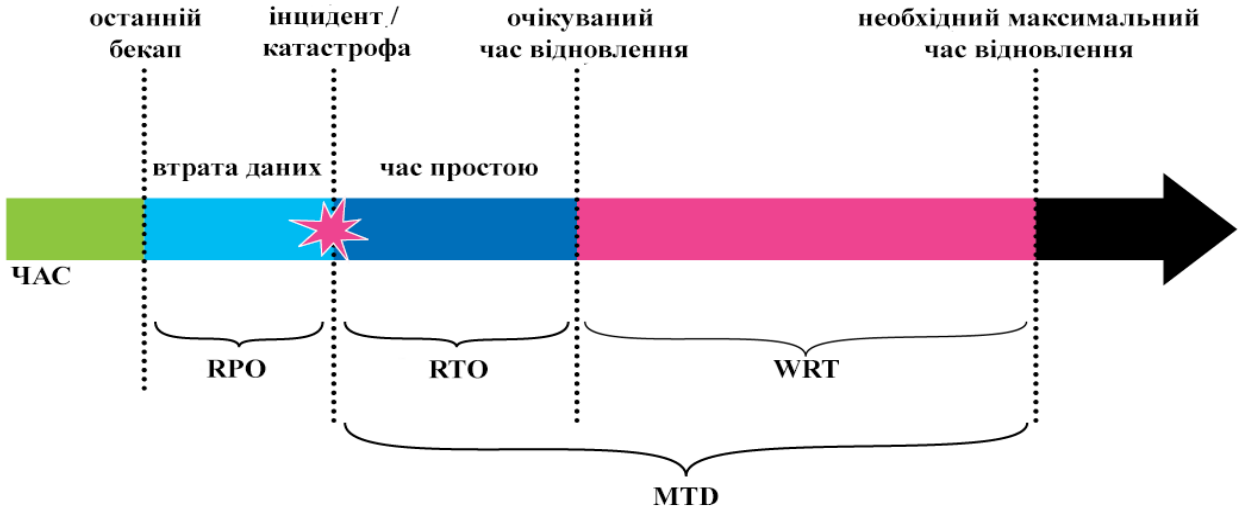


Рисунок 3.9 - Показники RPO, RTO, WRT, MTD

У табл. 3.3 наведено приклад класифікації програмного забезпечення та визначення допустимих показників RPO, RTO, MTD та частоти його перевірки.

Таблиця 3.3 – Приклад класифікації програмного забезпечення

Клас	Опис	RPO	RTO	MTD	Частота перевірки
Ключові сервіси	Програми, необхідні для відновлення або забезпечення функціонування бізнес-процесів (наприклад, мережа, операційні системи)	4 год.	<4 год.	<8 год.	6 міс.
Критично важливі програми	Програми чи послуги, які можуть серйозно вплинути на здоров'я людей або громадськість або завдати великої шкоди репутації організації, якщо вони недоступні.	4 год.	<4 год.	<8 год.	6 міс.
Критично важливо для бізнесу	Програми або послуги, які матимуть серйозний вплив на процеси організації/IT/OT, якщо їх немає.	8 год.	<48 год.	<60 год.	1 рік
Необхідно для бізнесу	Програми або служби, які безпосередньо підтримують основні функції	24 год.	>48 год.	<72 год.	2 роки
Підтримка бізнесу	Програми або сервіси, без яких виникнуть лише незручності; обробка може бути припинена на невизначений термін без істотного впливу.	24 год.	>48 год.	<80 год.	N/A

У результаті виконання аналізу впливу на бізнес отримуються такі дані:

– реєстр бізнес процесів організації – перелік ранжируваних за пріоритетами критичних процесів і відповідних взаємозалежностей;

– реєстр факторів реалізації ризиків та їх наслідків – зареєстровані економічні та виробничі впливи, викликані порушенням критичних процесів;

– реєстр ресурсів, необхідних для функціонування критичних процесів – допоміжні ресурси, необхідні для ідентифікованих критичних процесів;

– терміни простою і терміни відновлення – можливі терміни простою та відновлення критичних процесів і взаємопов’язаних інформаційних технологій.

Для подальшої роботи в інформаційній сфері створюють плани:

1. План безперервності бізнесу BCP (Business Continuity Plan) BCP – це методологія, яка дозволяє організації підтримувати роботу своїх ключових бізнес-функцій у разі кризи.

2. План аварійного відновлення DRP (Disaster Recovery Plan) – це набір процесів, які стосуються відновлення ваших інформаційних систем і операцій після того, як сталася руйнівна подія.

Простіше кажучи, коли трапляється аварійна ситуація, дії з забезпечення безперервності бізнесу і аварійного відновлення починаються одночасно – виконання BCP забезпечує роботу основних бізнес-функцій, тоді як дії за DRP дозволяють повернути роботу до нормального стану.

Зміст плану BCP для заходів кібербезпеки відповідає наведеним вище результатам аналізу впливу на бізнес. BCP має бути затверджений самою організацією, а зацікавлені сторони мають бути детально проінформовані. План також слід регулярно перевіряти.

Зміст плану DRP складається з таких розділів:

1. Опис розташування останніх проєктних документів, а також фізична копія їх останньої версії.

2. Опис та/або блок-схема системи – описується все, що потрібно відновити, і як це підключено до інших систем.

3. Екстрені контакти – дані контактів для відновлення системи. Це може бути як постачальник, так і системний інтегратор. Список контактів із іменами, номерами телефонів і адресами електронної пошти є важливим, щоб уникнути необхідності шукати номери телефонів під час спроби відновлення.

4. Склад групи аварійного відновлення – команда аварійного відновлення складається з ряду людей, завдання яких полягає в тому, щоб зосередитися на плануванні, реалізації, підтримці, перевірці та тестуванні

процедур організації для безперервності та відновлення бізнесу. Наявність команди, яка зосереджується на відновленні після катастроф, гарантує, що час реакції та збиток ресурсів буде зведено до мінімуму. Залежно від типу інциденту до команди включаються технічні спеціалісти, зовнішні (контрактні) сторони тощо, щоб забезпечити якнайшвидше виконання процесу відновлення та відновлення. Команда аварійного відновлення зазвичай складається з існуючих співробітників компанії, від IT-директора через IT-відділ до зацікавлених сторін у різних операційних підрозділах.

5. Розподіл ролей та обов'язків. Конкретні ролі, які можуть бути призначені в групі аварійного відновлення, такі:

- керівник групи відновлення – IT-директор, старший IT-менеджер або член команди виконавчого керівництва. Їхнє завдання – контролювати всю команду, координувати зусилля окремих членів і забезпечувати ефективність плану DRP;

- координатор кризового управління – співробітник, який контролює управління відновленням даних і ініціює процедури щоразу, коли виникає проблема чи катастрофа;

- експерт із забезпечення безперервності бізнесу – зосереджується на стратегії, необхідній для продовження або відновлення діяльності в разі аварії. Завдання також полягає в тому, щоб забезпечити відповідність планів DRP потребам бізнесу;

- консультанти з оцінки ефекту та відновлення – співробітники з різним досвідом у різних технологічних компонентах. Якщо трапляється катастрофа, вони відповідають за оцінку обсягу збитків в їхній конкретній області та методи відновлення. Прикладами сфер знань є мережі, сервери, сховища та бази даних;

- контролер IT-застосунків – відповідає за моніторинг усіх технологій на предмет потенційних аварій і забезпечення того, щоб усі окремі компоненти працювали разом, як тільки їх буде відновлено.

6. Опис відновлення працездатності техніки містить опис порядку, в якому необхідно виконати відновлення. Тут також описується, як системи можна повністю очистити. Описується як реалізується відновлення після того, як систему зламано або заражено вірусом; як відбувається відновлення, наприклад, після пожежі або пошкодження водою; як відбувається відновлення після збою локальної або глобальної мережі. Кожна процедура структурована таким чином:

- активація процедури;

- опис часу відновлення, залучених осіб і контактних даних;

- опис усіх уражених компонентів системи, включаючи комунікації, комп'ютери (клієнти та сервери), маршрутизатори тощо;

- опис організації процесу обміну повідомленнями між членами групи аварійного відновлення;

- деталі конструкції та налаштування системи, розташування резервних копій;

- опис процедури захисту і відновлення версій (відкат після змін);

- опис методу перевірки та підтвердження тестами після відновлення системи, перш ніж її можна буде повторно випустити;

- опис кроків проходження процедури відновлення;

- перегляд бази даних управління конфігураціями CMDB;

- оцінка виконаної процедури відновлення.

7. Опис місця розташування даних і резервних копій – вказується, які дані/програми потрібно відкотити (rolled back) та де зберігаються останні дані/програми. У певних середовищах, які за своєю природою мають відносно стабільну конфігурацію, можна виконати останнє резервне копіювання системи безпосередньо в DRP.

8. Опис процедури тестування та обслуговування – описується, як перевірити DRP, наприклад, в окремому середовищі, і як підтримувати DRP. Мета полягає в тому, щоб у разі збою оновлення за планом DRP виконувалося якомога швидше.

Переваги використання методу аналізу впливу на бізнес:

- забезпечується розуміння критичних процесів, що надає організації можливість досягнення встановлених цілей;

- є можливість оцінки необхідних ресурсів;

- є можливість перегляду виробничого процесу для підвищення стійкості організації.

До недоліків можна віднести:

- можливість недостатньої компетентності учасників опитування, інтерв'ю або нарад;

- зміни роботи в групі можуть вплинути на весь аналіз функціонування критичного процесу;

- можливість отримання спрощеної або занадто оптимістичної оцінки вимог до відновлення;

- процес досягнення адекватного рівня розуміння діяльності організації може бути досить складним.

Попередній аналіз небезпек PHA – аналітичний метод, націлений на ідентифікацію потенційних подій, можливих ситуацій і небезпек, які можуть завдати шкоди діяльності.

Метод PHA найчастіше застосовується на старті проєктів, коли інформації ще недостатньо через об'єктивні причини.

Інформація, отримана за методом попереднього аналізу може бути використана для розробки вимог до системи управління. Також даний метод оцінки ризику може використовуватися при аналізі наявних систем з метою ранжирування ризиків.

Для виконання попереднього аналізу небезпек використовуються:

- інформація щодо оцінюваної системі;

- доступні деталі проєкту системи.

Процес оцінки полягає у виконанні таких етапів:

- формування реєстру факторів ризику, ризиків та їх наслідків на основі даних про матеріали, що використовуються чи виготовляються, їх хімічної або іншої активності; переліку обладнання, що використовується; відомостей про робоче середовище; про схему розташування обладнання; відомостей про взаємодію компонентів системи тощо;

- для ідентифікації ризику і подальшої оцінки виконується одним з інших методів якісний аналіз наслідків небажаної події та їх ймовірностей;

- повторення методу на кожному етапі проєктування системи для виявлення нових небезпек і внесення необхідних змін;

- отримані результати можуть бути подані у вигляді таблиці або у вигляді «дерева».

Результатом виконання попереднього аналізу небезпек є:

- перелік небезпек і відповідних ризиків;

- рекомендації щодо прийняття ризику;

- рекомендовані засоби управління;

- вимоги до конструкції;

та/або

- запит на виконання більш детальної оцінки.

Однією з найбільших проблем у проведенні попереднього аналізу небезпек є суб'єктивність. Це може призвести до неузгодженості, що призведе до нестабільних результатів і забутих небезпек. Для запобігання цій та іншим проблемам сумісно з РНА використовуються:

- попередньо визначені **переліки контрольних запитань** (Checklist) ризиків, що допомагають систематично визначати потенційні ризики. Вони забезпечують повне охоплення, прискорюють ідентифікацію небезпек і сприяють узгодженості між проєктами та відділами;

- сеанси **мозкового штурму** (Brainstorming), в яких беруть участь різні експерти та зацікавлені сторони, вони використовують різноманітні знання та досвід, заохочуючи співпрацю та інновації;

- **дослідження небезпеки та працездатності HAZOP** – детально описують систему або процес, визначаючи потенційні відхилення, які можуть призвести до інцидентів безпеки. Оскільки це структурований підхід, розробники та інженери систематично перевіряють порушення та їхні наслідки;

- **аналіз видів і наслідків відмов FMEA**, який визначає точки відмов до їх виникнення та визначає пріоритетність ризиків, щоб команди могли зосередити ресурси на найбільш критичній області;

- **структурований метод «Що, якщо?» SWIFT**, який досліджує можливі сценарії та наслідки. Він є дуже доцільним, оскільки враховує широкий спектр небезпек, що дозволяє команді підготуватися до несподіванок.

До переваг методу попереднього аналізу небезпек відносяться:

- його можна використовувати в ситуації обмеженої інформації;

- він дозволяє досліджувати ризик на ранніх стадіях життєвого циклу системи.

Недоліки методу:

- метод надає тільки попередню інформацію;

- метод не є всебічним методом і не може забезпечити детальну інформацію про небезпечні події та способи їх запобігання.

3.3. Статистичні методи щодо оцінки ризиків на підприємстві

Необхідність проведення вимірювання ризику полягає у визначенні виправданого ризику. Ризик визнається виправданим, якщо мету, що була поставлена, не можна було досягти в даній обстановці дією (бездіяльністю), не поєднаною з ризиком, і особа, яка допустила ризик, обґрунтовано розраховувала, що вжиті нею заходи є достатніми для відвернення шкоди. Виправданий ризик – необхідний атрибут ефективного менеджменту. Відповідно постають запитання:

- що означає прийнятний (виправданий) ризик?

- де проходить межа, яка відділяє прийнятний ризик від неприйнятного?

Тому важливо визначити та оцінити результати настання ризику, причому спочатку оцінюють ймовірність того, що певна несприятлива подія відбудеться (ступінь), а потім – як це вплине на ситуацію (міру).

Чим досконалішими є методи кількісного вимірювання ризику, тим меншим стає чинник невизначеності.

Головні принципи кількісної оцінки ризику, яка ґрунтуються на широкому застосуванні апарату математичної статистики і теорії імовірності:

- передбачається стохастичний (випадковий) характер впливу ризикових факторів на діяльність (проєкт);

- для оцінки використовують абсолютні показники (які оцінюють міру ризику) і відносні показники (у вигляді коефіцієнтів);

- у проєктах, що мають аналоги, застосовуються методи математичної статистики (об'єктивні статистичні методи);

- в інноваційних проєктах, що не мають аналогів, використовується апарат теорії імовірності, що дозволяє моделювати майбутню діяльність (суб'єктивні статистичні методи);

- при цьому враховуються заходи щодо зниження ризиків і оцінюється їхня ефективність (вплив на результат);

- оскільки існує безліч факторів, що впливають на проєкт – повний їх аналіз неможливий, тому спрощують та розглядають лише найбільш загрозливі.

Статистичні методи оцінювання ризику ґрунтуються на певних припущеннях:

- їх використання передбачає, що ймовірності для всіх варіантів відомі або можуть бути точно визначені;

- у деяких випадках розподіл ймовірностей може бути заданий з високим ступенем достовірності на основі аналізу минулого досвіду при наявності великих обсягів фактичних статистичних даних.

Часто такі дані недоступні, тому розподіл визначається виходячи з припущень експертів, тоді імовірнісні оцінки несуть у собі велику частку суб'єктивізму.

Статистичні методи оцінки рівня ризику ґрунтуються на розрахунку рівня ризику за допомогою використання різних статистичних показників. Ця методика актуальна в застосуванні, якщо ситуації чи події відбуваються часто, і вони одночасні, тобто для реалізації цього методу потрібна наявність об'ємної кількості статистичних даних. Ця методика кількісного аналізу рівня ризику має свої переваги та недоліки. Перевагами є можливість застосування одного підходу при врахуванні різних факторів ризику та оцінки різних варіантів розвитку подій, а недоліками є необхідність застосування в розрахунках імовірнісних характеристик, а також важливість великого обсягу кількісних даних.

Багато основних ідей статистичної теорії рішень були розроблені Нейманом і Пірсоном у 1933 році. Систематична теорія для ситуації, коли немає апріорного розподілу, розвивалася Вальдом та було їм викладено відомі статистичні завдання мовою теорії прийняття рішень. У 1951 році Гіршик та Севідж продовжили дослідження Вальда в галузі теорії прийняття рішень. Фон Нейман та Моргенштерн розвинули аксіоматичний підхід до суб'єктивних корисностей у зв'язку з їхніми роботами з теорії ігор. На початку 1960-х років теоретичний інтерес перемістився до байєсівської теорії рішення, в якій суб'єктивні апріорні розподіли та корисності є основою системи та доказів.

Подальший розвиток цієї групи методів – розробка широко використовуваного методу «дерева рішень». Даний метод застосовується для оцінки ризиків тих рішень, які мають доступну для огляду кількість варіантів розвитку. При цьому, для побудови «дерева» аналітик повинен мати необхідну та достовірну інформацію з урахуванням ймовірності та часу настання різних сценаріїв проєкту. Послідовність збору даних для побудови «дерева рішень» можна подати таким чином: визначення складу та

тривалості фаз життєвого циклу проєкту, ключових подій; формулювання всіх можливих рішень; визначення ймовірності прийняття кожного рішення та вартості кожного етапу здійснення проєкту. З отриманих даних будується «дерево рішень», до складу якого включаються вузли роботи з реалізації проєкту.

Основними показниками, що використовуються під час статистичного аналізу та оцінки ризикових подій, є математичне очікування, показники мінливості (коливання) очікуваного результату, а також коефіцієнт кореляції [11, 15].

Для статистичних методів оцінки ризиків прийняті такі математичні припущення:

- якщо при прийнятті рішення орієнтуються на максимальне значення показника X, то вважають, що він має позитивний інгредієнт. Для цих випадків записують, що

$$X = X^{+};$$

- якщо ж під час прийняття рішень орієнтуються на мінімальне значення показника X, то вважають, що він має негативний інгредієнт. У цій ситуації пишуть, що

$$X = X^{-}.$$

Показник X є дискретною величиною, що має нормальний розподіл (щільність імовірності розподілу величини має нормальний характер, як наведено на рис. 3.10):

$$p(x < X') = \frac{1}{\sigma\sqrt{2\pi}} \int_{-3\sigma}^{X'} e^{-\frac{(x-M_0)^2}{2\sigma^2}} dx.$$

Імовірність найбільш очікуваного результату оцінюється приблизно в 50 %; якщо розрахунковий результат перевищує найбільш імовірний, ступінь ризику даної діяльності перевищує 50 %; якщо розрахунковий результат є нижчим найбільш імовірного, ступінь ризику становить менше 50 %.

Рисунок 3.10 – Щільність ймовірності розподілу випадкової величини (нормальний розподіл)

Для визначення області ризику та його рівня пропонується застосовувати емпіричну шкалу ризику у випадку використання як кількісної оцінки ризику ймовірності настання ризикової події. Варіант подібної емпіричної шкали наведено в табл. 3.4.

Таблиця 3.4 – Емпірична шкала вимірювання ризику

Області ризику	Градації ризику	Ймовірність небажаного результату	
Нормальна	Мінімальний	0-0.1	0-25 %
	Малий	0.1-0.3	
	Середній	0.3 -0.4	
Висока		0.4-0.6	25-50 %
Максимальна		0.6-0.8	50-75 %
Критична		0.8-1.0	75-100 %

Проте оцінка величини ризику за поданою емпіричною шкалою досить умовна, оскільки в оцінці ризику відіграє велику роль не тільки ймовірність, з якою може стати наявним збиток, а й сама величина збитку. Наприклад, збиток в одну грошову одиницю і в мільйон грошових одиниць, що відбувся з однаковою імовірністю, оцінюється підприємцем як зовсім різний ризик.

Основними параметрами, що характеризують нормальний розподіл, є математичне очікування $M(X)$ та середньоквадратичне відхилення $\sigma(X)$, а також показники, розраховані на їх основі. Будь-яке співвідношення $M(X)$ та $\sigma(X)$ піддається нормуванню, що дозволяє використовувати таблиці стандартного нормального розподілу до розрахунків імовірності ризиків.

Для оцінки величини ризику використовують статистичні параметри, перераховані в табл. 3.5.

Таблиця 3.5 – Статистичні параметри оцінки величини ризику

Параметр	Опис	Примітка
X	Випадкова величина.	Ризиковий параметр.
$M(X)$	Математичне очікування (очікування) випадкової величини X.	Значення величини події, яка пов'язана з невизначеною ситуацією.
$Mo(X)$	Модальне значення випадкової величини X	Відповідно до правила модального значення можуть враховуватись ті результати, ймовірність появи яких максимальна.
$D(X)$	Дисперсія (варіація) випадкової величини X.	Характеризує абсолютне коливання частоти ризику.
$\sigma(X)$	Середньоквадратичне (стандартне) відхилення випадкової величини X від її очікуваного значення.	Характеризує абсолютне коливання частоти ризику.
$V(X)$	Коефіцієнт варіації випадкової величини X.	Чим більший коефіцієнт варіації, тим сильніша коливність величини, що варіюється, відносно середньої величини і тим більший ризик.
$SV(X)$	Коефіцієнт семіваріації випадкової величини X.	Чим більша позитивна семіваріація, тим більший очікуваний від варіанта вирішення прибуток. Чим менша від'ємна семіваріація, тим менші прогнозовані збитки від варіанта вирішення.
$SSV(X)$	Семіквадратичне відхилення випадкової величини X від її очікуваного значення.	Показує абсолютне розсіювання, на якому знаходяться значення прибутку, більшого від математичного очікування. Чим більше значення показника, тим у більшому розмірі може вийти абсолютне значення фактичного очікуваного прибутку.
$As(X)$	Коефіцієнт асиметрії випадкової величини X.	Використовується у випадку несиметричного розподілу випадкової величини X.
$Ex(X)$	Коефіцієнт ексцесу випадкової величини X.	Використовується для порівняння проєктів з майже однаковими значеннями.

Очікуване значення випадкової величини X визначається через функцію математичного очікування. Середнє очікуване значення вимірює результат, який очікується в середньому. Імовірнісний зміст математичного очікування конкретного параметра від проведення підприємницької діяльності полягає в тому, що воно приблизно дорівнює середньоарифметичному всіх його можливих значень.

Математичне очікування оцінює міру (величину) ризику.

Якщо відомі всі можливі значення випадкової величини $X = \{x_1; x_2; \dots; x_n\}$ та ймовірності їх настання $P = \{p_1; p_2; \dots; p_n\}$, $\sum_{i=1}^{n} p_i = 1$, то для визначення очікуваного значення випадкової величини використовується середньозважена величина (очікуване значення, математичне очікування):

$$W = M(X) = \sum_{i=1}^{n} p_i \, x_i.$$

Якщо обирається альтернатива діяльності (проєкту) з декількох, то орієнтуються на ту, що має найбільші очікувані грошові надходження або найменші витрати.

Але математичне очікування $M(X)$ є кількісною характеристикою і саме по собі воно не дозволяє прийняти рішення на користь будь-якого варіанта.

У випадку, коли випадкова величина X має асиметричний розподіл ймовірностей, як оцінку ступеня ризику можна використовувати модальне значення цієї випадкової величини:

$$W = Mo(X)$$

Для дискретної випадкової величини мода (модальне значення) – це найбільш ймовірне значення випадкової величини (те, що зустрічається найчастіше). Для неперервної випадкової величини мода – це точка максимуму функції щільності розподілу ймовірності значень випадкової величини.

При одиничному виборі видається розумним припускати, що саме подія, що має максимальну ймовірність появи, і настане. Такий підхід у більшості випадків призводитиме до позитивного результату. Однак він має певні недоліки. Наприклад, він стикається з труднощами, коли:

- ряд станів мають рівну ймовірність появи;

- максимальний результат дають кілька альтернатив;

- ймовірність появи модального значення при одному зі станів середовища лише трохи вище, ніж для інших станів середовища, при цьому інші альтернативи виявляються більш оптимальними, іноді суттєво.

Як величина ризику в абсолютному вираженні часто використовується міра розсіювання значень показника відносно центра групування цих значень (міра мінливості або міра нестабільності). В якості центра групування значень показника використовується його математичне очікування або мода. Очевидно, що більші значення цих оцінок свідчать про більшу нестабільність відповідної діяльності (проєкту). Якщо центром групування значень показника є математичне очікування $M(X)$, то мірою ризику є середньозважене модуля відхилення цього показника від свого математичного очікування:

$$W = M(|X - M(X)|) = \sum_{i=1}^{n} p_i \, |x_i - M(X)|.$$

А якщо центром групування значень показника використовується мода $Mo(X)$, то мірою ризику є середньозважене модуля відхилення цього показника від модального значення:

$$W = M(|X - Mo(X)|) = \sum_{i=1}^{n} p_i \, |x_i - Mo(X)|.$$

Дисперсією $D(X)$ випадкової величини X є зважена щодо ймовірності величина квадратів відхилення випадкової величини X від її математичного очікування $M(X)$. Дисперсія характеризує міру розсіяння випадкової величини X навколо $M(X)$ і обчислюється за формулою

$$D(X) = \sum_{i=1}^{n} p_i\big(x_i - M(X)\big)^2 = \sum_{i=1}^{n} p_i {x_i}^2 - M(X)^2.$$

Вона вимірюється в квадратах одиниці виміру випадкової величини X і відображає площу її розсіювання. Чим більша дисперсія, тим вищий ризик, властивий стратегії.

Середньоквадратичне відхилення $\sigma(X)$ – це квадратний корінь з дисперсії. Чим менша величина середньоквадратичного відхилення, тим надійніша стратегія.

Середньоквадратичне (стандартне) відхилення $\sigma(X)$ є найбільш поширеним показником, що характеризує міру розсіювання випадкової величини X навколо математичного очікування і обчислюється за формулою:

$$\sigma(X) = \sqrt{D(X)}.$$

Середньоквадратичне відхилення відображає діапазон розкиду значень випадкової величини X і в теорії ризику вважається мірою невизначеності. Вимірюється в тих самих одиницях, що й випадкова величина X. Графічна інтерпретація $\sigma(X)$ наведена на рис. 3.11.

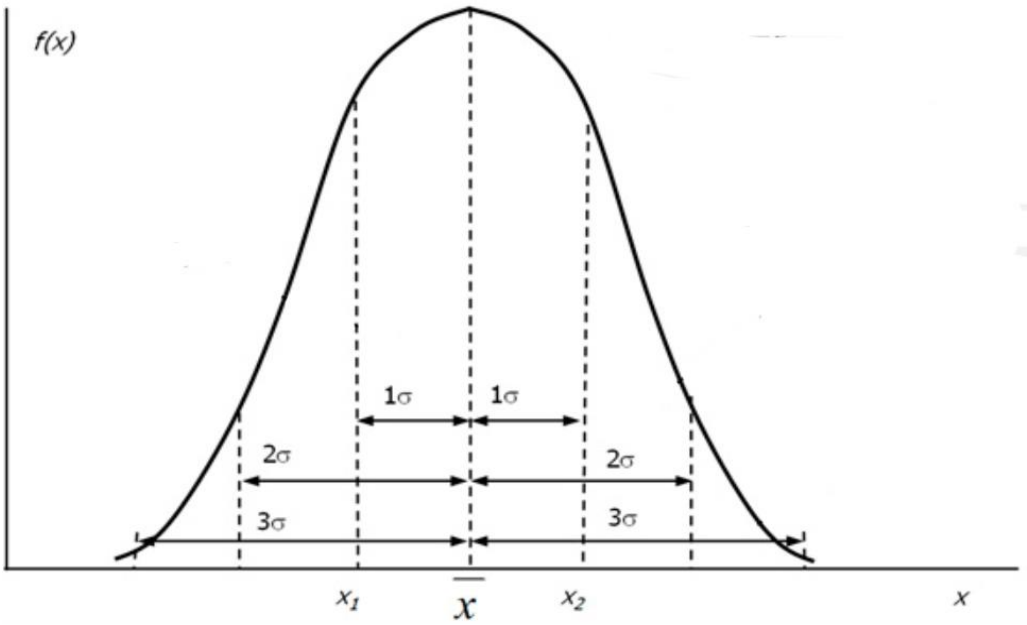


Рисунок 3.11 - Середньоквадратичне відхилення $\sigma(X)$

Підхід до оцінки ризику, що спирається на дисперсію $D(X)$ чи середньоквадратичне відхилення $\sigma(X)$, вважається класичним. Причому, чим більшими будуть ці величини, тим більшим буде ступінь ризику, пов'язаного з певною стратегією, тобто величина ризику:

$$W = D(X) \text{ або } W = \sigma(X).$$

Слід мати на увазі, що при класичному визначенні міри ризику однаково трактуються як додатні, так і від'ємні відхилення величини реального ефекту від сподіваної величини, тобто виконується гіпотеза про те, що коливання випадкової величини X в обидві сторони однаково небажані. Але в ряді випадків це не так. Якщо випадкова величина X відображає прибутки і оцінка прибутку є меншою від сподіваної величини прибутку, то це є ознакою несприятливої ситуації. У той же час додатне відхилення вказує на те, що реалізація випадкової величини (прибутку) є більшою, ніж сподівана величина, і це є, очевидно, кращою, тобто сприятливою ситуацією.

У теорії економічного ризику виходять з того, що ризик пов'язаний лише з несприятливими ефектами і для його оцінювання достатньо брати до уваги лише несприятливі відхилення від очікуваної величини.

При цьому в якості міри ризику використовується семіваріація $SV(X)$, яка розраховується шляхом вимірювання дисперсії всіх спостережень, що випадають нижче середнього або цільового значення набору даних. Формула для обчислення семіваріації:

$$SV(X) = \frac{1}{P^-}\sum_{i=1}^{n} \alpha_i p_i \left(x_i - M(X)\right)^2,$$

$$P^- = \sum_{i=1}^{n} \alpha_i p_i,$$

$$\alpha_i = \begin{cases} 0, \text{ у випадку сприятливого відхилення} \\ 1, \text{ у випадку несприятливого відхилення.} \end{cases}$$

Якщо ж, наприклад, $X = \{x_1; x_2; \dots; x_n\}$ відображає можливі варіанти збитків ($X = X^-$, тобто має негативний інгредієнт), то

$$\alpha_i = \begin{cases} 0, \text{при } x_i \le M(X^-) \\ 1, \text{при } x_i > M(X^-) \end{cases}; \quad i = \overline{1,n}.$$

З практичної точки зору зручніше (приймаючи до уваги вимірність величин) застосовувати семіквадратичне відхилення $SSV(X)$:

$$SSV(X) = \sqrt{SV(X)}.$$

Менше значення коефіцієнта семіваріації указує на менший ступінь ризиковості.

У випадках, коли випадкова величина X є ланцюговою величиною (розрахованою по відношенню до свого попереднього значення) і являє собою показник динаміки, для оцінки ризику можна використовувати середньогеометричне значення:

$$W = G(X^-).$$

Якщо X є дискретною випадковою величиною, тобто $X = \{x_1; x_2; \dots; x_n\}$, то:

$$G(X) = e^{M(\ln X)} = \prod_{i=1}^{n} x_i^{p_i}.$$

Якщо ж при цьому $p_1 = p_2 = \cdots = p_n = \frac{1}{n}$, то:

$$G(X) = \prod_{i=1}^{n} x_i^{1/n} = \sqrt[n]{\prod_{i=1}^{n} x_i}.$$

Для оцінки ризику можна використовувати також середньоквадратичне відхилення від зваженого середньогеометричного:

$$\sigma G(X) = \sqrt{\sum_{i=1}^{n} p_i \big(x_i - G(X)\big)^2}.$$

або ж оцінку цієї величини на основі дискретних даних (T – кількість періодів):

$$\sigma G(X) = \sqrt{\frac{1}{T}\sum_{t=1}^{T}\left(x_t - G(X)\right)^2}.$$

З точки зору неокласичного підходу до оцінки ризику доцільним є впровадження такого показника ступеня ризику, як семіквадратичне відхилення від зваженого середньогеометричного випадкової величини:

$$SSG(X) = \sqrt{SG(X)} = \sqrt{\sum_{i=1}^{n}\alpha_i p_i\left(x_i - G(X)\right)^2},$$

де $SG(X)$ – величина семіваріації по відношенню до зваженого середньогеометричного; $SSG(X)$ – семіквадратичне відхилення; α_i – індикатор i-го несприятливого відхилення.

У відносному вираженні ризик визначається як величина збитків (міра мінливості результату), віднесена до певної бази. За базу приймають зазвичай очікуваний результат. Відносне (середнє) лінійне відхилення випадкової величини X оцінюють за допомогою стандартного відхилення (коефіцієнта варіації) – часто його називають уніфікованим ризиком:

$$V(X) = \frac{\sigma(X)}{M(X)}.$$

Коефіцієнт варіації $V(X)$ є безрозмірною величиною, тому використовується, для порівняння проєктів з різними очікуваними результатами і ризиком: чим вищим є коефіцієнт, тим більший ризик.

Коефіцієнт варіації $V(X)$ використовується тоді, коли для двох альтернативних проєктів А і В виявиться, що $M(X_A) > M(X_B)$ та $\sigma(X_A) > \sigma(X_B)$ (або $M(X_A) < M(X_B)$ та $\sigma(X_A) < \sigma(X_B)$). Перевага надається тому проєкту, для якого є меншим коефіцієнт варіації. Коефіцієнт варіації як безрозмірна величина, дає можливість порівнювати результати двох проєктів в абсолютному вираженні непорівнянних, тобто таких, результати яких оцінюються різними найменуваннями. Наприклад, в одному випадку – кілограмами, в іншому – штуками.

У деяких випадках важливо визначити ситуації, коли ймовірність та величина позитивного (або негативного) результату набагато більша, ніж протилежний результат. Розуміння несиметричного ризику має вирішальне значення для прийняття правильних рішень. Можливість ідентифікувати асиметричний ризик допомагає уникнути потенційно небезпечних ситуацій, де не вистачає місця для помилок.

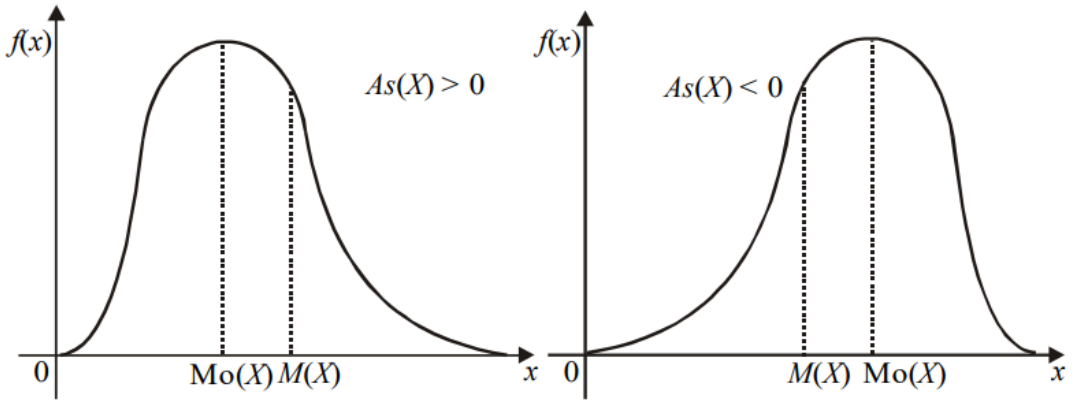
У випадку несиметричного розподілу випадкової величини X для оцінки ризику додатково використовують коефіцієнт асиметрії – величину, що характеризує асиметрію розподілу випадкової величини:

$$As(X) = \sum_{i=1}^{n} p_i \left(\frac{x_i - M(X)}{\sigma(X)} \right)^3 .$$

Якщо наявна статистична інформація щодо значень випадкової величини X за T періодів, коефіцієнт асиметрії обчислюють так:

$$As(X) = \frac{1}{T} \sum_{t=1}^{T} \left(\frac{x_t - M(X)}{\sigma(X)} \right)^3 .$$

Геометрична інтерпретація коефіцієнта асиметрії наведена на рис. 3.12.



а) б)

Рисунок 3.12 – Щільність розподілу ймовірностей у випадках $As(X) > 0$ (а), $As(X) < 0$ (б)

Коли $As(X) = 0$, то графік функції щільності ймовірності для випадкової величини X буде симетричним відносно $M(X)$. Несприятливі відхилення від сподіваного значення зазвичай знаходяться ліворуч у

близькості зі сподіваним значенням, а інші (сприятливі) – є досить віддаленими від сподіваної величини (такі значення показників, або «хвіст», розташовуються праворуч).

Якщо аналіз кількох проєктів свідчить, що їх показники ризику мають майже однакові очікувані значення, то для порівняння ризиків цих проєктів можна використати коефіцієнт ексцесу, що відображає концентрацію значень випадкової величини X навколо її очікуваного значення:

$$Ex(X) = \sum_{i=1}^{n} p_i \left(\frac{x_i - M(X)}{\sigma(X)}\right)^4 - 3.$$

Статистична оцінка коефіцієнта ексцесу (T – кількість періодів):

$$Ex(X) = \frac{1}{T}\sum_{t=1}^{T} \left(\frac{x_t - M(X)}{\sigma(X)}\right)^4 - 3,$$

$$Ex\left(X_{k_0}\right) = \max_{k=1,\dots,m} Ex(X_k).$$

Чим більший коефіцієнт ексцесу $Ex(X)$ тим більше є гостровершинним графік функції розподілу випадкової величини X, а отже менше значення ризику, і навпаки – чим більше є плосковершинним графік функції розподілу випадкової величини X, тим більше ризик.

Повертаючись до дисперсії як міри ризику, треба зазначити, що дисперсія, звичайно, не повністю характеризує ступінь ризику. Нерівність Чебишева дає оцінку ймовірності, що випадкова величина X прийме значення, далеке від свого очікуваного значення: ймовірність того, що випадкова величина X відхиляється від свого математичного очікування $M(X)$ більше ніж на заданий допуск ε, не перевершує її дисперсії $D(X)$, поділеної на ε^2:

$$P(|X - M(X)| < \varepsilon) \geq 1 - \frac{D(X)}{\varepsilon^2},$$

$$P(|X - M(X)| \geq \varepsilon) \leq \frac{D(X)}{\varepsilon^2}.$$

Нерівність Чебишева відображає, з якою імовірністю значення випадкової величини X будуть розміщуватися всередині ε-кола математичного очікування $M(X)$ та показує, що незначному ризику за середньоквадратичним відхиленням відповідає малий ризик і за лінійними відхиленнями.

Коефіцієнт Z оцінює ймовірність того, що результат діяльності виявиться не гірше якогось заздалегідь визначеного критичного рівня:

$$Z(X) = \frac{|M(X) - x_e|}{\sigma(X)},$$

де x_e – критичне значення випадкової величини X; задається: $x_e < X$, якщо є зацікавленість у максимізації випадкової величини X; $x_e > X$, якщо є зацікавленість у мінімізації випадкової величини X.

Коефіцієнт очікуваних збитків $K(Z)$ враховує відношення обсягу очікуваних збитків до суми очікуваних вигод та очікуваних збитків:

$$K(Z) = \frac{|M(Z^-)|}{|M(Z^-)| + |M(Z^+)|},$$

де Z – заплановане значення економічного показника X; $M(Z^-)$ – очікувана величина сприятливих відхилень X щодо Z; $M(Z^+)$ – очікувана величина несприятливих відхилень X щодо Z.

Формально $M(Z^-)$ та $M(Z^+)$ – це умовні математичні очікування відхилень X щодо Z, тобто

$$M(Z^-) = M(X - Z), X \in X(Z^-),$$
$$M(Z^+) = M(X - Z), X \in X(Z^+),$$
$$X = X(Z^+) \cup X(Z^-),$$

де $X(Z^-)$ – множина сприятливих значень X щодо Z; $X(Z^+)$ – множина його несприятливих значень.

В якості показників чутливості об’єкта (проєкту) щодо зміни тих чи інших чинників слід використовувати показники еластичності. Еластичність – це міра реагування однієї змінної величини (функції) на зміну іншої (аргумента).

Еластичність коефіцієнту очікуваних збитків $K(Z)$ відображає як змінюється ризик (у вигляді коефіцієнта очікуваних збитків $K(Z)$) при зміні планового значення Z; розраховується в дольовому або відсотковому вираженні:

$$e_Z \approx \frac{Z}{K(Z)} \cdot \frac{\Delta K(Z)}{\Delta Z}$$

Величина еластичності e_Z дає змогу визначити відсоткову зміну функції в результаті одновідсоткової зміни аргумента Z.

Перевага такого показника, як еластичність коефіцієнту очікуваних збитків $K(Z)$, перед іншими полягає в тому, що його величина не залежить від вибору одиниць вимірювання різних чинників.

Коефіцієнт ризику – співвідношення можливих втрат до розміру коштів підприємства:

$$W = \frac{x}{K},$$

де W – коефіцієнт ризику; x – максимально можливий обсяг збитків (грошових одиниць); K – обсяг власних фінансових ресурсів.

Аналіз ризику можна здійснювати з точки зору можливих (ймовірних) збитків, що є характерними для будь-якого об’єкта (проєкту). Для здійснення цього аналізу вводиться поняття областей (зон) ризику. Кожна з областей ризику характеризується різними значеннями коефіцієнта ризику (рис. 3.13):

1. Безризикова зона – це така область, в якій ймовірність виникнення збитків відсутня. У ній спостерігаються нульові збитки або прибуток, що перевищує очікувані значення.

2. Зона допустимого ризику – це область, де діяльність зберігає свою доцільність. Випадкові збитки тут можливі, але їх розмір менший за очікуваний прибуток.

3. Зона критичного ризику – це область, в якій ймовірність збитків може перевищити очікуваний прибуток і навіть досягти повного рівня

доходу від діяльності. У цій зоні збитки можуть бути настільки великими, що привести до втрати всіх вкладених коштів.

4. Зона катастрофічного ризику – це область, де можливі збитки настільки великі, що вони можуть перевищити критичний рівень і навіть дорівнювати повному майновому стану організації. Катастрофічний ризик може призвести до банкрутства, закриття підприємства та розпродажу його активів, а також до серйозної загрози для життя чи екології.

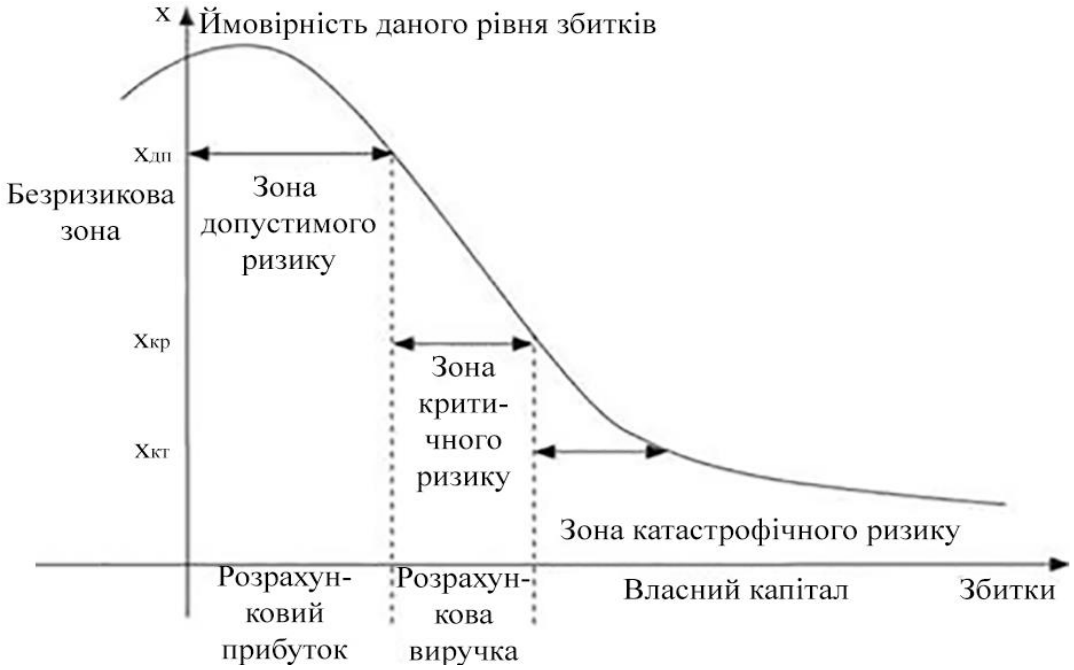


Рисунок 3.13 – Крива ймовірності рівня втрат за зонами ризику

Показник допустимого ризику: $W_{\text{дп}} = W(x_{\text{дп}}) = P(X \geq x_{\text{дп}})$, тобто $W_{\text{дп}}$ – це ймовірність того, що збитки виявляться більшими, ніж їх гранично допустимий рівень $x_{\text{дп}}$.

Показник критичного ризику: $W_{\text{кр}} = W(x_{\text{кр}}) = P(X \geq x_{\text{кр}})$, тобто $W_{\text{кр}}$ – це ймовірність того, що збитки виявляться більшими, ніж їх гранично допустимий критичний рівень $x_{\text{кр}}$.

Показник катастрофічного ризику: $W_{\text{кт}} = W(x_{\text{кт}}) = P(X \geq x_{\text{кт}})$, тобто $W_{\text{кт}}$ – це ймовірність того, що збитки виявляться більшими, ніж їх гранично допустимий катастрофічний рівень $x_{\text{кт}}$.

Знання цих показників дозволяє сформулювати висновки щодо можливості прийняття рішення стосовно здійснення певної діяльності. Однак для остаточного ухвалення рішення недостатньо лише цих значень – необхідно також визначити їх граничні значення, аби уникнути потрапляння в зону неприйнятного ризику. Ці граничні значення називаються критеріями допустимого, критичного та катастрофічного ризику – $k_{\text{дп}}$, $k_{\text{кр}}$, $k_{\text{кт}}$. Отже, маючи дані про три показники ризику та критерії граничного ризику, можна сформулювати загальні умови прийнятності рівня ризику для обраного виду діяльності:

$$W(x_{\text{дп}}) \le k_{\text{дп}},\ W(x_{\text{кр}}) \le k_{\text{кр}},\ W(x_{\text{кт}}) \le k_{\text{кт}}.$$

Якщо для певного виду діяльності здійснена оцінка величин $M(X)$ і $\sigma(X)$ і встановлені для даної організації величини критеріїв допустимого, критичного та катастрофічного ризиків $k_{\text{дп}}$, $k_{\text{кр}}$, $k_{\text{кт}}$, то можна оцінити границі зон ризику. Мінімальні порогові значення можливих збитків, що задовольняють поставленим вимогам, будуть:

$$x_{\text{дп}} = M(X) + \frac{\sigma(X)}{\sqrt{k_{\text{дп}}}},\ x_{\text{кр}} = M(X) + \frac{\sigma(X)}{\sqrt{k_{\text{кр}}}},\ x_{\text{кт}} = M(X) + \frac{\sigma(X)}{\sqrt{k_{\text{кт}}}}.$$

Вартісна оцінка ризиків Value-At-Risk [22] дозволяє оцінити величину максимально можливих втрат (збитків) з визначеним рівнем ймовірності. Може застосовуватись для вимірювання ринкового, кредитного та операційного ризиків різних проєктів у будь-якій сфері.

Value-At-Risk (VaR) характеризується трьома параметрами:

- базова валюта, в якій вимірюється показник;

- часовий горизонт, який залежить від ситуації. Найчастіше розрахунки здійснюють з горизонтом від 1 до 10 днів

- довірчий рівень, що відображає точність оцінки ризику. Використовується величина 95-99 %.

На рис. 3.14 наведено геометричну інтерпретацію VaR.

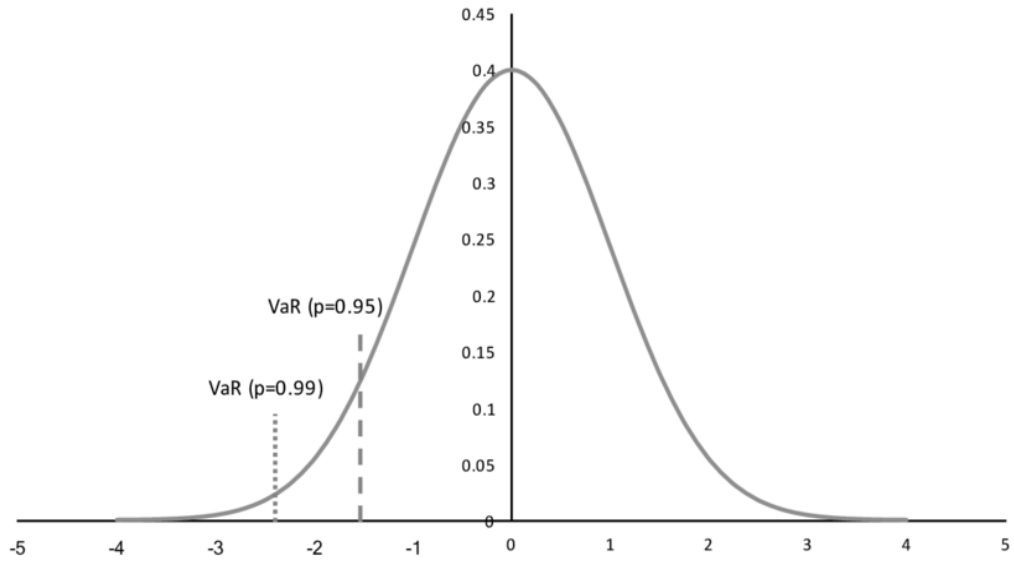


Рисунок 3.14 – Value-At-Risk

VaR визначає величину збитків, яка з імовірністю, що дорівнює рівню довіри (наприклад, 99 %), не буде перевищена. Тобто, при виборі 99 % довірчого інтервалу, оцінка VaR буде враховувати всі результати, крім 1 % найгірших, а при виборі 95 % довірчого інтервалу – не буде враховано вже 5 % найбільш небажаних результатів.

Особливість показника VaR у тому, що він об'єднує відхилення прибутковості активу з ймовірністю даного сценарію з урахуванням допустимого часу.

Оцінка VaR може відбуватися як шляхом визначення величини абсолютних збитків, так і шляхом визначення величини втрат відносно середнього доходу. Часовий горизонт, для якого розраховується VaR, часто вибирається виходячи з мінімального реального терміну, протягом якого можна реалізувати інструмент без суттєвого збитку.

VaR розраховується за формулою:

$$VaR = M(X) - \sigma(X) \cdot u_{\alpha},$$

де u_{α} – квантиль нормальної функції розподілу. Квантиль відображає положення шуканого значення випадкової величини X щодо середньозваженого $M(X)$, виражене в кількості стандартних відхилень $\sigma(X)$.

При рівні довіри (ймовірності відхилення) 99 %, квантиль становить 2.33, при 95 % – 1.65, при 90 % – 1.28.

Збитки в межах 1-3 VaR вважаються звичними та допустимими. Підприємство, яке не здатне впоратися із збитками, що в три рази перевищують VaR, як з рутинними подіями, ймовірно, не зможе функціонувати довгостроково. Збитки в діапазоні від 3 до 10 VaR використовуються для проведення стрес-тестування. Підприємство повинно бути впевненим, що врахувало всі відомі ситуації, здатні призвести до збитків у цьому діапазоні, і готове до їх подолання. Події, що викликають збитки понад 10 VaR, не повинні мати місця. Якщо такі події неминучі, їх слід хеджувати або застрахувати, або змінити бізнес-план, щоб уникнути їх, або збільшити рівень VaR.

За допомогою кореляційного аналізу можна визначити тісноту взаємозв'язку між показниками: оцінити, як сильно змінюється середня величина одного з них залежно від зміни іншого.

Взаємозв'язок може бути: повним (функціональним) та неповним (піддається впливу сторонніх факторів). Залежно від числа параметрів, що визначають стан аналізованого, виділяють парну (два взаємозалежні параметри) і множинну кореляцію (один параметр залежить від декількох інших). Коефіцієнт кореляції змінюється в діапазоні від 0 до 1. Чим сильніший і більш однозначний вплив одного параметру на іншій, тим вищий по модулю коефіцієнт кореляції.

У світовій практиці критичні значення коефіцієнта кореляції 0.5 і -0.5. Якщо модуль коефіцієнта кореляції більший за 0.5, то вважається, що між змінними існує сильний взаємозв'язок. Інакше взаємозв'язок між змінними – слабкий. Якщо значення коефіцієнта кореляції позитивне, то взаємозв'язок між змінними прямий, а якщо негативне, то зв'язок зворотний.

Для аналізу ризиків можуть використовуватись такі коефіцієнти кореляції:

1) коефіцієнт кореляції Пірсона;

2) рангова кореляція Спірмена;

3) тау Кендалла для обробки ранжируваних змінних;

4) точково-бісеріальна кореляція для вимірювання кореляції між двійковою змінною та безперервною змінною;

5) V Крамера для категоріальних змінних;

6) бісеріальна кореляція для оцінки взаємозв'язку між бінарною змінною і безперервною змінною;

7) коефіцієнт Фі – міра кореляції двох двійкових змінних (категоріальні змінні, що мають лише два рівні кожна).

Хоча аналіз кореляції є потужним інструментом, він має свої обмеження. Кореляція не передбачає причинно-наслідковий зв'язок: якщо два показника корелюють, це не означає, що один викликає інший. Крім того, кореляційний аналіз припускає, що зв'язок між двома параметрами є лінійним, що не завжди може мати місце. Нарешті, аналіз кореляції чутливий до викидів і може залежати від екстремальних значень даних.

3.4. Методологія оцінки ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури

У сучасних галузях, що мають важливе значення для критичної інфраструктури, широко застосовуються автоматизовані системи управління технологічними процесами, включаючи системи диспетчерського управління та збору даних, системи розподіленого управління та інші типи управлінських конфігурацій. Ще нещодавно питання безпеки об'єктів критичної інфраструктури вирішувалося в основному за двома напрямами: захист від несанкціонованого доступу та забезпечення стабільної роботи автоматизованих систем управління технологічними процесами. Однак із розвитком інформаційних технологій та глобалізацією інформаційно-телекомунікаційних мереж з'явилися нові загрози для безпеки об'єктів, пов'язані з можливими злочинними втручаннями та порушенням роботи ключових інформаційних систем, що відповідають за управління і

забезпечення безпеки критичної інфраструктури. Забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури регулюється Законом України «Про основні засади забезпечення кібербезпеки України» (чинна редакція від 28.06.2024 року), який визначає правові та організаційні принципи захисту життєво важливих інтересів людей, суспільства та держави в кіберпросторі, а також основні цілі, напрямки та принципи державної політики в цій сфері, повноваження відповідних органів і установ, а також механізми координації діяльності для забезпечення кібербезпеки.

Згідно з цим Законом України, кіберзахист визначається як сукупність організаційних, правових та інженерно-технічних заходів, а також методів криптографічного та технічного захисту інформації, що спрямовані на запобігання кіберінцидентам, виявлення та захист від кібератак, усунення їхніх наслідків і відновлення стабільності та надійності роботи комунікаційних і технологічних систем. Забезпечення кібербезпеки досягається через створення системи управління інформаційною безпекою (СУІБ) згідно з міжнародним стандартом ISO/IEC 27001:2022 або через розробку комплексної системи захисту інформації (КСЗІ) відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».

Одним із ключових етапів побудови СУІБ та КСЗІ є створення системи управління ризиками. У рамках цієї системи процес оцінки ризику є основою для наукових досліджень в області аналізу та вдосконалення існуючих методів оцінки ризику, розробки нових підходів для підвищення точності оцінок і виконання математичних операцій над ризиками.

Стейкхолдери інформаційних систем прагнуть мінімізувати ризики кібербезпеки та знизити витрати на заходи, спрямовані на їх зменшення. Економічна доцільність застосування різних заходів обробки ризику, як організаційних, так і технічних, визначається шляхом порівняння вартості цих заходів із максимально можливими збитками від впливу кількох ризиків.

Результати оцінки суми ризиків дають підстави для прийняття рішення щодо прийнятності їхнього рівня та доцільності або необхідності подальшої обробки цих ризиків. Під сумою ризиків розуміється певна величина, що визначається як добуток ймовірності реалізації ризиків та величини збитків, які можуть виникнути внаслідок їхнього прояву. Така оцінка є важливою для визначення ризику складних проєктів (наприклад, розробки складних інформаційних систем), де враховуються як наслідки реалізації проєкту, так і ймовірність їх виникнення.

На сучасному етапі розвитку науки та техніки існує об'єктивна суперечність між необхідністю розрахунку суми ризиків та обчисленням комплексного ризику, з одного боку, та відсутністю розроблених методів для їхнього точного розрахунку, з іншого.

З огляду на це, дослідження, які стосуються розробки методології оцінки ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури, орієнтуючись на створення відповідних методів для розрахунку суми ризиків, є надзвичайно актуальними.

Є досить багато понять «ризик». Одне з них визначає ризик R як ймовірність або можливість p настання випадкової події, що призводить до певних збитків h [7, 19], і може бути записано у вигляді:

$$R = p \cdot h.$$

Залежність збитків h у результаті настання деякої події від ймовірності p її настання можна записати таким чином:

$$h(p) = \frac{R}{p}, \text{де } p \neq 0.$$

Нехай існує множина ризиків. Кожний ризик можна представити графіком функції, який визначається ймовірністю p або можливістю настання випадкової події, що може призвести до певних наслідків (збитків) h. Максимальні значення наслідків можуть бути визначені, наприклад експертним шляхом, як максимальні збитки, що можуть бути завдані активам компанії (матеріальні, нематеріальні, людські). Ймовірності

виникнення подій, що призводять до максимальних наслідків в умовах дії кожного ризику визначається з графіку, як координати точок перетину (як наведено на рис. 3.15).

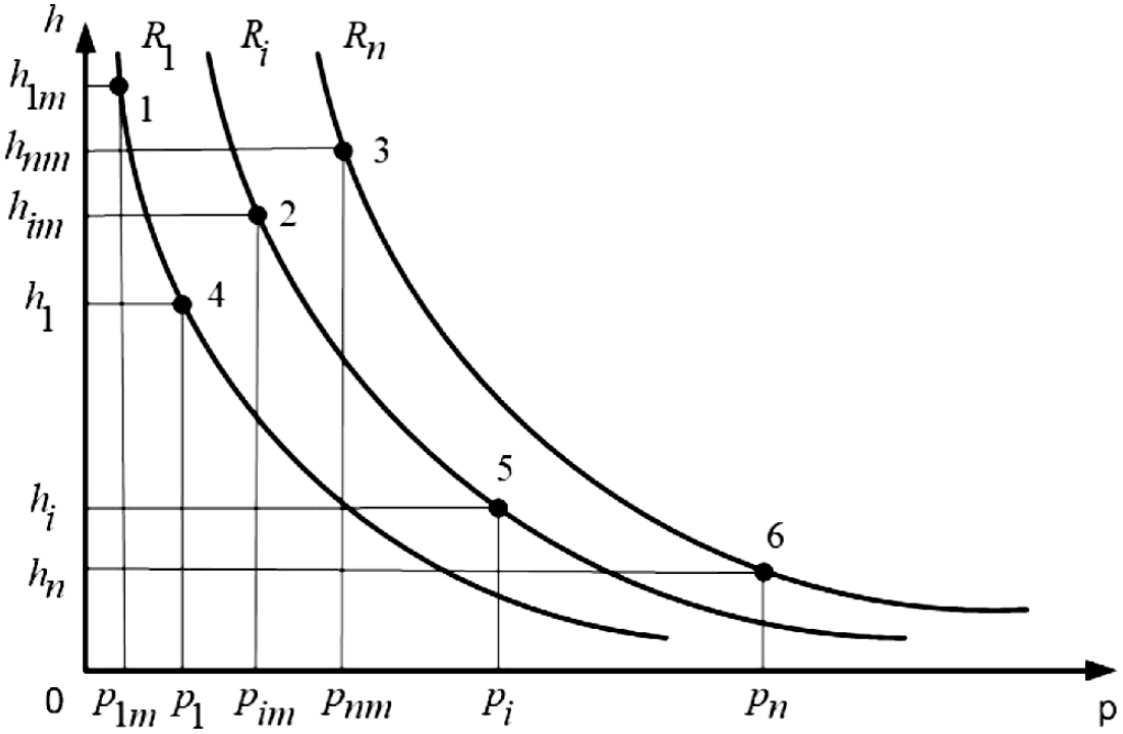


Рисунок 3.15 – Графіки ризиків

У випадку дії кількох ризиків значення сумарного наслідку не буде перевищувати суми максимальних наслідків для кожного з них.

Метод розрахунку суми ризиків полягає в поетапному визначенні: максимальних значень збитків для кожного ризику; ймовірностей настання подій, що призводять до цих максимальних збитків (точки 1, 2, 3 на рис. 3.15); величини сумарних збитків, що не перевищує максимальні збитки для кожного окремого ризику; ймовірності настання максимальних збитків, як суми ймовірностей для сумісних подій. Загальний ризик обчислюється як добуток величини сумарних збитків та ймовірності їх виникнення.

На основі отриманого значення суми ризиків можна побудувати графік сумарного ризику, який наведено на рис. 3.16.

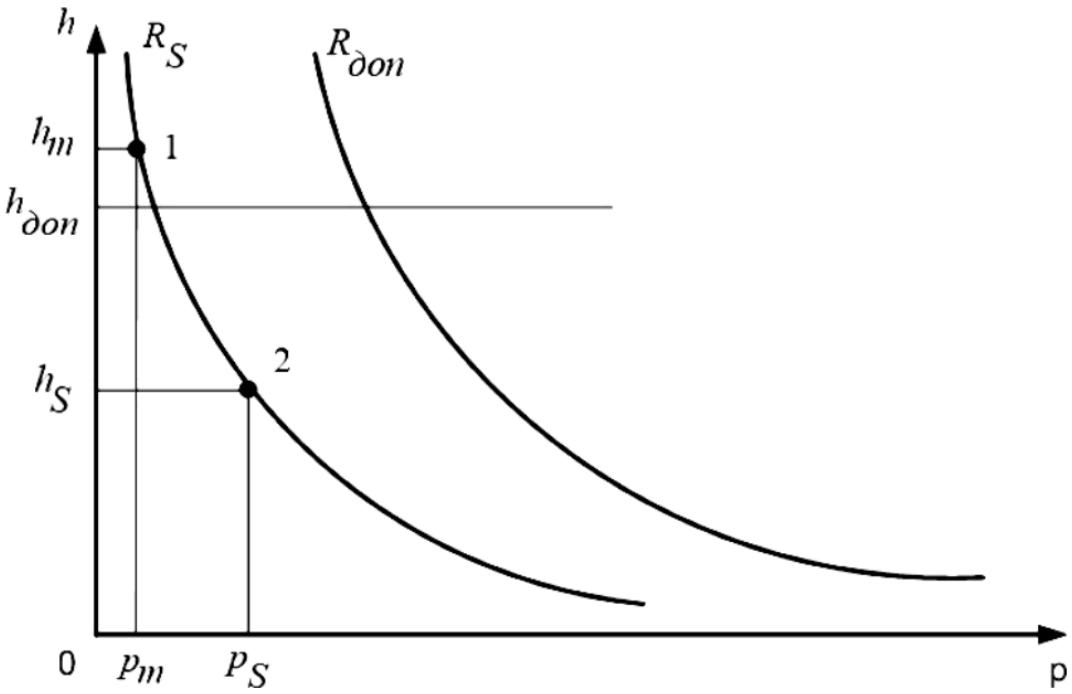


Рисунок 3.16 – Графік сумарного ризику

Отримані результати дозволяють визначити величину загальних збитків і ймовірність їхнього настання, а також проводити оцінку суми ризиків з метою підтримки прийняття рішень щодо їх обробки. Оцінка ризику включає порівняння отриманих даних з встановленими критеріями допустимого ризику або максимально допустимих збитків. Переваги цього методу визначення суми ризиків полягають у його наочності та простоті розрахунків.

Проте існуючі методи оцінки ризиків не враховують суб'єктивний аспект ризику, що ускладнює точну і коректну оцінку.

Як показують дослідження, повний ризик можна представити у вигляді комплексного числа:

$$R = r + iv,$$

де r – об'єктивний ризик; v – суб'єктивний ризик; $i = \sqrt{-1}$.

Об'єктивний ризик r визначається, як добуток об'єктивної ймовірності (припущення щодо її настання, що базується на особистому досвіді) і величини реальних наслідків від настання такої події. Суб'єктивний ризик v визначається, як добуток суб'єктивної ймовірності події (припущення щодо її

настання, що базується на частоті, з якою подібний результат був отриманий в аналогічних умовах), що призводить до ризику, і величини суб'єктивних наслідків від настання такої події. Технічно суб'єктивна і об'єктивна ймовірність визначається за допомогою спеціально організованих експертних процедур.

Модуль комплексного ризику $|R_S|$ визначає дійсну його характеристику, а аргумент комплексного ризику φ_S, являється показником превалювання однієї складової ризику над іншою:

$$|R_S| = \sqrt{r^2 + v^2}, \varphi_S = arctg\frac{v}{r}, r \neq 0.$$

Надання ризику у вигляді комплексного числа, з урахуванням об'єктивної та суб'єктивної складових частин, відкриває перспективи побудови моделей поведінки з ризиками на основі застосування апарату теорії функцій комплексної змінної.

Узагальнена методологія ґрунтується на методі експертних оцінок та містить такі етапи:

1. Визначення базових параметрів.
2. Збір вхідних даних.
3. Обчислення суми ризиків об'єктивної складової.
4. Обчислення суми ризиків суб'єктивної складової.
5. Визначення загальної суми ризиків.
6. Візуалізація результатів обчислень.

Застосовуючи цю методологію, можна створювати програмні та апаратно-програмні системи, що ґрунтуються на методах розрахунку суми ризиків та оцінки комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури.

Контрольні питання

1. Які існують види оцінки та аналізу ризиків?
2. Як виконується якісний аналіз ризиків?

3. Як виконується кількісний аналіз ризиків?

4. Як виконується вимірювання ризику?

5. Що таке ступінь ризику?

6. Що таке міра ризику?

7. Для чого використовується і як виглядає матриця оцінки ризику?

8. Що таке ціна ризику?

9. Що є загрозами в інформаційних системах?

10. Які існують фактори впливу на ризики?

11. Наведіть основний алгоритм якісного аналізу ризику.

12. Що є метою формально-логічних методів оцінки ризику?

13. Що лежить в основі експертних методів оцінки ризику?

14. Які риси мають статистичні методи аналізу ризиків?

15. Які риси мають розрахунково-аналітичні методи аналізу ризиків?

16. Що лежить в основі нормативних методів аналізу ризиків?

17. Які особливості використання методів моделювання для аналізу ризиків?

18. Що регулює стандарт ISO 31010-2019?

19. Назвіть кілька методів оцінки ризику зі стандарту ISO 31010-2019.

20. У чому полягає сутність методу оцінки ризику «краватка-метелик» BTA?

21. Які основні переваги та недоліки методу оцінки ризику «краватка-метелик» BTA?

22. У чому полягає сутність аналізу причин і наслідків ризикових подій?

23. Яким чином будується діаграма Ісікава?

24. На чому базується аналіз впливу на бізнес BIA?

25. Які показники часу враховуються в аналізі впливу на бізнес?

26. Які основні переваги та недоліки аналізу впливу на бізнес?

27. Які дії виконуються при попередньому аналізі небезпек PHA?

28. Які статистичні параметри використовуються для оцінки величини ризику?

29. Які існують зони ризику?

30. За допомогою якого параметру можна оцінити величину максимально можливих втрат з визначеним рівнем ймовірності?

31. Які варіанти кореляційного аналізу використовуються для оцінки ризиків?

32. У чому полягає сутність оцінки ризиків кібербезпеки інформаційної системи об’єктів критичної інфраструктури?

33. На чому базується узагальнена методологія оцінки ризиків кібербезпеки?

4. ОСНОВНІ ЗАГРОЗИ ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ ДЛЯ КОРИСТУВАЧІВ

4.1. Організаційно-технічні заходи щодо технічного захисту інформації

Інформаційна сфера – область діяльності, що відноситься до створення, передачі і використання інформації, включаючи особисту і суспільну свідомість, інформаційну і телекомунікаційну інфраструктуру та власне, інформацію. Інформаційна сфера – це частина соціальної діяльності суспільства, тому в ній проявляються загальні закони буття, загальні і специфічні закономірності соціального розвитку.

Єдиний інформаційний простір країни – це сукупність інформаційних ресурсів та інформаційної інфраструктури, що дозволяє на основі єдиних принципів і за загальними правилами забезпечувати безпечну інформаційну взаємодію держави, організацій і громадян при їх рівнодоступності до відкритих інформаційних ресурсів, а також максимально повне задоволення їх інформаційних потреб на всій території держави при збереженні балансу інтересів на входження в світовий інформаційний простір і забезпечення національного інформаційного суверенітету.

Інформаційні ресурси – інформаційна інфраструктура (апаратура і системи створення, обробки, збереження і передачі інформації), включаючи файли і бази даних та інформацію й інформаційні потоки.

Загроза інформаційній безпеці – це такий стан, коли проявляються наміри або дії, які можуть нанести шкоду інтересам особистості, суспільства та держави в галузі інформації.

Незаконне використання інформаційних і телекомунікаційних систем і інформаційних ресурсів – їх використання без відповідного дозволу або порушення встановлених правил, законодавства чи принципів міжнародного права.

Інформаційна інфраструктура містить:

- організаційні структури, що забезпечують функціонування і розвиток єдиного інформаційного простору (зокрема, збирання, обробку, збереження, поширення, пошук і передачу інформації). Забезпечувальну частину складають науково-методичне, інформаційне, лінгвістичне, технічне, кадрове, фінансове забезпечення;

- інформаційно-телекомунікаційні структури – територіально розподілені державні і корпоративні комп'ютерні мережі, телекомунікаційні мережі і системи спеціального призначення та загального користування, мережі і канали передачі даних, засоби комутації і керування інформаційними потоками;

- телекомунікаційні технології;

- системи засобів масової інформації.

Інформаційна безпека – захищеність (стан захищеності) основних інтересів особистості, суспільства і держави в сфері інформації, включаючи інформаційну і телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі, як повнота, об'єктивність, доступність і конфіденційність. Інформаційна безпека є складовою національної безпеки. Але особливістю інформаційної безпеки є те, що вона, як невід'ємна частина, входить до інших складових національної безпеки: економічної, воєнної, політичної безпеки тощо [9].

На сучасному етапі основними реальними та потенційними загрозами національній безпеці України в інформаційній сфері є:

- прояви обмеження свободи слова та доступу громадян до інформації;

- поширення засобами масової інформації культу насильства, жорстокості, порнографії;

- комп'ютерна злочинність та комп'ютерний тероризм;

- розголошення інформації, яка становить державну та іншу, передбачену законом таємницю, а також конфіденційної інформації, що є

власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Базові засади інформаційної безпеки нашої держави закладено в статтях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України.

У ст. 1 закону інформація визначається як документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі.

Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій.

Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України.

Основними видами інформації є:

- статистична;

- адміністративна інформація (дані);

- масова інформація;

- інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування;

- правова інформація;

- інформація про особу;

- інформація довідково-енциклопедичного характеру;

- соціологічна інформація.

За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом [20]. Держава здійснює контроль за режимом доступу до інформації. Обмеження права на одержання відкритої

інформації забороняється законом. Класифікація інформації залежно від режиму доступу наведена на рис. 4.1.

Рисунок 4.1 – Види інформації за режимом доступу

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну.

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

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю (військова, комерційна, банківська, професійна, лікарська, адвокатська таємниця тощо), розголошення якої завдає шкоди особі, суспільству і державі.

Інформація, що становить військову таємницю – це вид таємної інформації, який охоплює відомості в сфері оборони, державної безпеки та охорони правопорядку, розголошення якої може завдати шкоди інтересам державної безпеки, бойової готовності Збройних Сил України та інших військових формувань, їхніх окремих підрозділів, якщо ці відомості не належать до державної таємниці згідно з законодавством України.

Особливим видом таємної інформації є державна таємниця. Вона охоплює відомості в сфері оборони, економіки, зовнішніх відносин, державної безпеки і органів правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України і які визначені в порядку, встановленому законом, державною таємницею та підлягає охороні з боку держави.

Віднесення інформації до категорії відомостей, що становлять державну таємницю, порядок її захисту та обігу, доступ до неї визначається

Законом України «Про державну таємницю», яким закладено правову основу створення та функціонування системи охорони державної таємниці в Україні.

Ступень таємності інформації визначається наданим грифом таємності «Таємно», «Цілком таємно» та «Особливої важливості». Гриф надається на певний термін, який залежить від ступеня таємності: для грифу «Таємно» – 5 років, «Цілком таємно» – 10 років, «Особливої важливості» – 30 років.

До інформаційних ресурсів України входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами.

Інформаційний суверенітет України забезпечується:

- виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету;
- створенням національних систем інформації;
- встановленням режиму доступу інших держав до інформаційних ресурсів України;
- використанням інформаційних ресурсів на основі рівноправного співробітництва з іншими державами.

Класифікація інформації у відповідності до Закону України «Про інформацію»

Концепція на базі прийнятих законів, підзаконних актів та узагальнення їх застосування визначає державну політику України в сфері технічного захисту інформації, основні напрями та організаційні засади подальшого розвитку системи захисту інформації в Україні. Початок створення такої системи слід віднести до 1994 р., коли було затверджено Постанову Кабінету Міністрів України «Про затвердження Положення про технічний захист інформації в Україні» (від 27.09.1994 р., поточна редакція від 04.05.2008 р.), якою визначалися першочергові дії держави щодо технічного захисту інформації.

У загальних положеннях концепції визначено, що технічний захист інформації (ТЗІ) – це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

Прогрес у різних галузях науки і техніки призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна легко підключатись до ліній телекомунікацій та різноманітних технічних засобів оброблення інформації вітчизняного та іноземного виробництва з метою здобування, пересилання та аналізу розвідувальних даних.

За таких умов створилися можливості витоку інформації, порушення її цілісності та блокування. Витік інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, – це одна з основних можливих загроз національній безпеці України в інформаційній сфері.

Зі створенням правових та організаційних основ ТЗІ були створені правові та організаційні основи криптографічного захисту інформації. У травні 1998 р. (відповідно, саме положення було підготовлено дещо раніше) прийнято Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» (поточна редакція від 12.09.2009 р.).

У липні 2002 року був прийнятий Закон України «Про Національну систему конфіденційного зв’язку» (поточна редакція від 01.01.2022 р.), у січні 2003 р. надано розпорядження Президента України «Про заходи щодо забезпечення розвитку і функціонування Національної системи конфіденційного зв’язку», з дорученням Президента Кабінету Міністрів щодо практичної організації такої системи.

Загрози безпеці інформації в Україні зумовлені:

- не виваженістю державної політики в галузі інформаційних технологій, що може призвести до безконтрольного та неправомірного доступу до інформації та її використання;

- діяльністю інших держав, спрямованою на одержання переваги в зовнішньополітичній, економічній, військовій та інших сферах;

- недосконалістю організації в Україні міжнародних виставок апаратури різного призначення (особливо пересувних) та заходів екологічного моніторингу, що може використовуватися для здобування інформації розвідувального характеру;

- діяльністю політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб, спрямованою на одержання переваги в політичній боротьбі та конкуренції;

- злочинною діяльністю, спрямованою на протизаконне одержання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам;

- використанням інформаційних технологій низького рівня, що призводить до впровадження недосконалих технічних засобів із захистом інформації, засобів контролю за ефективністю ТЗІ та засобів ТЗІ (далі – засоби забезпечення ТЗІ);

- недостатністю документації на засоби забезпечення ТЗІ іноземного виробництва, а також низькою кваліфікацією технічного персоналу в сфері ТЗІ.

Принципами формування і проведення державної політики в сфері ТЗІ є:

- додержання балансу інтересів особи, суспільства та держави, їх взаємна відповідальність;

- єдність підходів до забезпечення ТЗІ, які визначаються загрозами безпеці інформації та режимом доступу до неї;

- комплексність, повнота та безперервність заходів ТЗІ;

- відкритість нормативно-правових актів та нормативних документів з питань ТЗІ, які не містять відомостей, що становлять державну таємницю;

- узгодженість нормативно-правових актів та нормативних документів з питань ТЗІ з відповідними міжнародними договорами України;

- обов'язковість захисту інженерно-технічними заходами інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в органах державної влади та органах місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, у державних установах і організаціях (далі – державні органи, підприємства, установи і організації);

- виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту конфіденційної інформації, що не належить державі, та відкритої інформації, важливої для особи та суспільства, якщо остання циркулює поза межами державних органів, підприємств, установ і організацій;

- покладення відповідальності за формування та реалізацію державної політики в сфері ТЗІ на спеціально уповноважений центральний орган виконавчої влади;

- ієрархічність побудови організаційних структур системи ТЗІ та керівництво їх діяльністю в межах повноважень, визначених нормативно-правовими актами;

- методичне керівництво спеціально уповноваженим центральним органом виконавчої влади в сфері ТЗІ діяльністю організаційних структур системи ТЗІ;

- координованість дій та розмежування сфер діяльності організаційних структур системи ТЗІ з іншими системами захисту інформації та системами забезпечення інформаційної та національної безпеки;

- фінансова забезпеченість системи ТЗІ за рахунок Державного бюджету України, місцевих бюджетів та інших джерел.

Система захисту об'єктів від витоку інформації складається, в основному, із організаційних і технічних заходів, метою яких є ліквідація або суттєве зменшення можливості витоку конфіденційної інформації, а також контролю захищеності технічних засобів у період їх експлуатації.

Організаційний захід – це захід по захисту інформації, проведення якого не потребує застосування спеціально розроблених технічних засобів.

До основних організаційних і режимних заходів відносяться:

- проведення робіт із захисту інформації організаціями, які мають ліцензію на діяльність у сфері захисту інформації, видану відповідними органами;

- категоріювання та атестація об'єктів технічних засобів приймання, обробки, зберігання та передачі інформації (ТЗПІ) і виділених для проведення закритих заходів приміщень по виконанню вимог забезпечення захисту інформації при проведенні робіт з відомостями відповідного ступеню таємності;

- використання на об'єкті сертифікованих ТЗПІ та допоміжних технічних засобів і систем (ДТЗС);

- встановлення контрольованої зони біля об'єкта;

- залучення до робіт з будівництва, реконструкції об'єктів ТЗПІ, монтажу апаратури організацій, що мають ліцензію на діяльність у сфері захисту інформації по відповідним пунктам;

- організація контролю і обмеження доступу на об'єкти ТЗПІ та у виділені приміщення;

- введення територіальних, частотних, енергетичних, просторових і часових обмежень у режимах використання технічних засобів, що підлягають захисту;

- відключення на період закритих заходів технічних засобів, що мають елементи, які виконують роль електроакустичних перетворювачів (лінії зв'язку тощо).

Технічний захід – це дія із захисту інформації, яка передбачає застосування спеціальних технічних засобів, а також реалізацію технічних рішень.

Технічні заходи містять:

- встановлення за допомогою технічних засобів потенційних каналів витоку інформації та визначення методів та засобів для їх блокування;

- перевірку техніки, яка використовується, на відповідність величини паразитних випромінювань допустимим рівням;

- екранування приміщень або техніки, яка використовується;

- перемонтаж окремих мереж, кабелів та ліній зв'язку;

- застосування спеціальних пристроїв і засобів захисту;

- використання засобів активного захисту;

- перевірку адекватності та надійності функціонування застосованих технічних засобів рівню потенційних загроз.

На початку робіт з ТЗІ необхідно визначити види інформації та від якого роду загроз треба захищатися. Для цього в першу чергу визначають категорію приміщення. При цьому з'ясовують види та ступень таємності інформації, що може циркулювати в приміщенні. Далі розглядаються конструктивні особливості приміщення та умови його розташування, наявність побутової техніки та апаратури для обробки інформації, її типи та технічні характеристики. З'ясовується та враховується наявність біля об'єкту, що треба захищати, іноземних установ, автостоянок, приватних фірм (тобто місць, з яких можна організувати стаціонарне та мобільне зняття інформації).

Заміряється відстань до таких місць і визначається охоронна зона, у межах якої несанкціоноване зняття інформації вважається неможливим. Це надає змогу з'ясувати типи та ступень можливих загроз та встановити відповідну категорію захисту інформації.

Якщо поряд з об'єктом є іноземні установи чи фірми, де можна організувати стаціонарне зняття інформації, категорійність приміщення підвищується на один ступень.

Складається акт про встановлення категорійності приміщення, в якому відбиваються всі питання, що перераховані вище. Такий акт складається представниками підрозділу з ТЗІ та членами комісії, яка призначається керівником установи, де проводяться такі роботи.

Встановлення категорійності приміщення надає змогу скласти план робіт з ТЗІ, в якому визначаються обсяги та напрямки проведення робіт з ТЗІ, термін їх проведення, необхідні технічні засоби для захисту інформації на об'єкті. Ці роботи повинен проводити ліцензіант, тобто установа, яка має державну ліцензію на проведення таких робіт. Надалі всі роботи з ТЗІ проводяться ліцензіантом. Якщо в установі є підрозділ з ТЗІ, який має ліцензію на виконання всього потрібного обсягу робіт, то ці роботи можуть проводитися таким підрозділом.

При проведенні робіт з ТЗІ необхідно провести ряд заходів, зокрема:

- визначити та змонтувати необхідні технічні засоби, що потрібні для захисту інформації на об'єкті;
- провести необхідні вимірювання, які б підтвердили ефективність застосування обраних технічних засобів захисту та їх правильне функціонування.

Після проведення всього комплексу технічних робіт ліцензіант разом з замовником складають акт про надання об'єкту певної категорії із захисту інформації. Лише після одержання та затвердження такого акту на об'єкті можна обробляти інформацію з обмеженим доступом.

Технічний захист інформації від її несанкціонованого зняття полягає в застосуванні спеціальних технічних методів її захисту, які блокують потенційні канали витоку інформації, тобто заважають спробам її незаконного отримання.

Для того, щоб захищати інформацію від витоку необхідно знати потенційні канали витоку та методи їх блокування.

Починаючи вивчення методів та засобів технічного захисту інформації, слід зазначити, що викладення матеріалу обмежується мінімумом тих фізичних і технічних даних, які необхідні для розуміння.

Всі перераховані вище методи інформаційної безпеки реалізуються за допомогою основних засобів захисту: формальних (фізичних, апаратних, програмних, апаратно-програмних, криптографічних) та неформальних (організаційних, законодавчих та морально-етичних). Класифікацію наведено на рис. 4.2.

Рисунок 4.2 – Засоби захисту інформації

Фізичні засоби захисту призначені для зовнішньої охорони території об’єктів та захисту компонентів інформаційної системи організації. Спектр сучасних фізичних засобів захисту дуже широкий. До цієї групи засобів захисту належать, наприклад, різні засоби екранування робочих приміщень та каналів передачі даних.

Апаратні засоби захисту – це пристрої, вбудовані в блоки інформаційної системи (сервера, комп’ютери тощо). Вони призначені для внутрішнього захисту елементів обчислювальної техніки та засобів зв’язку. Основні функції апаратних засобів захисту полягають у забороні несанкціонованого (неавторизованого) зовнішнього доступу віддаленого користувача; забороні несанкціонованого (неавторизованого) внутрішнього доступу до баз даних у результаті випадкових чи умисних дій персоналу; захисті цілісності програмного забезпечення тощо. До апаратних засобів відносяться: генератори шуму, мережеві фільтри, радіоприймачі сканування, і безліч інших пристроїв, що перекривають потенційні канали витоку інформації або дозволяють їх виявити.

Програмні засоби захисту призначені для виконання функцій захисту інформаційної системи за допомогою програмних засобів (антивірусний захист, міжмережеві екрани тощо). Прикладом комплексних рішень служать DLP-системи та SIEM-системи. DLP-системи (Data Leak Prevention – запобігання витоку даних) служать для запобігання витоку, переформатування інформації та перенаправлення інформаційних потоків. SIEM-системи (Security Information and Event Management – управління подіями та інформаційною безпекою) забезпечують аналіз у реальному часі подій безпеки, що виходять від мережевих пристроїв та застосунків. SIEM-системи використовується також для журналювання даних та генерації звітів з метою сумісності з іншими даними.

Апаратно-програмні засоби захисту – це засоби, які основані на синтезі програмних та апаратних засобів.

Криптографічні засоби – це засоби захисту інформації, пов’язані із застосуванням інструментів шифрування. Це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Сюди можуть входити програмні компоненти шифрування (криптопровайдери), засоби організації VPN, засоби ідентифікації, засоби формування та перевірки ключів і електронного цифрового підпису.

Організаційні засоби – це заходи, що регламентують поведінку співробітника організації. Елементи організаційної безпеки наведені на рис. 4.3.

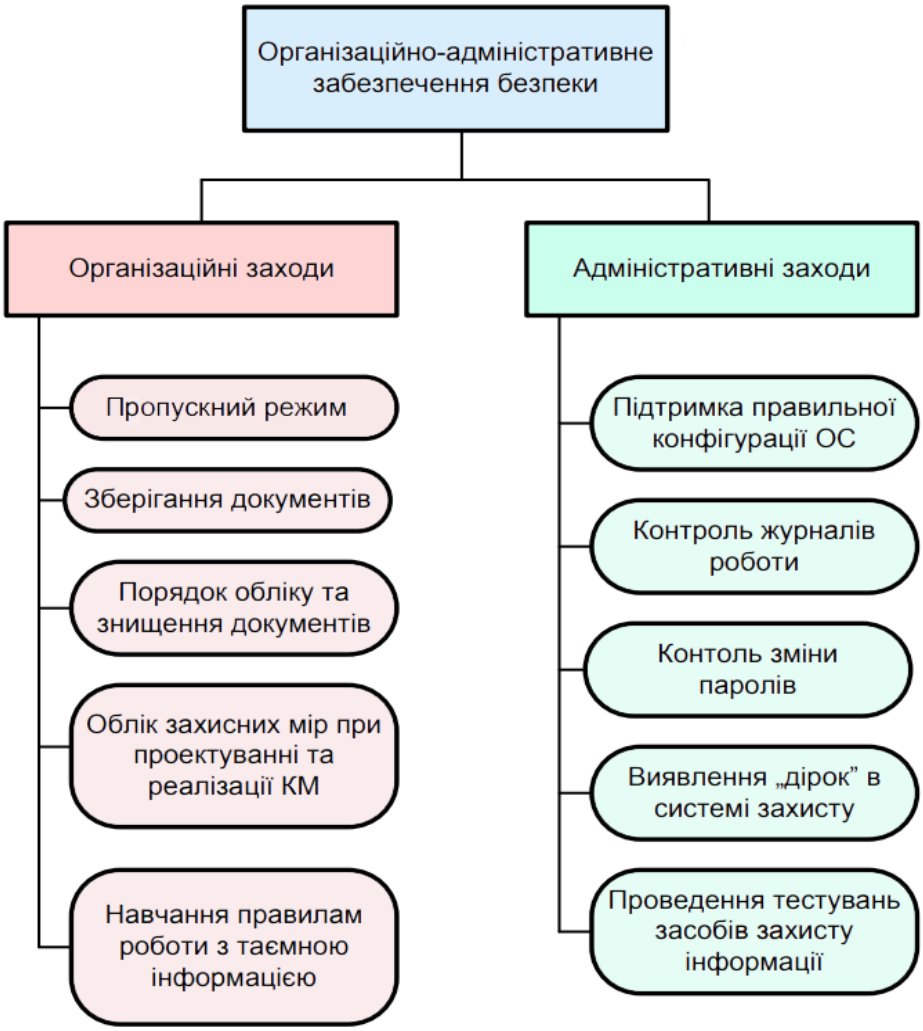


Рисунок 4.3 – Елементи організаційної безпеки

Вони складають сукупність заходів щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу. Регламент роботи користувачів із конфіденційною інформацією називають правилами розмежування доступу. Правила встановлюються керівництвом компанії спільно зі службою безпеки та постачальником, який запроваджує систему безпеки.

Законодавчі засоби – це чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання ІТ. Грамотно побудована система захисту не порушує права користувачів та норми обробки даних. Основні елементи законодавчої (правової) безпеки наведені на рис. 4.4.

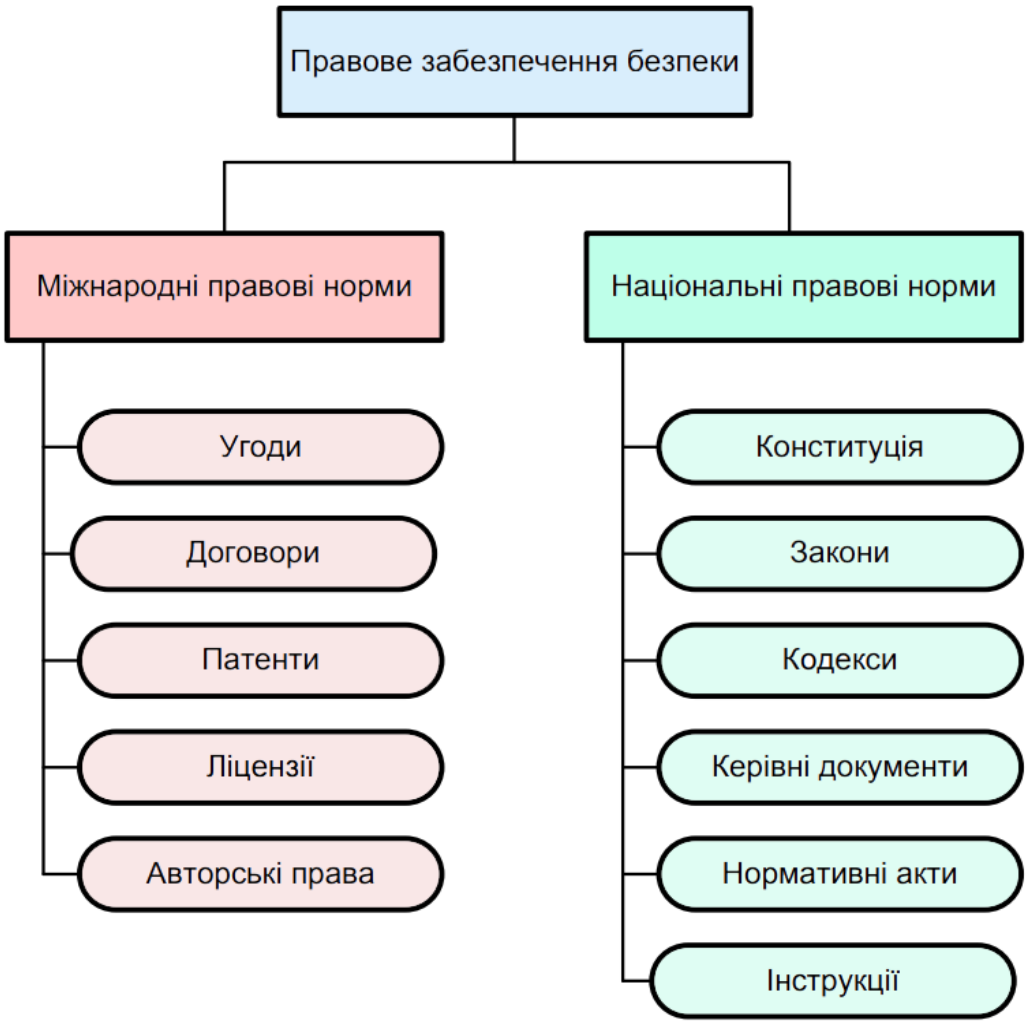


Рисунок 4.4 – Елементи законодавчої (правової) безпеки

Морально-етичні засоби – це правила і норми поведінки співробітників у колективі. Морально-етичні норми бувають як неписаними, так і оформленими в деякий статут. Ці норми не є обов'язковими, як законодавчі, проте, їх недотримання веде до падіння авторитету, престижу людини чи організації.

Інформаційна сфера відіграє все зростаючу роль у забезпеченні безпеки всіх сферах життєдіяльності суспільства, тому захист інформації є одним з важливих напрямків діяльності держави. Для побудови системи захисту інформації необхідно визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації і цілі, а також інші умови і дії, що порушують безпеку. Також необхідно розглядати заходи захисту інформації від неправомірних дій, що призводять до нанесення збитку.

Можна виділити три основні моделі інформаційної безпеки: концептуальна модель, математична модель та функціональна модель.

Концептуальна модель відповідає на загальні питання і схематично відбиває загальну структуру моделі інформаційної безпеки, на якій будуються інші моделі і концепції інформаційної безпеки [13].

Основні компоненти моделі безпеки інформації наведені на рис. 4.5.

Рисунок 4.5 – Концептуальна модель безпеки інформації

Для побудови концептуальної моделі інформаційної безпеки незалежно від того, наскільки проста чи складна інформаційна система, необхідно визначити, як мінімум, що саме захищати, від кого захищати і яким чином захищати. Цей обов'язковий мінімум може бути достатнім для невеликих інформаційних систем. Однак беручи до уваги можливі наслідки, кращим варіантом є побудова повної концептуальної моделі інформаційної безпеки, в якій обов'язково визначаються:

- джерела інформації (співробітники, документи, публікації, технічні носії, технічні засоби, відходи);

- загрози – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і нанесення збитків інформаційній системі (загрози цілісності – умисне перетворення даних, що містяться в інформаційній системі за рахунок спотворення, помилок, втрат та підробки; загрози конфіденційності – неправомірний доступ к інформації з обмеженим доступом за рахунок розголошення, витоку інформації, несанкціонованого доступу; загрози доступності – повна або тимчасова неможливість отримання доступу до ресурсів інформаційної системи за рахунок блокування доступу, захоплення або знищення ресурсів; загрози спостереженості і керованості інформаційною системою – за рахунок порушення можливості інформаційної системи фіксувати діяльність користувачів і процесів, використання об'єктів за рахунок порушення аудиту, ідентифікації і автентифікації, розподілу обов'язків, цілісності комплексу заходів захисту). Класифікація загроз інформаційній безпеці наведена на рис. 4.6.;

- об'єкти загроз (відомості про склад, стан і діяльність організації, інформаційна системи, інформаційно-телекомунікаційна система, об'єкт інформаційної діяльності);

- джерела загроз (конкуренти, злочинці, корупціонери, адміністративні органи, спецслужби);

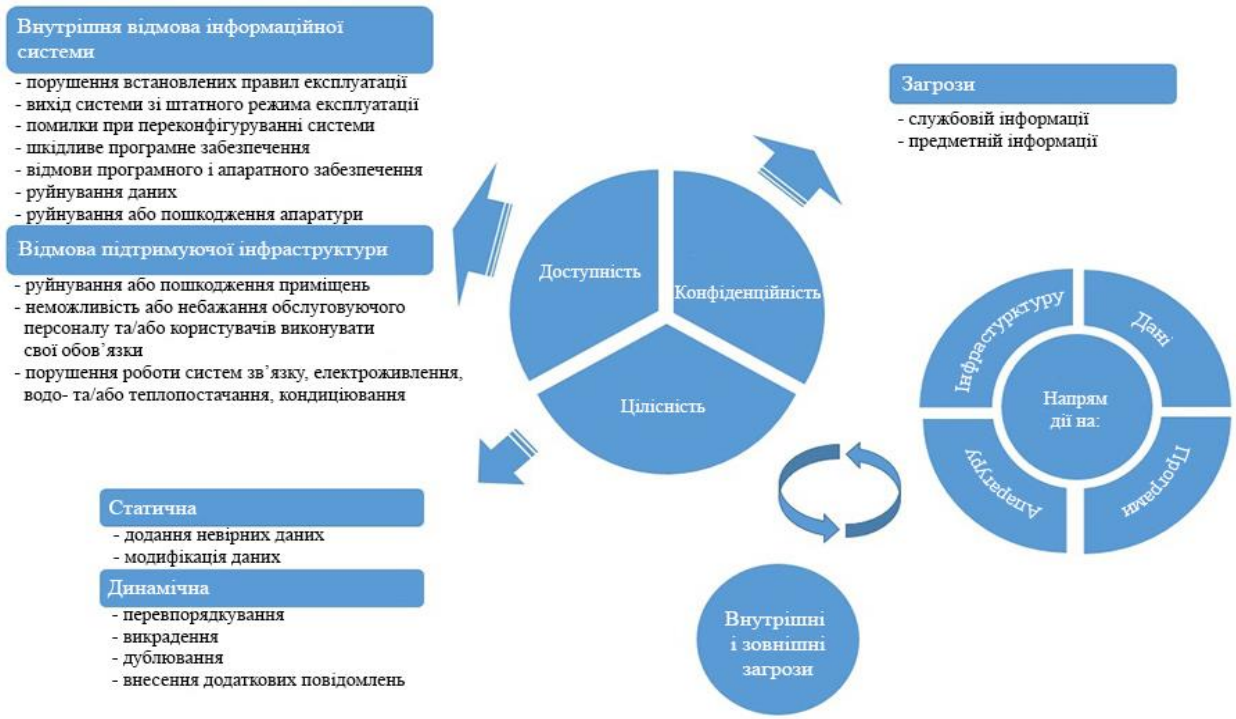


Рисунок 4.6 – Класифікація загроз інформаційній безпеці

- цілі загроз (ознайомлення з конфіденційною інформацією різними шляхами і способами без порушення її цілісності, модифікація інформації в кримінальних цілях – часткова або значна зміна складу і змісту відомостей, знищення інформації як акт вандалізму з метою прямого нанесення матеріального збитку);

- способи доступу (за рахунок розголошення – умисних або необережних дій осіб у повідомленнях, пересилці, публікації та інших способах через канали поширення і засоби масової інформації, яким відповідні відомості були довірені в установленому порядку, що привели до ознайомлення з ними осіб, не допущених до них; за рахунок витоку інформації – безконтрольний вихід інформації з обмеженим доступом за межі організації або кола осіб, яким вона була довірена по різних каналах витоку інформації, у тому числі візуально-оптичним, акустичним, електромагнітним, електричним і матеріально-речовим; за рахунок несанкціонованого доступу – протиправного умисного оволодіння інформацією з обмеженим доступом особою, яка не має права доступу до відомостей, що охороняються за допомогою шпигунства, вивідування,

підслуховування, копіювання, підробки, знищення, перехоплення, фотографування тощо);

- напрями захисту (правовий, організаційний, інженерно-технічний морально-етичний);

- засоби захисту інформації (фізичні, апаратні, програмні, апаратно-програмні, криптографічні);

- способи захисту інформації (попередження, запобігання, припинення, протидія).

Математична та функціональна модель безпосередньо пов’язані одна з одною. Математична модель являє собою формалізований опис сценаріїв у вигляді логічних алгоритмів представлених послідовністю дій порушників та заходів у відповідь. Розрахункові кількісні значення параметрів моделі характеризують функціональні залежності, що описують процеси взаємодії порушників із системою захисту та можливі результати дій. Саме такий вид моделі найчастіше використовується для кількісних оцінок уразливості об’єкта, побудови алгоритму захисту оцінки ризиків та ефективності вжитих заходів.

При побудові даних моделей необхідно спиратися такі найважливіші обставини:

- вибір математично строгих критеріїв для оцінки оптимальності системи захисту інформації для даної архітектури інформаційної системи;

- чітке математичне формулювання завдання побудови моделі засобів захисту інформації, що враховує задані вимоги до системи захисту та дозволяє побудувати засоби захисту інформації відповідно до цих критеріїв.

На практиці в умовах численних ризиків загроз безпеці зробити подібну чисельну оцінку без використання методів математичного моделювання, очевидно, неможливо.

Математичне моделювання також застосовують для побудови математичної моделі потенційного порушника, в якій можливе визначення коефіцієнта або ймовірності реалізації загрози атаки потенційним

порушником. Також може бути розглянуто завдання резервування елементів системи, яке вирішується для захисту від порушення конфіденційності оброблюваної в інформаційній системі інформації.

Залежно від цілей та розв'язуваного завдання, може бути побудовано та застосовано безліч математичних моделей частини системи інформаційної безпеки, які допоможуть ще на стадії проєктування оцінити її ефективність.

Немаловажним питанням при побудові будь-яких моделей чи систем є життєвий цикл цієї моделі чи системи. Недостатньо тільки побудувати систему інформаційної безпеки на основі застосування різних моделей, ще необхідно дотримуватися життєвого циклу даної системи. У ній, незалежно від розмірів організації та специфіки її інформаційної системи, роботи із забезпечення інформаційної безпеки, у тому чи іншому вигляді повинні міститись такі етапи або кроки:

1) планування або розробка;

2) впровадження або реалізація;

3) перевірка або моніторинг;

4) корегування або удосконалення.

При цьому важливо не упустити будь-яких істотних аспектів. Це гарантуватиме певний мінімальний (базовий) рівень інформаційної безпеки, обов'язковий для будь-якої інформаційної системи.

4.2. Ризики під час роботи в мережі Інтернет

У зв'язку зі зростаючою роллю інформаційно-комунікаційних технологій у сучасному суспільстві проблема захисту даних від втрати, викрадення, спотворення або пошкодження потребує посиленої уваги. Вирішення цієї проблеми сприяє забезпеченню інформаційної безпеки як окремої особистості, організації, так і всієї держави [5].

Інформаційна безпека – це стан захищеності систем передавання, опрацювання та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність даних.

Інформаційна безпека базується на принципах:

- доступності – забезпечення доступу до загальнодоступних даних усім користувачам і захист цих даних від блокування зловмисниками;

- конфіденційності – забезпечення доступу до даних на основі розподілу прав доступу;

- цілісності – захист даних від їх зловмисного або випадкового знищення чи спотворення.

Також під інформаційною безпекою розуміють комплекс заходів, спрямованих на забезпечення захищеності даних від несанкціонованого доступу, використання, оприлюднення, внесення змін чи знищення.

Кримінальним кодексом України передбачено кримінальну відповідальність за порушення інформаційної безпеки.

З технічної точки зору, залежно від результату шкідливих дій, можна виділити такі види загроз інформаційній безпеці:

- отримання несанкціонованого доступу до секретних або конфіденційних даних;

- порушення або повне припинення роботи комп'ютерної інформаційної системи;

- отримання несанкціонованого доступу до керування роботою комп'ютерної інформаційної системи;

- знищення або спотворення даних.

Серед основних загроз використання комп'ютерних мереж для користувачів, виділяють:

- комунікаційні ризики – ризики, що пов'язані зі спілкуванням у мережі та використанням онлайн-ігор. Проявляються під час спілкування в соціальних мережах, онлайн-месенджерах, форумах, блогах та інших ресурсах. До цієї категорії належать кібербулінг, сексуальні домагання (секстінг, грумінг, онлайн-знайомства), загрози репутації в мережі, спілкування з незнайомими, потенційно небезпечні соціальні групи;

- контентні ризики – незаконна, потенційно небезпечна інформація в мережі, негативний контент, матеріали сексуального характеру, порнографія, матеріали, що містять жорстокість, насильство та агресію, пропаганда наркотиків, алкоголю, сигарет, самогубств, небезпечних способів схуднення тощо;

- споживчі ризики – неякісна, контрафактна продукція, втрата коштів, розкрадання персональних даних під час інтернет-шопінгу, фішинг (виуджування персональних даних), мобільне шахрайство;

- технічні ризики – пошкодження пристроїв, інформації, програмного забезпечення, зламування акаунтів, крадіжка персональних даних, здирництво грошей, шкідливі програми, а також освоєння нових пристроїв, програм, онлайн-сервісів.

У 2020 році компанія Microsoft провела дослідження ризиків у мережі Інтернет і виділила 4 такі типи ризиків, які частково або повністю перекривають перші три типи загроз:

1. Комунікаційні ризики:

- небажаний контакт – безпосередній контакт (засобами комунікаційного зв'язку або особисто) з людиною, яка отримала контактні дані в мережі Інтернет без особистої її згоди на контакт;

- обман, шахрайство та махінації – поширення хибних чуток (наприклад, листів щастя), злочинні спроби отримати особисту інформацію часто з метою отримання грошової вигоди (наприклад, фішингові листи), шкідливі листи, замасковані під листи від родичів, знайомих, співробітників або клієнтів організації (наприклад, віруси);

- гендерна, етнічна, релігійна, расова та інша ненависть (хейт-спіч) – агресивна мова, спрямована на людину або групу людей за ознакою статі, етнічним походженням, релігією, расою, інвалідністю або сексуальною орієнтацією;

- дискримінація – людина, яка зазнає дискримінації або виключення за ознакою статі, етнічного походження, релігії, раси, інвалідності або сексуальної орієнтації.

2. Репутаційні ризики:

- доксінг – процес збирання, розповсюдження або розміщення інформації про людину (наприклад, ім'я, вік, адреса електронної пошти, номер телефону, фотографії тощо) без її дозволу;

- збитки особистої репутації – збитки від руйнування образу, створеного на базі особистої інформації, якою користувач або інші особи ділилися в мережі Інтернет у блогах, публікаціях, фотографіях, твітах, відео тощо;

- збитки професійної/робочої репутації – збитки або руйнування образу, створеного за допомогою робочої інформації, якою користувач або інші люди ділилися в мережі Інтернет у блогах, публікаціях, фотографіях, твітах, відео тощо;

- порнографічна помста – відверте сексуальне зображення одного або кількох людей, яке розповсюджується без їхньої згоди.

3. Поведінкові ризики;

- грубе поводження – слова або повідомлення, надіслані іншій людині в мережі Інтернет, які є недобрими, несправедливими або зловмисними;

- тролінг – навмисна дія, спрямована на те, щоб вивести когось із себе або роздратувати, використовуючи коментарі в мережі Інтернет або соціальних мережах розумним, але оманливим способом;

- мізогінія – вираз або демонстрація неприязні, зневаги або упередженого ставлення щодо жінок;

- терористичне вербування – спроба представників терористичної організації завербувати людину з заподіяння шкоди;

- відкриті погрози та образи (харрасмент) – погрози або інша образлива поведінка (не сексуальне домагання), яка надсилається онлайн або розміщена в мережі для перегляду іншими особами;

- мікроагресія – ненавмисні висловлювання на адресу будь-якої маргіналізованої групи суспільства (наприклад, релігійних чи етнічних меншин, жінок, ЛГБТ, людей з інвалідністю тощо);

- кібербулінг – мережа Інтернет, телефони або інші пристрої використовуються для надсилання або розміщення текстів, зображень або відео, призначених для заподіяння шкоди, збентеження або залякування іншої людини;

- телефонний тероризм – обман служб екстреної допомоги (поліції, пожежної служби, медичної служби) з метою екстреного реагування на підставі помилкового повідомлення про критичний інцидент або злочин.

4. Сексуальні ризики:

- отримання небажаних повідомлень сексуального характеру;

- сексуальне домагання – людина, яка просить про вступ у сексуальні стосунки чи розмову про секс, або про надання небажаної особистої інформації сексуального характеру;

- надсилання небажаних повідомлень сексуального характеру;

- сексуальний шантаж – погрози поширення особистих матеріалів, людині, яка не надає зображення сексуального характеру, сексуальні послуги або гроші. Злочинець також може загрожувати заподіяти шкоду друзям або родичам, використовуючи інформацію, яку він отримав з електронних пристроїв;

- небажана сексуальна увага – небажане сексуально-орієнтоване дратування, жарт чи флірт у мережі або за допомогою електронних пристроїв.

Організація KCSIE (Keeping Children Safe in Education) з Великобританії запропонувала класифікацію Інтернет-ризиків на основі принципу «4Cs of online safety: Content, Contact, Conduct Commerce»:

1. Контент (Content). Вміст – це все, що розміщено в мережі Інтернет (текст, зображення, відео тощо). Користувачі можуть бачити незаконний, невідповідний або шкідливий вміст (порнографія, фейкові новини, расизм,

самоушкодження, самогубство, антисемітизм, радикалізація, екстремізм тощо).

2. Контакт (Contact). Контакт стосується ризику заподіяння шкоди користувачам під час взаємодії з іншими користувачами в мережі Інтернет (булінг, грумінг, перегляд недоречної комерційної реклами тощо).

3. Поведінка (Conduct). Поведінка означає те, як люди поводяться в мережі Інтернет. Деяка поведінка в мережі Інтернет може збільшити ймовірність або навіть завдати шкоди (залякування, надсилання порнографії).

4. Комерція (Commerce). Комерція – ризик, пов’язаний із такими речами, як азартні онлайн-ігри, неприйнятна реклама, фішинг або фінансове шахрайство.

Розрізняють три шляхи захисту даних:

- захист доступу до обчислювальної техніки;
- захист даних у мережі Інтернет;
- захист даних на носіях інформації.

Серед заходів безпеки, яких повинен дотримуватися кожен користувач, перше місце займає його особиста організованість і відповідальне ставлення до зберігання важливих даних.

Для забезпечення інформаційної безпеки в мережі Інтернет недостатньо захистити дані на комп’ютері-клієнті або комп’ютері-сервері. Захист даних у мережі Інтернет повинен як мінімум супроводжуватись використанням підключень, захищених шифруванням. Використання протоколу зашифрованого підключення забезпечує більш ефективний захист даних. Наприклад, за замовчуванням Google шифрує з’єднання з Gmail, а також при виборі інших сервісів Google, наприклад Google Disk, активується протокол шифрування SSL, який використовується до завершення сеансу роботи.

4.3. Загальний підхід до технічного захисту інформації

Класична схема обробки та розповсюдження інформації [24] відома з теорії інформації та наведена на рис. 4.7.

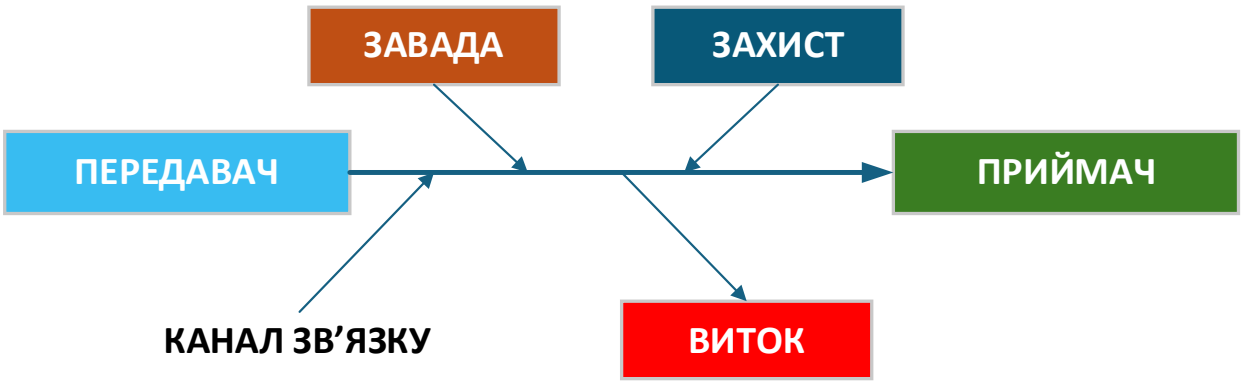


Рисунок 4.7 – Класична схема обробки, розповсюдження та захисту інформації

Ця схема містить передавач інформації, канал зв'язку (або канал зберігання інформації, чи обидва канали разом), та приймач (який може мати систему вторинної обробки) інформації. З позиції класичної теорії інформації канал зв'язку є найбільш уразливою ділянкою для дії завади.

Це ж правило діє і при розгляді проблем захисту інформації. Але з точки зору захисту інформації канал зв'язку можна розглядати з двох позицій:

1. Як канал витоку.

2. Як ділянку, що зручна для захисту.

Технічний захист інформації є цілим комплексом робіт: від обладнання приміщень засобами обмеження доступу, шифрування даних, інформування колективу та виявлення передбачуваних каналів витоку до постійного оновлення засобів та способів підтримки безпеки.

Основними об'єктами захисту інформації є:

- інформаційні ресурси, які мають відомості, віднесені до таємної або конфіденційної інформації;

- засоби і системи інформації (інформаційно-обчислювальні комплекси), у тому числі: програмні засоби (системи управління базами

даних, операційні системи тощо), автоматизовані системи управління, системи зв’язку і передачі даних, технічні засоби прийому, передачі і обробки інформації обмеженого доступу, їх інформативні фізичні поля. Тобто системи і засоби, що безпосередньо обробляють інформацію, яка віднесена до таємної або конфіденційної;

- системи, що не віднесені до засобів і систем інформатизації, але розташовані в приміщеннях, де оброблюється конфіденційна інформація. Такі технічні засоби і системи звуться додатковими технічними засобами і системами (ДТЗС). До них відносять: технічні засоби відкритого телефонного зв’язку, засоби оповіщення, системи пожежної та охоронної сигналізації, радіофікації, годинофікації, електропобутові прилади та інші, а також самі приміщення, що призначені для обробки інформації з обмеженим доступом.

Окремі технічні засоби або група технічних засобів, що призначені для обробки конфіденційної інформації, разом з приміщеннями, де вони розташовуються, складають об’єкт технічних засобів прийому, переробки, зберігання і передачі інформації.

Об’єкт технічного захисту інформації – це будова, приміщення, окремий основний технічний засіб або їх група, об’єднана загальним призначенням, які підлягають захисту від технічних розвідок. Об’єкт може бути однією зі складових, але він може поєднувати в собі і всі зазначені складові.

Все залежить від того які, по-перше, види інформації необхідно захистити та, по-друге, в яких приміщеннях об’єкту циркулює ця інформація. Якщо це лише один вид інформації, що може циркулювати в одному або групі приміщень будівлі, виконують лише заходи з захисту цього виду інформації та певних приміщень.

Якщо треба захищати велику кількість приміщень (велику група, яка, наприклад, складається з підгруп), об’єкт захисту може складатися зі всієї будівлі.

Якщо необхідно захистити декілька видів інформації, що циркулює в приміщеннях об’єкту, то використовується комплексний захист інформації.

Питання технічного захисту інформації розбиваються на два великих класи задач:

- захист інформації від несанкціонованого доступу (НСД), а саме доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу;

- захист інформації від витоку технічними каналами (акустичні канали, оптичні канали тощо).

Для забезпечення технічного захисту інформації створюється комплекс технічного захисту інформації, що є складовою КСЗІ.

Захист від НСД може здійснюватися в різних складових інформаційної системи:

- прикладне та системне програмне забезпечення;

- апаратна частина серверів та робочих станцій;

- комунікаційне обладнання та канали зв’язку;

- периметр інформаційної системи.

Контрольні питання

1. Що входить до складу інформаційної інфраструктури?

2. Які існують реальні та потенційні загрози національній безпеці України в інформаційній сфері?

3. Які існують режиму доступу до інформації?

4. Чим зумовлені загрози безпеці інформації в Україні?

5. Які основні принципи формування і проведення державної політики в сфері технічного захисту інформації?

6. Що містять технічні заходи з захисту інформації?

7. Які є формальні та неформальні засоби захисту інформації?

8. Що відноситься до апаратних засобів захисту інформації?

9. Що відноситься до програмних засобів захисту інформації?

10. Що відноситься до криптографічних засобів захисту інформації?

11. Що відноситься до елементів організаційної безпеки?

12. Що відноситься до елементів законодавчої безпеки?

13. Що входить до складу концептуальної моделі інформаційної безпеки?

14. Як класифікуються загрози інформаційній безпеці?

15. На яких принципах базується інформаційна безпека в мережі Інтернет?

16. Які існують загрози інформаційній безпеці в мережі Інтернет?

17. З чого складається класична схема обробки, розповсюдження та захисту інформації?

18. Що є основними об’єктами захисту інформації?

5. ЗАСОБИ І МЕТОДИ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ АКУСТИЧНОЇ ІНФОРМАЦІЇ

5.1. Несанкціонований доступ до інформації

Актуальність і особлива важливість забезпечення безпеки функціонування автоматизованих систем обробки інформації пов'язана:

- з різким збільшенням потужностей сучасних комп'ютерів;
- зі збільшенням обсягів інформації, які накопичуються, зберігаються та обробляються;
- з зосередженням в єдиних базах даних інформації різного призначення і приналежності;
- зі стрімким розвитком спектра програмних засобів, що не задовольняють елементарним вимогам безпеки;
- з розширенням мережевих технологій, зв'язком локальних мереж віддалених офісів через мережу Інтернет.

Технічні і програмні засоби добування інформації – це подолання системи захисту, обмеження або заборона доступу до них посадових осіб, дезорганізації роботи технічних засобів, виведення з ладу комунікаційних і комп'ютерних мереж, усього високотехнологічного забезпечення функціонування системи управління.

Під способами несанкціонованого доступу до конфіденційної інформації прийнято розуміти різні методи, за допомогою яких зловмисник може отримати цінні конфіденційні дані організації.

Способи несанкціонованого доступу до інформації [6]:

- підкуп співробітників;
- вербування співробітників;
- вивідування даних;
- підслуховування;
- спостереження;

- крадіжка даних;

- несанкціоноване копіювання;

- підробка та модифікація інформації;

- підключення;

- перехоплення;

- фотографування;

- часткове ознайомлення;

- легальні методи.

Також окремо можна виділити знищення інформації як серйозну загрозу діяльності організації.

Підкуп співробітників. Зловмисникові не складає труднощів скористатися ініціативою працівника (інсайдера – особи, яка має доступ до конфіденційної інформації в силу свого службового становища або родинних зв'язків), незадоволеного ситуацією в організації. Практика показує, що деякі співробітники або мають нагальну потребу в грошах, або готові передати конфіденційну інформацію через жадібність. Важливо розуміти, що мотиви зловмисника часто виходять за межі лише фінансової вигоди. Існують випадки, коли працівники надають секретні відомості з помсти за образи з боку керівництва. Для здобуття цінної інформації конкуренти можуть звертатися не тільки до високопосадовців або ключових фахівців, а й до рядових співробітників.

Вербування співробітників. Вербування та підкуп співробітників часто є тривалим процесом. Агенти конкурента можуть місяцями вивчати працівника та його родину, щоб знайти найефективніший спосіб співпраці і зробити з нього агента, який працюватиме на інтереси конкурентної компанії. Іноді для того, щоб залучити інсайдера до співпраці, збирають компрометуючі матеріали, застосовують загрози, психологічний тиск або навіть агресивні методи залякування. Також є випадки, коли зловмисники використовують м'якіші способи для отримання конфіденційної інформації.

Вони можуть діяти непрямо, передаючи кошти через посередників або навіть через відомих осіб, які займаються громадською діяльністю.

Вивідування даних. Методи збору інформації часто мають складний і продуманий характер. Однією з поширених практик є переманювання спеціалістів через створення фальшивих вакансій. Такі оголошення публікуються з метою заманити фахівця в пастку. Типова особливість цього підходу – обіцянки великих премій, пільг та значного підвищення доходу. На випробувальному терміні новачку пропонують зарплату, яка вдвічі перевищує його поточний оклад у компанії конкурента. Багато спеціалістів, не підозрюючи небезпеки, потрапляють у таку пастку, охоче діляться своїми знаннями та досвідом, надаючи конкуренту цінну інформацію. Після закінчення випробувального терміну, коли вся необхідна інформація вже отримана, співробітнику відмовляють у подальшій співпраці.

Іншим методом збору інформації є спроба працевлаштування. Конкурент може направити свого агента на співбесіду з метою отримати важливі дані про компанію, зокрема, про її проблеми, стратегії, слабкі місця тощо.

Однак найбільш ефективним способом збору інформації є спілкування з родичами, друзями та знайомими інсайдерів. Саме тому кожен співробітник, який має доступ до конфіденційної інформації, повинен правильно формувати свою політику спілкування з оточенням і дотримуватися відповідної поведінки в повсякденному житті.

Підслуховування. Підслуховування відноситься до найпопулярніших способів видобутку цінної інформації. Підслуховування здійснюється такими методами:

- шляхом використання радіозакладок та диктофонів;
- шляхом використання програмного забезпечення для отримання значних відомостей під час телефонних переговорів, передачі радіосигналів;
- шляхом використання різної техніки, що уловлює (перехоплює) аудіосигнал.

Існує також практика підслуховування за умов таємної присутності. Для запобігання витоку інформації використовують пристрої, що глушать передачу сигналу через створення радіоперешкод. Проте ці пристрої не можуть запобігти запису розмови за допомогою диктофонів, які можуть бути приховано встановлені поблизу. Пристрої для підслуховування часто є складними і надзвичайно непомітними. Зловмисники зазвичай надають перевагу підслуховуванню в громадських місцях, де підслуховуючий пристрій може бути легко прихований і закріплений на тілі, залишаючись непомітним.

Спостереження. Спосіб передбачає застосування різних технічних пристроїв. Спостереження може вести як одна, так і кілька осіб. При груповому спостереженні один, рідше два спостерігачі завжди знаходяться в безпосередній близькості та інформують решту групи про поточну ситуацію. Цей спосіб використовують для з'ясування особливостей поведінки співробітника, маршрутів його пересування, іншої важливої інформації. У такий спосіб встановлюють факт підготовки організації до різноманітних заходів. Сучасні системи дозволяють стежити за об'єктами при низькому рівні освітлення та на великих відстанях. Навіть за умов практично повної темряви на відстані приблизно одного кілометра спостерігач легко зможе визначити потрібний об'єкт і впізнати людину.

Відстеження розташування об'єкта є важливою частиною стеження. Зазвичай для спрощення спостереження об'єкта встановлюють радіомаяки. Пристрої стеження відрізняються компактними розмірами і часто залишаються непомітними. Їх можна вмонтувати у фари автомобіля, замаскувати на деревах, землі. Деякі прилади маскуються під предмети гардеробу (ремені, капелюхи).

Крадіжка даних. Найефективнішим способом запобігання крадіжці даних у компанії є встановлення постійного контролю за діями співробітників. Близько 80 % людей не візьмуть важливі документи, оскільки це суперечить їх моральним принципам. Усунення спокус викрасти

конфіденційну інформацію допомагає значно знизити ризик її крадіжки та забезпечити безпеку організації.

Несанкціоноване копіювання. Копіювання інформації виконується в різний спосіб, зокрема за допомогою технічних засобів. Захист від копіювання електронної інформації розроблено давно, проте зробити ксерокопію цінних документів може кожен співробітник організації. Тому необхідно встановлювати контроль за використанням копіювальних апаратів.

Підробка та модифікація інформації. Зловмисники можуть підробляти інформацію з метою здобуття секретних даних. Часто підробці піддаються листи, рахунки та бухгалтерська документація. Підготовка до підробки та модифікації інформації зазвичай включає промислове шпигунство, яке активно практикується в багатьох країнах. Одним з видів фальсифікації є пряма підробка, коли змінюються смс-повідомлення з метою отримання конфіденційних відомостей. Проте найбільш поширеним методом є використання комп'ютерних вірусів, які здатні змінювати програмне забезпечення для крадіжки документів та інформації.

Підключення. Підключення може здійснюватися як контактними, так і безконтактними методами. Зловмисники можуть підключатися до різних ліній для отримання інформації, таких як лінії периферійних пристроїв великих і малих ЕОМ, радіомовні лінії, лінії для залів нарад, диспетчерські, а також лінії передачі даних. Можливо також підключення до ліній живлення, заземлення та оптоволоконних мереж. Безконтактне підключення дозволяє здійснити підключення на великій відстані від об'єкта. Для цього можуть використовуватися, наприклад, кільцеві трансформатори.

Перехоплення. Для перехоплення інформації можуть використовуватися такі пристрої:

- панорамні аналізатори;
- антенні підсилювачі широкосмугового типу;
- кінцева апаратура;
- антенні системи.

Ресивери здатні перехоплювати інформацію, що передається через електромагнітні хвилі, як наддовгі, так і короткі. Діапазон їхнього охоплення дуже широкий. Сучасні засоби перехоплення дозволяють встановлювати радіоконтакт на відстані кількох десятків тисяч кілометрів. Загроза полягає в тому, що навіть без повної розшифровки отриманої інформації зловмисники можуть зробити важливі висновки про діяльність організації.

Часткове ознайомлення. Отримати доступ до конфіденційної інформації часто виявляється неможливим, але навіть часткове ознайомлення з нею може задовольнити інтереси зловмисника. Випадкове або навмисне розкриття документів, що потрапляють до очей сторонніх осіб, залишений увімкнений монітор з важливими відомостями – це лише кілька прикладів. Такий метод можна застосувати, якщо в організації часто порушується виробнича дисципліна. Для часткового отримання інформації також можуть використовуватися тонкі оптоволоконні кабелі з мікрокамерами, які можна непомітно провести через замкову щілину.

Особливо небезпечними є люди з розвиненою зоровою пам’яттю, включаючи фотографічну. Відомі випадки, коли агенти конкурентів могли запам’ятовувати важливі дані, просто поглянувши на документи. Такі крадіжки неодноразово стосувалися розробок відомих дизайнерів і модельєрів, чиї робочі процеси могли бачити, здається, випадкові відвідувачі. Важливо розуміти, що зловмисники з хорошою пам’яттю часто проходять спеціальні курси, які навчають їх швидко вибудовувати логічні ланцюжки і робити висновки, що дозволяє їм не тільки запам’ятовувати цінну інформацію, а й миттєво розкривати стратегії та плани.

Фотографування. Отримання інформації за допомогою фотографування дозволяє зловмисникам залишатися непомітними. Сучасні об’єктиви та фотоапарати здатні робити знімки на відстані кількох сотень метрів, забезпечуючи чітке зображення. Фотографування в інфрачервоному діапазоні дозволяє отримувати дані з документів, в яких були внесені виправлення, а також відновлювати інформацію з документів, які частково

згоріли. Фотокамера може бути прихована в годиннику, виглядати як гаманець, запальничка, портсигар або навіть бути виконана у вигляді пластикової картки.

Легальні методи. Більшість компаній надають перевагу збору інформації законними методами. Для цього співробітники можуть брати участь у різноманітних офіційних заходах. За допомогою мозкового штурму та колективної роботи вони роблять висновки, які дозволяють виявити важливі плани та стратегії конкурентів. Збір даних здійснюється через торгових партнерів, клієнтів, постачальників, підрядників, профспілки та стажерів. Тісні зв'язки з медіа та журналістами також сприяють отриманню цінної інформації.

Знищення інформації. Існує багато випадків використання диверсійних методів для знищення цінної інформації, що може здійснюватися різними доступними способами. Такі акти часто мають кримінальний або навіть терористичний характер. Для видалення важливих даних можуть застосовуватися спеціальні вірусні програми, звані «логічними бомбами». Наприклад, у педагогічному центрі в Ізраїлі (місто Хайфа) такий вірус знищив розроблюване програмне забезпечення, на яке було витрачено понад 7 000 годин роботи.

Деякі способи несанкціонованого доступу до інформації схематично зображені на рис. 5.1.

Нині переважна частина інформації видобувається з допомогою технічних засобів. Технічні засоби суттєво розширюють та доповнюють можливості людини щодо добування інформації, забезпечуючи:

- знімання інформації з носіїв, які недоступні органам почуттів людини;

- добування інформації без порушення меж контрольованої зони;

- передачу інформації практично в реальному масштабі часу в будь-яку точку земної кулі;

- аналіз та обробку інформації в обсязі та за час, недосяжних людиною;

- консервацію і скільки завгодно тривале зберігання видобутої інформації.

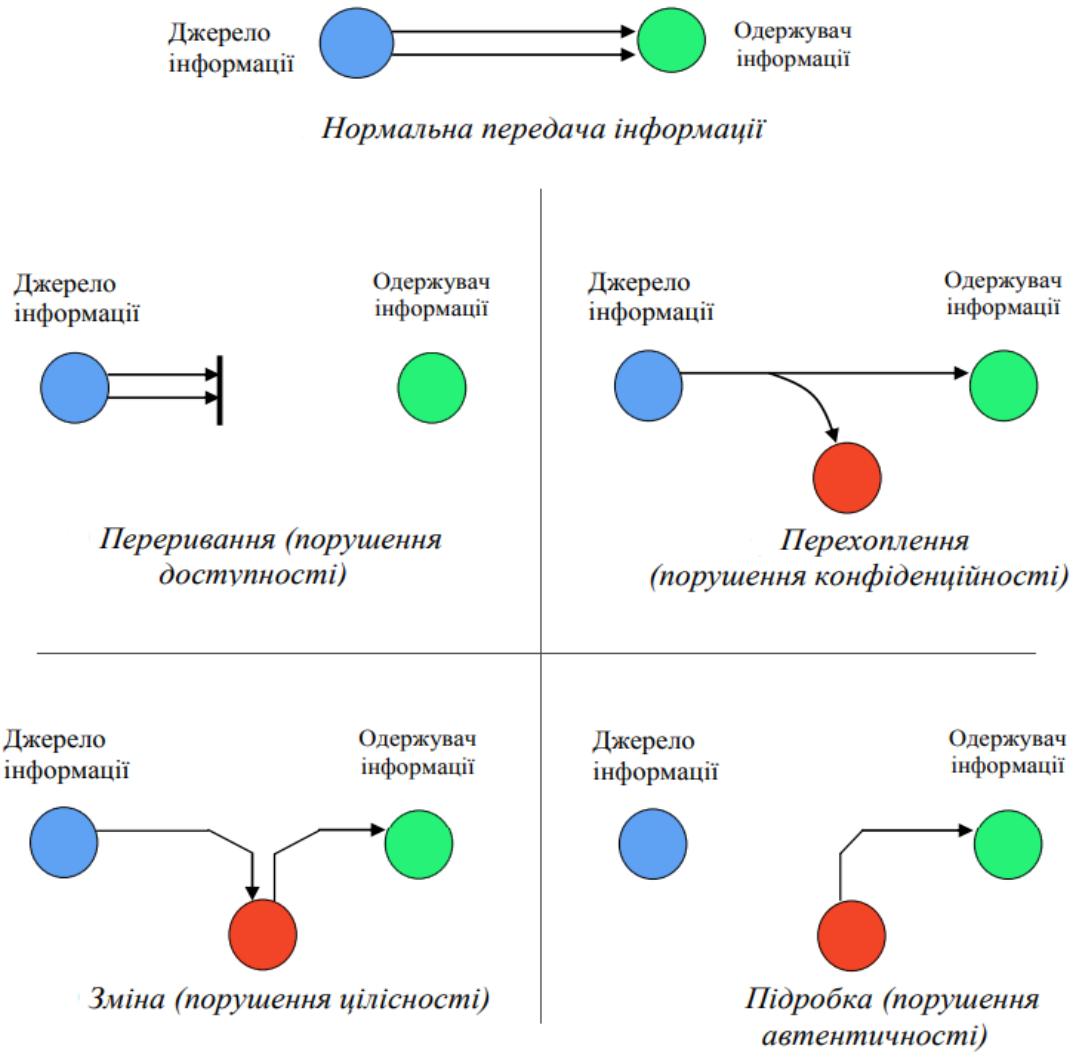


Рисунок 5.1 – Деякі способи несанкціонованого доступу

Класифікація технічних засобів для несанкціонованого добування інформації наведена на рис. 5.2.

Усі засоби можна поділити за такими ознаками:

1. За видом сигналів, що використовуються для отримання інформації:

- акустичні (мікрофонні закладні пристрої);
- механічні (стетоскопи);
- електричні (телефонні закладні пристрої).

2. За часом роботи:

- постійно функціонуючі;

- функціонуючі за детермінованим алгоритмом (за заданий інтервал часу, при появі акустичних сигналів, при відповіді на телефонний дзвінок, при подачі команди з пункту перехоплення).

Рисунок 5.2 – Класифікація пристроїв несанкціонованого зняття інформації

3. За часом передачі інформації:

- передача інформації в реальному часі;

- передача інформації в невеликі інтервали часу з використанням апаратури стискання.

4. За способом передачі інформації:

- накопичення інформації;

- радіоканал;

- фізична лінія (електрична мережа, радіотрансляційна мережа, телефонна лінія).

5. За способом електроживлення:

- з автономним електроживленням;

- з живленням від фізичної лінії (електричної мережі, радіотрансляційної мережі, телефонної лінії).

Одним із потенційних каналів несанкціонованого доступу до інформації є несанкціонована зміна прикладних та спеціальних програм порушником з метою отримання конфіденційної інформації. Ці зміни можуть мати на меті зміни правил розмежування доступу або обходу їх (при впровадженні в прикладні програми системи захисту) або організацію непомітного каналу отримання конфіденційної інформації безпосередньо з прикладних програм (при ін'єкціях в прикладні програми). Один з варіантів класифікації наведено на рис. 5.3.

Рисунок 5.3 – Класифікація програмних засобів добування інформації

Серед програмних засобів добування інформації можна виділити такі:

1. З використанням програм носіїв:

- люки (Trapdoors). Люк є прихованою точкою входу в програму, завдяки чому відкривається безпосередній доступ до деяких системних функцій. Люки зазвичай вставляють під час проєктування системи. Системні програмісти організують їх при налагодженні програми, але після завершення розробки їх прибирають або залишають для подальшої підтримки програми. Якщо ж люки використовуються для отримання несанкціонованого доступу (наприклад, для таємного контролю доступу до даної програми після її встановлення), тоді вони стають загрозою. Виявити люки можна шляхом аналізу роботи програм;

- логічні бомби (Logic Bombs). Логічна бомба – це комп'ютерна програма, яка призводить до пошкодження файлів або комп'ютерів. Пошкодження варіюється від спотворення даних до стирання всіх файлів та/або пошкодження комп'ютера. Логічну бомбу, як правило, вставляють під час розробки програми, а спрацьовує вона при виконанні деякої умови (час, дата, кодове слово, наявність або відсутність певних файлів, запуск програми від імені певного користувача тощо);

- троянські коні (Trojan Horses). Троянський кінь – це програма, яка призводить до несподіваних (і зазвичай небажаних) наслідків у системі. Особливістю троянського коня є те, що користувач звертається до цієї програми, вважаючи її корисною. Троянські коні здатні розкрити, змінити чи знищити дані чи файли. Їх вбудовують у програми широкого користування, наприклад, у програми обслуговування мережі, електронної пошти та ін. Антивірусні засоби не виявляють ці програми, але системи управління доступом мають механізми ідентифікації та обмеження їхньої дії;

- віруси (Viruses). Визначення вірусів дуже різноманітні, як і самі віруси. Найбільш поширене визначення: комп'ютерний вірус – це програма, яка здатна заражати інші програми, модифікуючи їх так, щоб вони включали копію вірусу (або його різновид). Залежно від області поширення та впливу

віруси діляться на руйнівні та неруйнівні, резидентні та нерезидентні, що заражають структури та коди початкового завантаження систем, системні файли, прикладні програми та ін. За час свого існування типовий вірус проходить чотири стадії: фаза спокою (вірус не діє, а чекає події, яка його активізує), фаза розмноження (вірус виконує своє копіювання), фаза запуску (вірус активується для отримання можливості виконувати свої функції), фаза виконання (вірус виконує свої функції).

2. Незалежні програми:

- утиліти схованого адміністрування (Backdoors). За своєю функціональністю багато чим нагадують різні системи адміністрування, розроблювані і розповсюджувані фірмами-розробниками програмних продуктів. Будучи встановленими на комп'ютер, утиліти прихованого адміністрування дозволяють віддалено виконувати майже повний спектр дій по адмініструванню та управлінню системою, даними тощо;

- програми-крадії паролів (Password Grabber) – це спеціально призначені програми для крадіжки паролів. Захоплення пароля є активним, безпосереднім впливом на комп'ютерну систему в цілому. Виконується за допомогою імітації реальної форми введення паролю або шляхом впливу на програмне забезпечення з формами введення паролів;

- intended-віруси. До intended-вірусів відносяться віруси, які не здатні розмножуватися через помилки або розмножуються тільки один раз – з авторської копії. З'являються найчастіше при невдалій перекомпіляції якогось існуючого вірусу, через недостатній рівень знань розробника;

- конструктор вірусів – це утиліта, призначена для виготовлення нових комп'ютерних вірусів на основі існуючих шаблонів;

- поліморфні генератори, як і конструктори вірусів, не є вірусами в буквальному значенні цього слова, оскільки в їх алгоритми не закладаються функції розмноження. Головною функцією подібного роду програм є шифрування тіла вірусу і генерація відповідного розшифровувача –

створення поліморфних вірусів (програмний код змінюється при кожному новому зараженні за допомогою шифрування);

- черв'яки (Worms). Черв'як – це програма, яка поширюється в системах та мережах по лініях зв'язку. Такі програми подібні до вірусів у тому відношенні, що вони заражають інші програми, а відрізняються від них тим, що вони не здатні самовідтворюватися. На відміну від троянського коня черв'як потрапляє в систему без відома користувача і копіює себе через мережу за допомогою деякого транспортного засобу (електронну пошту, віддалений запуск програм, віддалену реєстрацію тощо);

- зомбі (Zombie). Зомбі – це програма, яка приховано приєднується до інших підключених у мережу Інтернет комп'ютерів, і використовує комп'ютер для запуску атак, що ускладнює відстеження шляхів до розробника або розповсюджувача програми-зомбі. Зомбі використовують при атаках, спрямованих на відмову в обслуговуванні (DDoS атаки).

5.2. Захист інформації від витоку по технічних каналах

ТЗІ призначений для захисту інформації від витоку по технічних каналах витоку інформації.

На теперішній час для несанкціонованого зняття інформації широко використовуються технічні канали витоку інформації (ТКВІ).

Технічний канал витоку інформації – це сукупність небезпечних фізичних сигналів, середи їх розповсюдження та зберігання, об'єктів технічної розвідки, способів і засобів технічної розвідки, що можуть бути застосовані для зняття інформації з об'єкту, що охороняється.

Небезпечний фізичний сигнал (небезпечний сигнал) – це сигнал, що містить інформацію, яку необхідно захищати.

У нашій країні прийнято поділяти ТКВІ за такою класифікацією:

- акустичні канали витоку інформації, куди входять також канали з акустично-електричними перетвореннями;

- радіотехнічні канали витоку інформації, куди входять, по-перше, відкриті канали радіотехнічного зв'язку та, по-друге, канали, що утворюються за рахунок паразитних випромінювань та наводок;

- оптичні канали витоку інформації;

- речовий канал витоку інформації, який визначається людським фактором.

Акустичні канали витоку інформації характеризуються тим, що середовищем для поширення мовленнєвих сигналів є повітря. Витік акустичної інформації за межі огороджувальних конструкцій може відбуватися трьома основними шляхами:

- мембранний ефект, що виникає через коливання тонких, відносно легких елементів конструкцій (наприклад, віконного скла, фанерних, гіпсокартонних або пластикових перегородок), які здатні прогинатися під впливом звукових хвиль;

- через тріщини, отвори, щілини та інші акустичні отвори, тобто пряме розповсюдження акустичних коливань у просторі;

- перетворення акустичних коливань у віброакустичні, а потім знову в акустичні коливання. У цьому випадку частина енергії акустичних коливань перетворюється в механічні вібрації твердих частинок матеріалу, не переміщуючи речовину, і може потім бути передана через ці вібрації.

Радіотехнічний (радіоелектронний) канал витоку інформації використовує електричний струм або електромагнітне поле як носій інформації. Це один з найбільш інформативних каналів, оскільки незахищені засоби передачі, прийому та обробки інформації, що працюють від електричного струму, утворюють радіоелектронний канал витоку. У цьому каналі носієм інформації є електричний струм і електричне поле, що охоплюють частотний діапазон від звукових коливань до десятків гігагерців.

Оптичний (оптико-електронний) канал витоку інформації виникає, коли лазерний промінь опромінює вібруючі в акустичному полі тонкі віддзеркалювані поверхні, такі як скло вікон, дзеркала чи картини. Відбите

лазерне випромінювання модулюється за амплітудою і фазою, після чого воно приймається оптичним приймачем, і при демодуляції виділяється мовленнєва інформація. Для перехоплення таких даних використовуються локаційні системи, зокрема «лазерні мікрофони», які працюють у близькому до інфрачервоного діапазоні і мають дальність дії до кількох сотень метрів.

Речовий (матеріально-речовий) канал витоку інформації передбачає отримання даних з відходів виробничої та трудової діяльності. Це можуть бути зіпсовані накладні, фрагменти документів, чернетки листів, браковані деталі, панелі, корпуси пристроїв нових моделей техніки, що розробляються на підприємстві. Відомо, що іноді для збору інформації «промислові шпигуни» можуть активно переглядати сміттєві контейнери, що часто дає цінні відомості. Основними джерелами витоку інформації в матеріально-речовому каналі є:

- чернетки документів, макети матеріалів, вузлів та пристроїв;
- відходи діловодства і видавничої діяльності;
- магнітні та інші носії інформації, що містять дані з обмеженим доступом;
- бракована продукція та її елементи;
- відходи виробництва, що містять демаскуючі речовини в газоподібному, рідкому або твердому вигляді;
- радіоактивні матеріали.

ТКВІ можуть бути природними та штучними, у тому числі створеними навмисно.

Природні ТКВІ утворюються на базі фізичних властивостей джерел виникнення небезпечних сигналів, самих небезпечних сигналів та середовища їх розповсюдження. Для навмисного створення ТКВІ можуть використовуватися зміни фізичних властивостей джерел та середовищ розповсюдження небезпечних сигналів, а також поданням спеціальних сигналів на окремі елементи приміщення. Це, як правило, робиться шляхом

конструктивних змін джерел та конструкції об’єкту, де розповсюджуються небезпечні сигнали.

Але для зняття інформації з ТКВІ завжди використовується апаратура технічної розвідки.

Крім того, сама апаратура технічної розвідки, що розміщена на об’єкті, який охороняється, утворює навмисний канал витоку інформації.

Проведення робіт з розробки, впровадження та підтримки і перевірки працездатності системи ТЗІ на об’єкті, що охороняється, вимагає проведення певних організаційно-технічних заходів. Їх проведення призначено для забезпечення надійності захисту інформації на об’єкті. Одним із найважливіших завдань при цьому є виявлення та блокування всіх потенційних каналів витоку інформації з об’єкту.

Друге завдання – це постійна перевірка працездатності та надійності функціонування системи технічного захисту. Саме в цих заходах полягає сутність ТЗІ.

На рис. 5.4 наведено загальну класифікацію видів інформації, яка може бути об’єктом злочинних посягань. Це оптична, акустична, електронна, електромагнітна та письмова (друкована) інформація.

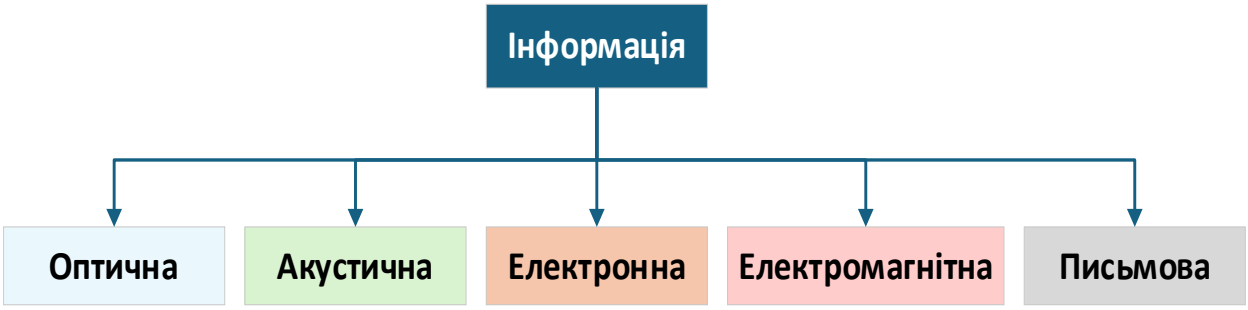


Рисунок 5.4 – Загальна класифікація видів інформації

Відповідно, всі види інформації мають різну фізичну природу її походження, носіїв і каналів розповсюдження та зберігання, або різні параметри одного й того ж явища, яке може бути покладене в основу для її переносу чи зберігання.

У відповідності до прийнятої класифікації поділу ТКВІ слід розглянути почергово фізику утворення акустичних, радіотехнічних та оптичних каналів.

При розгляді фізичних основ утворення акустичних каналів витоку інформації особливу увагу слід приділити акустично-електричним перетворенням. Сама назва каналів витоку свідчить про те, що небезпечними сигналами, що можуть витікати через нього, є акустичні сигнали.

Акустичний сигнал – це механічні коливання часток пружного середовища. Отже, виходячи з цього визначення, акустичні сигнали можуть розповсюджуватися в будь-якому пружному середовищі. Єдине середовище, в якому розповсюдження акустичного сигналу неможливо – повний вакуум (відсутні частинки повітря, тобто немає пружного середовища).

Саме цим пояснюється можливість проходження акустичних сигналів через елементи будівельних конструкцій (стіни, стелі, підлоги, двері, скло вікон, труби тощо).

Акустичний сигнал може безпосередньо прийматися слуховими органами людини та інших живих істот. При цьому, людина сприймає акустичні коливання в діапазоні частот від 20 до 20000 Гц. Цей діапазон зветься звуковим діапазоном частот.

Частоті 1 Гц відповідає коливання, яке утворює повний період за 1 сек., як наведено на рис. 5.5. Отже, частота сигналу – це кількість повних періодів коливання за 1 сек. Крім звукового, розділяють інфразвуковий (від 0 до 20 Гц) та ультразвуковий (вище 20 000 Гц) діапазони частот. Ці частоти чує більшість тварин, але люди їх не чують.

Залежно від фізичної природи виникнення інформаційних сигналів, середовища поширення акустичних коливань і способів їхнього перехоплення технічні канали витоку акустичної (мовленнєвої) інформації можна розділити на повітряні, вібраційні, електроакустичні, оптико-електронні і параметричні.

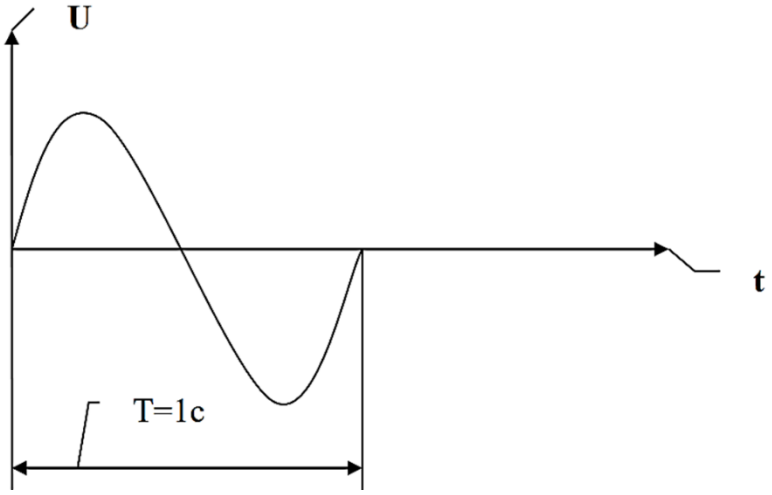


Рисунок 5.6 – Гармонійне коливання з частотою 1 Гц

Щоб передати звук через канали зв’язку або зберегти його в пристроях для запису, акустичний сигнал потрібно перетворити в електричний. Для цього використовують спеціальний перетворювач – мікрофон. Для зворотного перетворення акустичного сигналу в електричний застосовуються гучномовці. Принцип перетворення акустичного сигналу в електричний показано на прикладі вугільного мікрофону, зображеного на рис. 5.7.

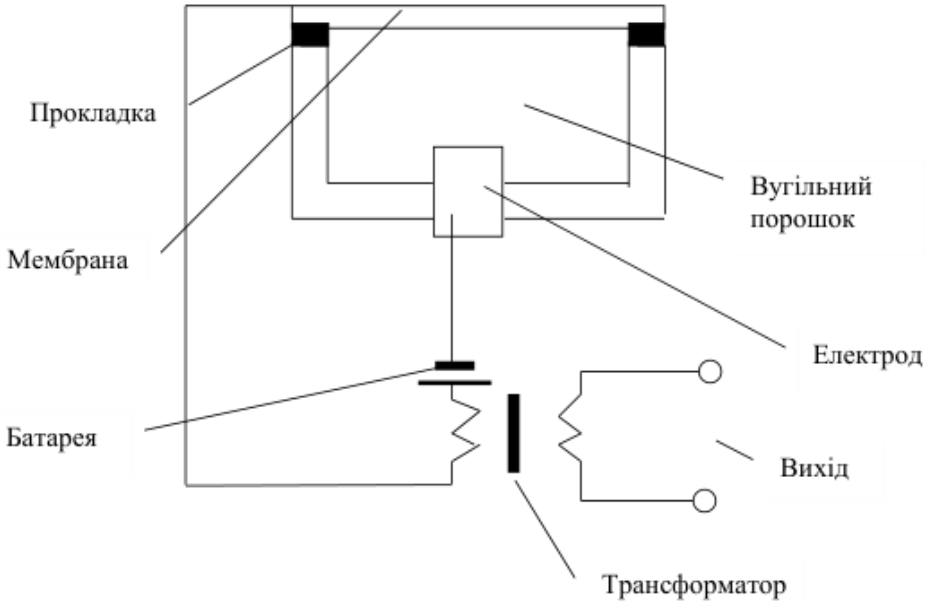


Рисунок 5.6 – Будова вугільного мікрофону

Вугільний мікрофон є найпростішим типом мікрофона, який має найгірші характеристики перетворення та спричиняє найбільші спотворення сигналів. Наразі використовуються динамічні, конденсаторні та електретні

мікрофони, які є необхідними компонентами всіх пристроїв для зняття акустичної інформації.

Акустичну інформацію можна отримати не лише за допомогою технічних засобів розвідки, але й випадковим прослуховуванням, без спеціальних намірів отримати цю інформацію. Для її перехоплення можуть застосовуватися високочутливі мікрофони. Якщо їх використання неможливе, застосовують спрямовані мікрофони, що мають вузьку діаграму спрямованості. Перехоплену мовленнєву інформацію можна записувати за допомогою портативних пристроїв (диктофонів) або передавати через радіоканали, мережі електроживлення, оптичні канали, з'єднувальні лінії, сторонні провідники чи інженерні комунікації.

Фізичні принципи каналів витоку, що виникають через паразитні випромінювання та наводки пов'язані з тим, що кожен електронний пристрій генерує паразитне випромінювання на своїй індивідуальній частоті. Це явище спричинене численними паразитними ємнісними з'єднаннями, які виникають між проводами, друкованими схемами, ніжками електронних компонентів тощо.

У процесі виникають нові непередбачувані паразитні ланцюги, появу яких неможливо точно передбачити під час проєктування або виробництва пристроїв. Ці паразитні ланцюги призводять до утворення паразитних позитивних зворотних зв'язків, що перетворює будь-який (навіть низькочастотний) електронний пристрій (наприклад, підсилювач) на передавач, який випромінює паразитні коливання в ефір на високих та надвисоких частотах.

У процесі розробки та виробництва більшості побутових пристроїв ці випромінювання часто ігноруються, оскільки вони не впливають на основні функції апаратури. Однак, у розробці спеціальних або захищених пристроїв їм приділяється значна увага.

Через те, що ці коливання є високочастотними, вони, навіть маючи невелику потужність, можуть поширюватися на сотні метрів. Оскільки в

будь-якій апаратурі є нелінійні елементи (транзистори та мікросхеми), на них відбувається модуляція паразитного випромінювання інформаційними сигналами, що обробляються в апаратурі.

Окрім того, що такі сигнали можуть бути перехоплені з ефіру, вони також викликають утворення наводок.

Наводка – це сигнал, що виникає в будь-якому провіднику (наприклад, на трубах центрального опалення) через явище самоіндукції. Коли змінне електромагнітне поле (електромагнітна хвиля) потрапляє на нерухомий провідник, воно викликає появу змінного струму в цьому провіднику.

Оскільки паразитне випромінювання містить небезпечні сигнали, їх можна зняти з будь-яких струмопровідних конструкцій та мереж.

Фізичні принципи оптичних каналів витоку інформації не потребують детального розгляду, оскільки ці питання вивчаються в курсі спеціальної техніки.

Під технічним каналом витоку інформації розуміють сукупність об’єкта розвідки, технічного засобу розвідки (ТЗР), за допомогою якого збирається інформація про об’єкт, і фізичного середовища, де розповсюджується інформаційний сигнал.

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх розповсюдження і способів перехоплення ТЗР більш детально технічні канали витоку інформації можна поділити на:

- радіоканали (електромагнітне випромінювання радіодіапазону);
- електричні (засоби провідникового зв’язку та різні струмопровідні комунікації);
- акустичні (розповсюдження звукових коливань);
- оптичні (електромагнітне випромінювання в інфрачервоній і ультрафіолетовій частини спектру).

На рис. 5.7 наведено загальну характеристику каналів витоку оптичної, акустичної, електронної та електромагнітної інформації. Деякі з цих каналів

можуть бути комбінованими, тобто бути каналами витоку для кількох видів інформації.

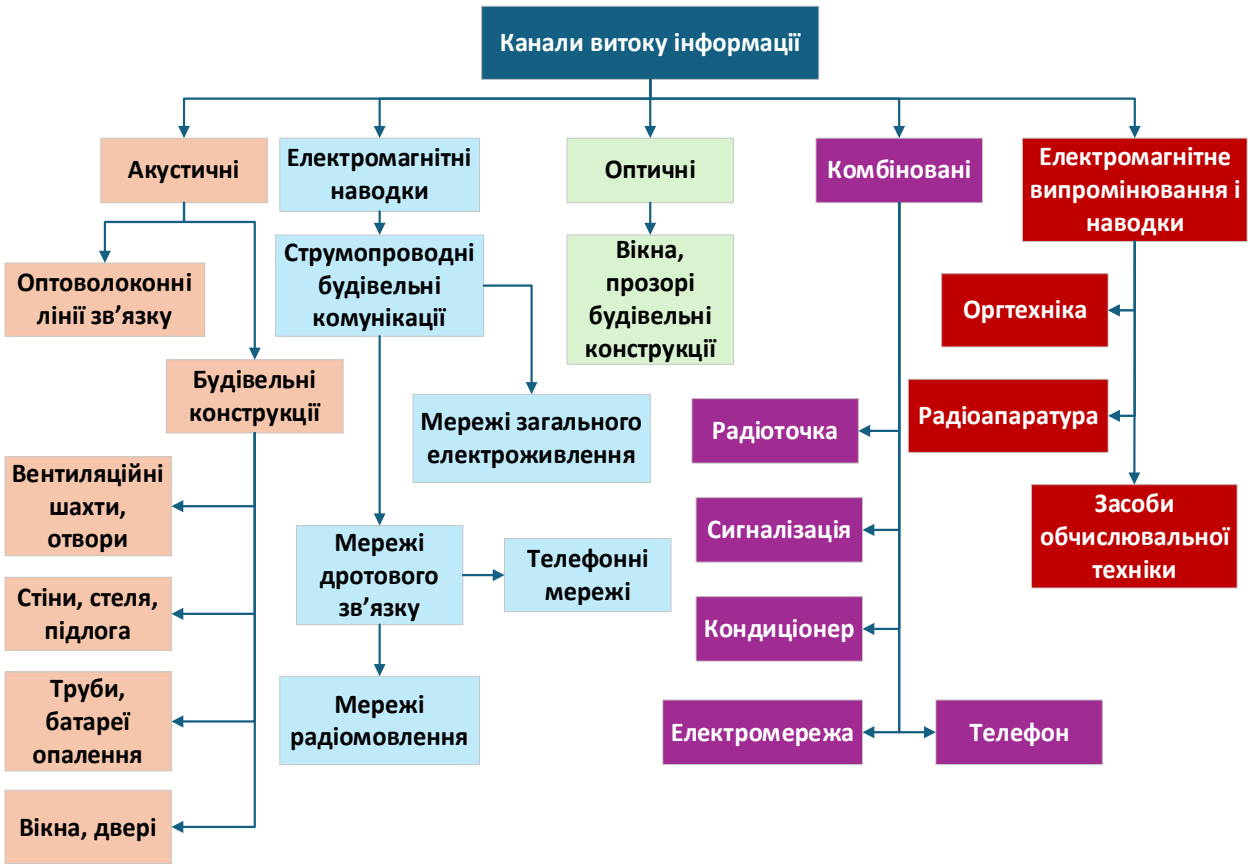


Рисунок 5.7 – Канали витоку інформації

Наприклад, скляні конструкції та вікна можуть служити каналами витоку не лише для акустичної та оптичної інформації, але й для електронної та друкованої (наприклад, для зчитування тексту з екрану комп'ютера). Телефонний апарат може бути використаний для перехоплення акустичної, електронної та електромагнітної інформації тощо.

Таким чином, для розуміння принципів технічного захисту інформації необхідно знати методи та засоби її зняття, а також оцінити реальні загрози, пов'язані з використанням різних каналів витоку.

На рис. 5.8 наведено основні методи і засоби комбінованого зняття акустичної інформації. Спочатку зазначено канал витоку, а потім перераховані можливі способи та засоби зняття інформації. Залежно від розташування та облаштування об'єкта, що охороняється, можуть бути

використані різні канали витоку, а також різні методи перетворення та засоби перенесення інформації.

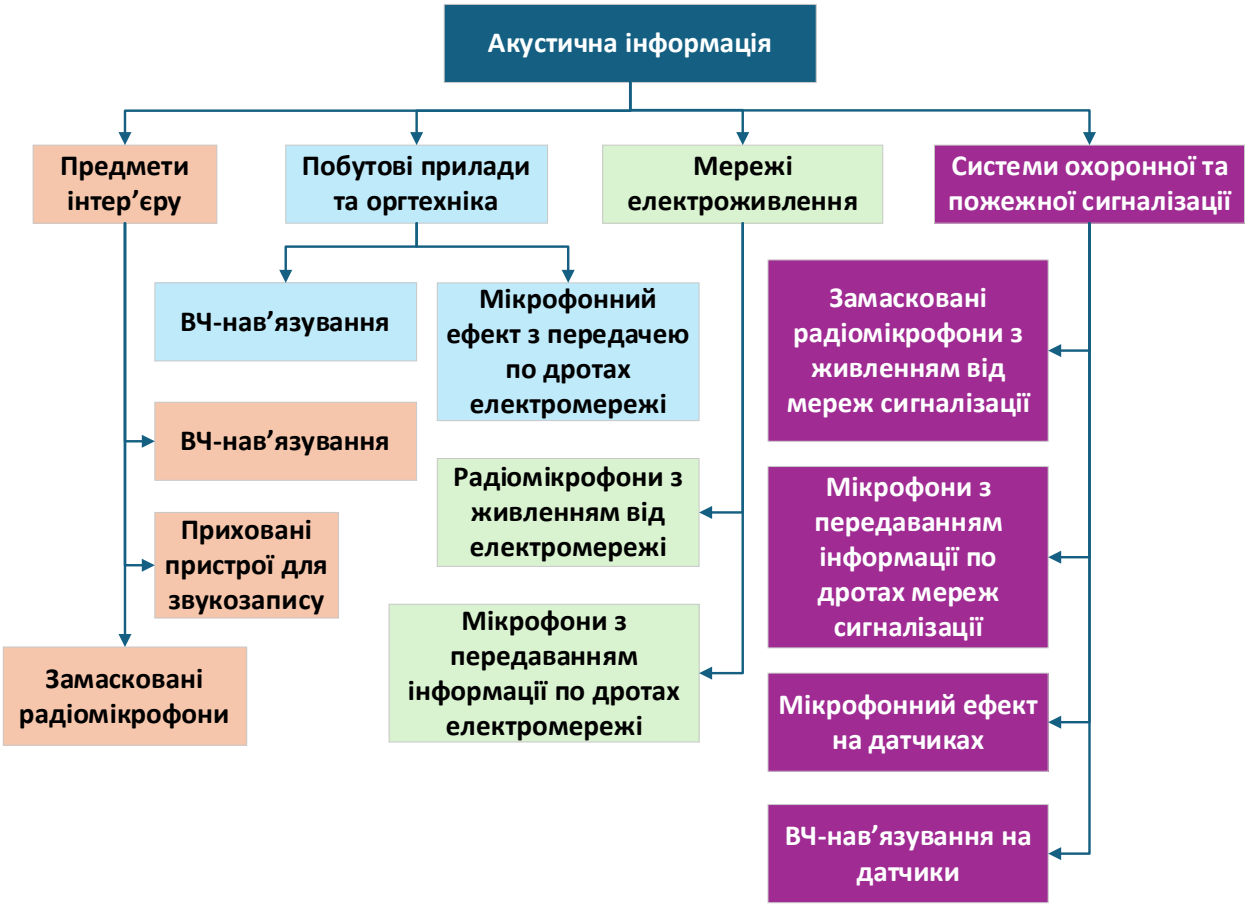


Рисунок 5.8 – Комбіновані методи та засоби зняття акустичної інформації

Наприклад, акустичну інформацію можна зняти в приміщенні за допомогою радіомікрофона, що працює від електричної мережі, або ж за допомогою дротового мікрофону, який також підключений до мережі. У цьому випадку інформація передаватиметься через електричну мережу, і її можна перехопити навіть на трансформаторній підстанції.

Для отримання акустичної інформації з закритого приміщення все частіше застосовують метод ВЧ-нав'язування, коли для збору даних використовують предмети, виготовлені таким чином, щоб вони ставали резонансними елементами модуляційної системи. Під час ВЧ-опромінення цього предмета відбувається модуляція мовленнєвих сигналів високочастотним радіовипромінюванням, спрямованим на цей об'єкт.

У закритих приміщеннях акустичні сигнали можна отримувати завдяки тому, що будівельні елементи (стіни, підлоги, стелі, вікна, труби, закриті двері) виконують функцію акустичних мембран і ефективно передають звукові коливання. Тому за допомогою віброперетворювача та підсилювача можна зчитувати звукову інформацію через стіни, підлогу або стелю. Також акустичний сигнал можна виявити на відстані через зачинені вікна, направивши лазерне випромінювання на скло або використовуючи спрямований мікрофон. Методи та засоби зняття акустичної інформації з будівельних конструкцій наведені на рис. 5.9.

Рисунок 5.9 – Методи та засоби зняття акустичної інформації з будівельних конструкцій

Акустична інформація може також бути отримана з побутових приладів та апаратури зв'язку (рис. 5.10).

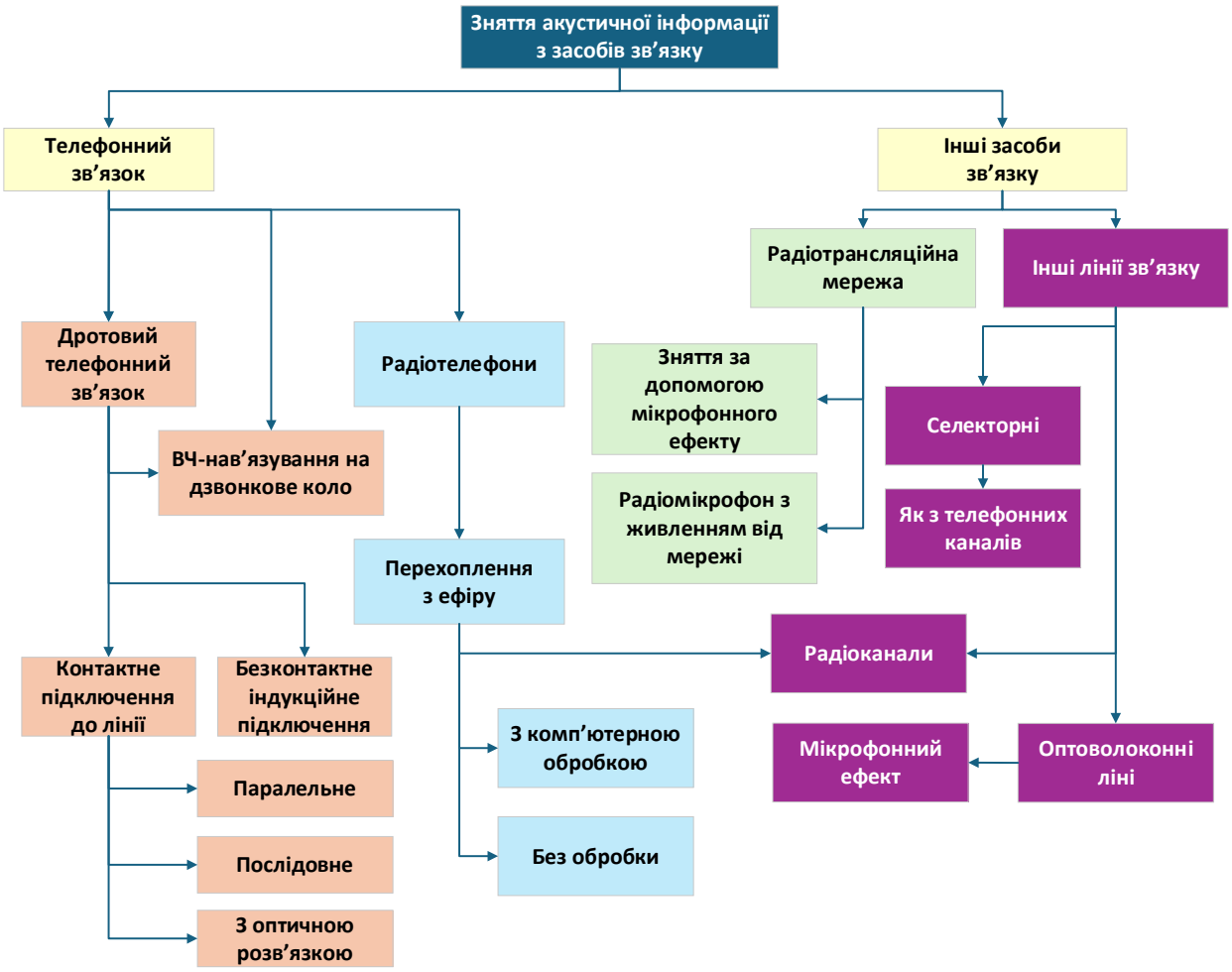


Рисунок 5.10 – Методи та засоби зняття акустичної інформації з засобів та ліній зв'язку

Наявність незахищеного телефонного апарату в режимному приміщенні дозволяє легко прослуховувати всю акустичну інформацію, навіть без використання радіомікрофонів чи складної спецтехніки і навіть у випадках, коли трубка лежить на апараті, і здається, що телефон вимкнений. Дзвінкове коло телефону містить елементи, що утворюють резонансний контур, який постійно підключений до телефонної мережі з напругою від 40 до 60 В. Частина цих елементів може бути мембраною, що коливається під впливом акустичних сигналів, тобто механічних коливань повітря. Крім того, можна застосовувати ВЧ-нав'язування або зчитування сигналів через

індукційні датчики чи датчики з високим вхідним опором, які підключаються до лінії зв'язку за межами приміщення або об'єкта, і які надзвичайно складно виявити.

Існує також постійна загроза встановлення радіомікрофону, який називають радіозакладним пристроєм або радіозакладкою. Подібні пристрої можуть використовувати злочинні угруповання або служби безпеки окремих фінансово-промислових груп. Види радіомікрофонів наведені на рис. 5.11.

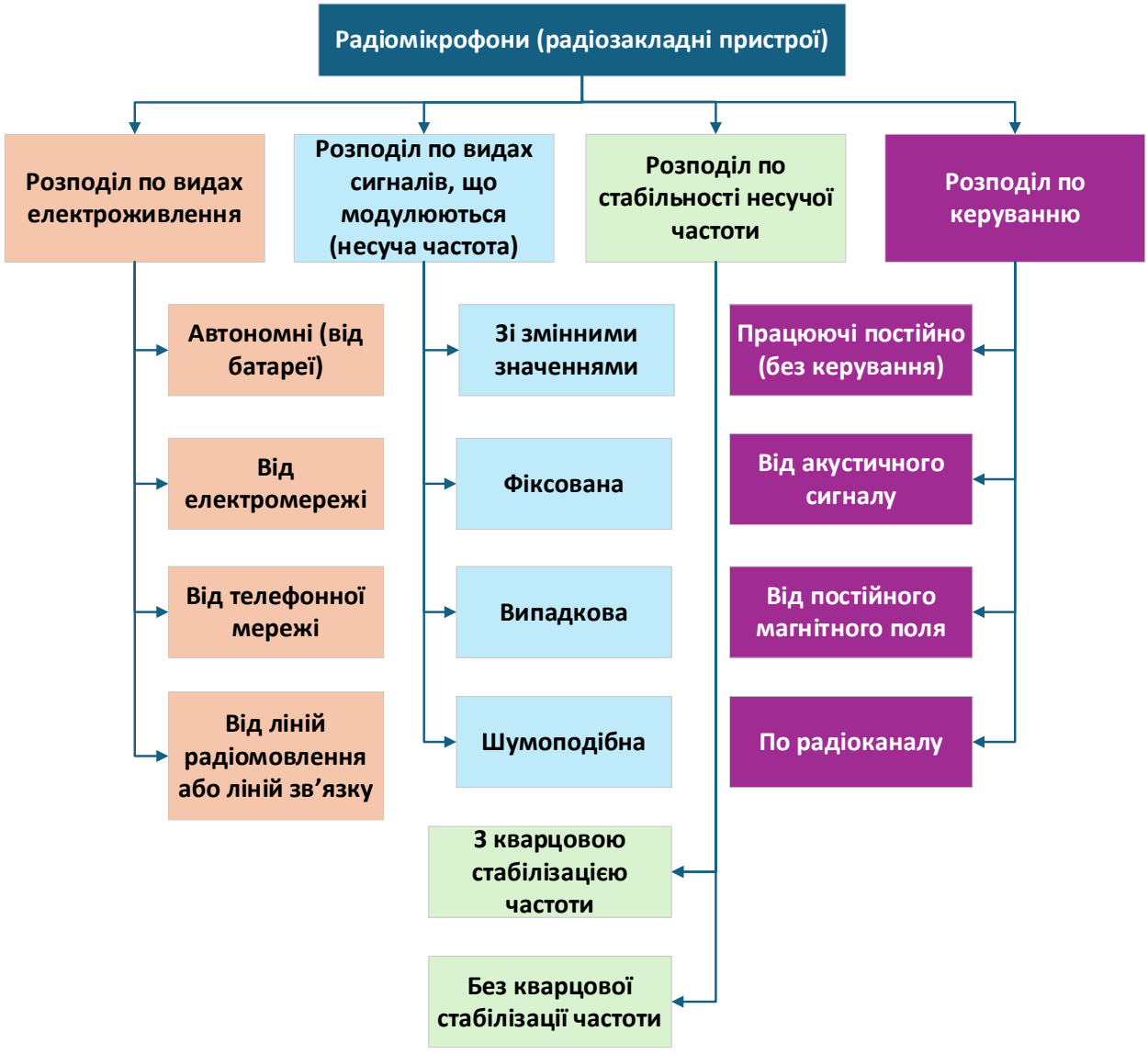


Рисунок 5.11 - Види радіомікрофонів для зняття акустичної інформації

З аналізу методів та засобів отримання акустичної інформації можна побачити, скільки загроз для її викрадення створює сучасна техніка. Однак, крім акустичної інформації, сучасні технології перехоплення також

дозволяють отримувати електронну та електромагнітну інформацію, що фактично дає змогу викрадати будь-які документи, які створюються, передаються та зберігаються в незахищених системах електронної обробки даних.

Отримання інформації, що зберігається в електронному вигляді, здійснюється завдяки паразитному електромагнітному випромінюванню, яке є присутнім у всіх електронних пристроях, включаючи обчислювальну та офісну техніку. Це явище неможливо повністю уникнути, оскільки воно зумовлене конструкційними та технологічними особливостями радіокомпонентів, що використовуються в електронних пристроях. Паразитне випромінювання, через нелінійність амплітудних характеристик, що завжди властива електронному обладнанню, модулюється обробленими інформаційними сигналами та випромінюється в ефір у вигляді модульованих коливань. Такі високочастотні коливання можуть проникати через ланцюги вторинного електроживлення в електромережу, а також поширюються як електромагнітні наводки на всі струмопровідні елементи в приміщенні, де розміщена електронна техніка. Хоча рівень цих паразитних коливань є незначним і, зазвичай, не перевищує рівень власних шумів техніки, достатньо навіть цього мінімального сигналу для його перехоплення за допомогою сучасних чутливих пристроїв. Для глобального збору інформації з розвідувальними цілями також використовуються супутники Землі та стаціонарні пункти розвідки.

Як наведено на рис. 5.12, інформацію в електронному та електромагнітному вигляді можна отримувати як з ліній зв’язку, так і з електронних пристроїв обробки даних.

Для перехоплення інформації з ефіру застосовуються панорамні радіоприймачі (для роботи на стаціонарних розвідувальних об'єктах) та компактні сканери (для мобільних розвідувальних точок). Ці пристрої мають широкий спектр функцій: вони здатні приймати сигнали з різними видами

модуляції, відстежувати частотний діапазон станцій, працювати під управлінням комп'ютера та виконувати інші задачі.

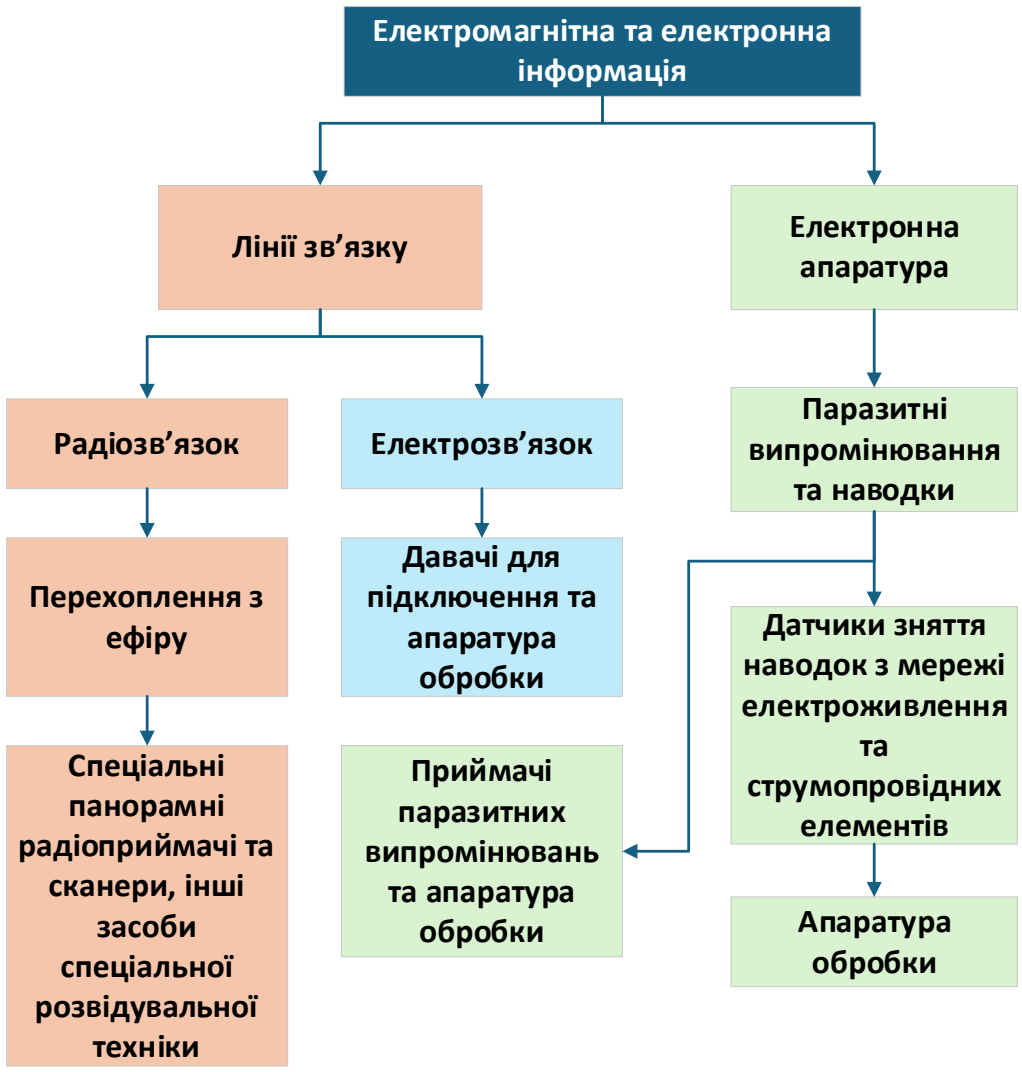


Рисунок 5.12 – Канали та засоби зняття електромагнітної та електронної інформації

Для зняття інформації з ліній зв'язку використовуються датчики з високим вхідним опором для підключення в паралель, а також індукційні датчики для безконтактного перехоплення сигналів. Виявити їх на лінії зв'язку без використання складних спеціалізованих пристроїв майже неможливо.

Інформація, що наводиться на струмопровідні конструкції приміщення, знімається за допомогою спеціальних приймачів наводки, які працюють за принципом частотно-селективного підсилювача з високим коефіцієнтом підсилення та широким динамічним діапазоном. Для покращення

співвідношення сигнал/завада при обробці отриманих даних використовуються пристрої спектральної обробки сигналів. Подібним чином також знімається інформація, що потрапляє в електромережу у вигляді модульованих сигналів паразитного випромінювання або наводок.

Письмова інформація може бути отримана в двох формах: оптичній та електронній. Шляхи отримання письмової інформації наведені на рис. 5.13.

Рисунок 5.13 – Шляхи отримання письмової інформації

Електронну інформацію можна отримати через зняття з ліній зв'язку (факсимільний зв'язок, електронна пошта) або перехоплення паразитних випромінювань та наводок (наприклад, сигнал з дисплея комп'ютера, який має високий рівень паразитного випромінювання). Також електронну письмову інформацію можна скопіювати з магнітних або оптичних носіїв, а також отримати через сканування паперових документів.

Оптичну інформацію можна отримати за допомогою прихованих телекамер, які можуть працювати як в інфрачервоному, так і у видимому

спектрі. Крім того, для збору оптичної інформації можуть використовуватися фотоапарати, ксерокопіювальні апарати або просто через крадіжку документів.

При розробці системи захисту інформації необхідно передбачити блокування технічних каналів витоку інформації. Найбільш вірогідними способами їх використання є зняття акустичної та електромагнітної інформації. Найчастіше для цього застосовуються механізми перетворення акустичних сигналів в електричні, а також паразитні випромінювання та наводки. Крім того, завжди існує ймовірність, що зловмисник використає ВЧ-нав'язування. Для блокування таких каналів витоку застосовуються активні методи протидії, зокрема активне створення завад у радіотехнічному та звуковому діапазонах частот. Водночас, необхідно забезпечити, щоб технічні засоби, які потребують захисту, могли виконувати свої основні функції без перешкод з боку систем захисту інформації.

Для цього в різних країнах на різних етапах розвитку методів та засобів технічного захисту інформації були розроблені спеціальні прилади, використання яких вимагало узгодження їх характеристик і можливостей для формування єдиного комплексу захисту інформації.

На сьогоднішній день вітчизняною компанією PIAC створено та атестовано комплекс засобів лінійного захисту інформації PIAC–ЛЗ, що відповідає технічним умовам ТУ У 31.6-33694400-002:2009, і призначений для захисту інформації від витоку через дротові провідні лінії електроживлення, системи пожежної та охоронної сигналізації, радіо- та телефонні мережі тощо.

До складу комплексу входить ряд пристроїв, зокрема:

- трансформатори різної потужності з екранованою обмоткою PIAC-4ТР;

- прилади захисту інформації в електромережі з придушенням небезпечних сигналів у частотному діапазоні від 20 кГц до 1 ГГц PIAC-4ЗМ/1 та PIAC-4ЗМ/2;

- генератор шумоподібного сигналу в мовленнєвому частотному діапазоні в режимі очікування виклику телефонного апарату в лініях аналогового телефонного зв'язку РІАС–4ША;

- фільтр загороджувальний високих частот РІАС-4 ФМ;

- прилад зашумлення телефонних кабелів захищених телефонних мереж РІАС–4ШЛ;

- прилад високочастотного шуму РІАС–1С, РІАС–1М, РІАС–2М для створення електромагнітних перешкод в ефірі в діапазоні частот від 180 Гц до 2 ГГц;

- генератор акустичного шуму РІАС–2ГС, РІАС–2ГМ для захисту об'єктів від витоку конфіденційної інформації акустичними та віброакустичними каналами шляхом генерації шумового сигналу в діапазоні частот від 180 Гц до 5.6 кГц;

- пристрій радіоелектронного захисту РІАС–РЗ/О для боротьби з безпілотними літальними апаратами.

Усі пристрої, що входять до складу комплексу, побудовані на єдиній елементній базі та за однаковим принципом роботи. Більшість із них оснащена вбудованими пристроями автоматизованого контролю працездатності.

Захист каналів зв'язку посідає особливе місце в загальній структурі комплексної системи захисту. Інформація повинна залишатися конфіденційною як у процесі її переміщення в межах внутрішньої мережі, так і під час передачі в інші інформаційні системи. Ніколи не можна виключити можливість витоку даних, що передаються дротовими каналами зв'язку. А перехоплення інформації, що передається лініями стільникового та радіорелейного зв'язку, є для технічно підготовленого зловмисника ще легшим завданням.

Криптографічні методи та засоби захисту інформації.

Криптографічними засобами захисту називаються спеціальні методи та засоби перетворення інформації, в яких маскується її зміст. Основними

видами криптографічного закриття є шифрування і кодування даних, що захищаються. При цьому шифрування є такий вид закриття, при якому самостійному перетворенню піддається кожен символ даних, що закриваються; при кодуванні дані, що захищаються, діляться на блоки, що мають смислове значення, і кожен такий блок замінюється цифровим, буквеним або комбінованим кодом.

Під криптологією (від грецького kruptos – таємне та logos повідомлення) розуміється наука про безпеку (секретність) зв'язку.

Повідомлення – вхідний текст, представлений у цифровому вигляді.

Криптограма – повідомлення зі спотвореним логічним змістом.

Шифрування даних – процес перетворення відкритих даних у зашифровані дані за допомогою шифру.

Шифр – безліч оборотних перетворень безлічі повідомлень у безліч можливих криптограм, за певними правилами із застосуванням ключів.

Ключ – конкретний секретний стан деякого параметра, що забезпечує вибір одного перетворення з сукупності можливих для використовуваного методу шифрування.

Для криптографічного закриття інформації в системах обробки даних найбільшого поширення набуло шифрування. Використовується кілька систем шифрування: заміна (підстановка), перестановка, гамування, аналітичне перетворення даних, що шифруються. Широке поширення набули комбіновані шифри, коли вихідний текст послідовно перетворюється з використанням двох чи навіть трьох різних шифрів.

Підсистема криптографічного захисту поєднує засоби криптографічного захисту інформації та призначена для забезпечення цілісності, конфіденційності, автентичності критичної інформації, а також забезпечення юридичної значущості електронних документів в інформаційній системі.

Функції підсистеми криптографічного захисту:

- забезпечення цілісності переданої по каналах зв’язку та інформації, що зберігається;

- захист повідомлень, що передаються каналами зв’язку;

- приховування змісту конфіденційних повідомлень, що передаються каналами зв’язку і зберігаються на носіях;

- забезпечення юридичної значущості електронних документів;

- забезпечення аутентифікації джерела даних.

Функції підсистеми криптографічного захисту спрямовані на ліквідацію найбільш поширених загроз повідомленням в автоматизованих системах:

1. Загрози, спрямовані на несанкціоноване ознайомлення з інформацією:

- несанкціоноване читання інформації;

- незаконне підключення до апаратури та ліній зв’язку;

- зняття інформації на шинах живлення;

- перехоплення електромагнітних імпульсів з ліній зв’язку.

2. Загрози, створені задля несанкціонованої модифікації (порушення цілісності) інформації:

- зміна службової або змістовної частини повідомлення;

- підміна повідомлення;

- вилучення (знищення) повідомлення.

3. Загрози, спрямовані на спотворення автентичності відправника повідомлення:

- незаконне присвоєння ідентифікаторів іншого користувача, формування та відправлення електронного документа від його імені, або твердження, що інформація отримана від якогось користувача, хоча вона сформована самим порушником;

- повторна передача документа, сформованого іншим користувачем;

- спотворення критичних з точки зору автентичності полів документа (дати формування, порядкового номера, адресних даних, ідентифікаторів відправника та одержувача тощо).

4. Загрози, пов’язані з невизнанням участі:

- відмова від факту формування електронного документа;

- відмова від факту отримання електронного документа або неправдиві відомості про час його отримання;

- ствердження, що одержувачу в певний момент була надіслана інформація, яка насправді не надсилалася (або надсилалася в інший час).

Підсистема зв’язку вважається найбільш уразливою підсистемою, тому слід приділити особливу увагу питанням її захисту.

Одна з компаній, яка спеціалізується на створенні телекомунікаційних мереж спеціального призначення, розробці та серійному виробництві засобів спеціального зв’язку та криптографічного захисту інформації є вітчизняна компанія Трител. Серед розробок цієї компанії в якості прикладу можна вказати комплексну систему захисту інформації ЛАВИНА-Е, до складу якої входять комплекс криптографічного захисту Лавина-Е (рис. 5.14), шифратор з інтегрованим модулем комутації Тритон-Е та шифратор з інтегрованим модулем перетворення мовленнєвої інформації Скат-Е.

Рисунок 5.14 – Комплекс криптографічного захисту Лавина-Е

До складу комплексу входять шифратор О371-Е(РЕ), пристрій генерації ключових даних О372-Е та централізована система керування (ЦСК). Шифратор О371-Е(РЕ) призначений для криптографічного захисту

трафіку IP-мереж високого рівня таємності. Використовується для захисту каналів дротового, супутникового, радіорелейного та стільникового (3G, 4G) зв'язку. Він виготовляється у варіантах для використання на стаціонарних (О371-Е) та рухомих (О371-РЕ) об'єктах. Пристрій генерації ключових даних О372-Е призначений для генерації, зберігання та розподілу ключових даних. Централізована система керування (ЦСК) призначена для віддаленого керування мережею шифрованого зв'язку.

На рис. 5.15 наведено шифратор з інтегрованим модулем комутації Тритон-Е.

Рисунок 5.15 – Шифратор з інтегрованим модулем комутації Тритон-Е

Шифратор з інтегрованим модулем комутації Тритон-Е, О271-Е(РЕ), призначений для криптографічного захисту трафіку IP-мереж високого рівня таємності. Вбудований керований чотири-портовий комутатор дозволяє підключати абонентське обладнання безпосередньо до шифратора. Використовується для захисту каналів дротового, супутникового, радіорелейного та стільникового (3G, 4G) зв'язку. Виробляється у варіантах для використання на стаціонарних (О271-Е) та рухомих (О271-РЕ) об'єктах.

На рис. 5.16 наведено шифратор з інтегрованим модулем перетворення мовленнєвої інформації Скат-Е.

Рисунок 5.16 – Шифратор з модулем перетворення мовленнєвої інформації Скат-Е

Шифратор з інтегрованим модулем перетворення мовленнєвої інформації Скат-Е забезпечує криптографічний захист мовленнєвої інформації та трафіку IP-мереж високого рівня таємності. Вбудований модуль перетворення мовленнєвої інформації дозволяє підключити телефонну трубку або гарнітуру безпосередньо до шифратора. Він забезпечує можливість роботи з обладнанням дротового, супутникового, радіорелейного, стільникового (3G, 4G) та КХ/УКХ зв’язку та призначений для використання на стаціонарних та рухомих об’єктах.

Схема застосування комплексу наведена на рис. 5.17.

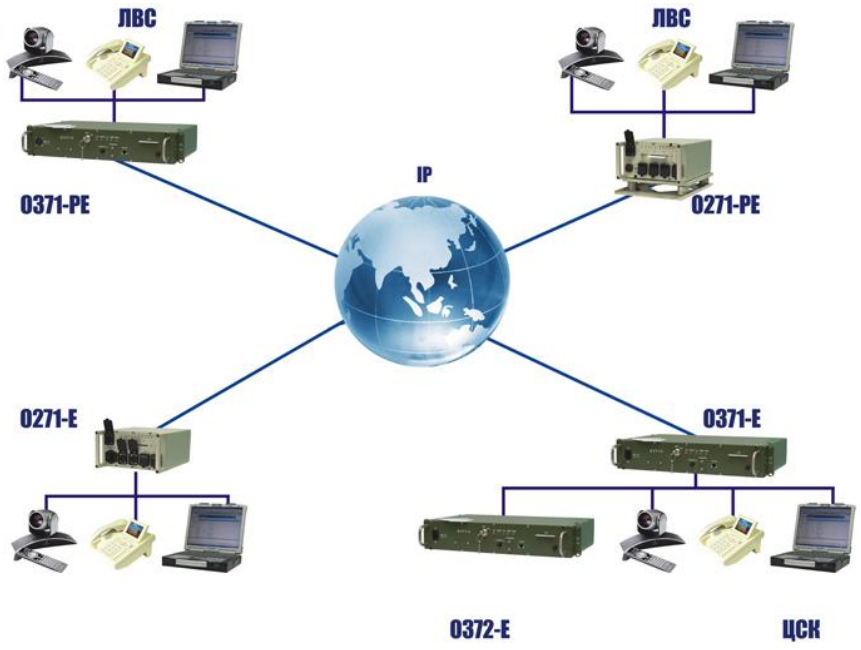


Рисунок 5.17 - Схема застосування комплексу ЛАВИНА-Е

5.3. Основні загальні положення технічного захисту інформації

Об’єктом технічного захисту є інформація, що становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження (далі – інформація з обмеженим доступом ІзОД).

Об’єкти захисту, а також мету й завдання технічного захисту інформації (ТЗІ) визначають особи, які володіють, користуються або розпоряджаються ІзОД відповідно до своїх прав і повноважень, наданих законодавством України, підзаконними актами та нормативними документами з ТЗІ. Носіями ІзОД можуть бути фізичні поля, сигнали, хімічні речовини, які утворюються під час інформаційної діяльності, виробництва та експлуатації різноманітної продукції. Середовищем поширення цих носіїв можуть бути лінії зв’язку, сигналізації, управлінські та енергетичні мережі, прикінцеве і проміжне обладнання, інженерні комунікації та споруди, відгороджувальні будівельні конструкції, а також світлопроникні елементи будівель і споруд, повітря, вода, ґрунт, рослинність та інші середовища.

Витік або порушення цілісності ІзОД, що включає їх спотворення, модифікацію, руйнування або знищення, може бути наслідком реалізації загроз безпеці інформації.

Концепція захисту інформації – офіційно прийнята система поглядів на проблему інформаційної безпеки і шляхи її вирішення з урахуванням розробки сучасних тенденцій. Вона є методологічною основою політики розробки практичних заходів її реалізації. Розробку концепції захисту проводять таким чином:

- визначення цільової установки захисту (які реальні цінності, виробничі процеси, програми, масиви даних необхідно захищати). Доцільно диференціювати за значимістю окремі об’єкти, які підлягають захисту;

- аналіз злочинних дій, які потенційно можуть бути здійснені стосовно об’єкта. Визначення ступеню реальної небезпеки найбільш поширених злочинів і аналіз ймовірних дій зловмисників;

- аналіз обставин (місцевих специфічних умов, виробничих процесів, раніше встановлених технічних засобів захисту). Формування переліку організаційних, технічних та інших заходів, які забезпечують максимальну безпеку при заданому залишковому ризику при мінімальних затратах на їх реалізацію.

Метою ТЗІ с запобігання витоку або порушенню цілісності ІзОД. Мста ТЗІ може бути досягнута побудовою системи захисту інформації, що є організованою сукупністю методів і засобів забезпечення ТЗІ. Технічний захист інформації здійснюється поетапно:

1 етап – визначення й аналіз загроз;

2 етап – розроблення системи захисту інформації;

3 етап – реалізація плану захисту інформації;

4 етап – контроль функціювання та керування системою захисту інформації.

Визначення й аналіз загроз. На першому етапі, відповідно до прийнятої концепції захисту інформації, необхідно провести аналіз об’єктів захисту, ситуаційного плану, умов функціонування підприємства, установи чи організації, оцінити ймовірність виникнення загроз та потенційну шкоду від їх реалізації, а також підготувати основні дані для створення окремої моделі загроз.

Джерелами загроз можуть бути діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних та фізичних осіб.

Загрози можуть бути реалізовані через:

- технічні канали, до яких відносяться канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

- канали спеціального впливу, при яких формуються поля і сигнали, спрямовані на руйнування системи захисту або порушення цілісності інформації;

- несанкціонований доступ, що здійснюється через підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, обхід засобів захисту для отримання доступу до інформації або нав'язування хибної інформації, а також застосування підкладних пристроїв, програм чи комп'ютерних вірусів.

Опис загроз та схем їх реалізації формують окрему модель загроз.

Розроблення системи захисту інформації. На другому етапі необхідно розробити план ТЗІ, який включатиме організаційні, первинні технічні та основні технічні заходи для захисту ІзОД, а також визначити зони безпеки інформації. Організаційні заходи мають регулювати порядок інформаційної діяльності з урахуванням норм і вимог ТЗІ на всіх етапах життєвого циклу об'єкта захисту. Первинні технічні заходи передбачають захист інформації шляхом блокування загроз без використання засобів ТЗІ, а основні технічні заходи – із застосуванням засобів технічного захисту інформації.

Для технічного захисту інформації потрібно використовувати методи приховування або методи технічної дезінформації. Заходи захисту повинні:

- відповідати наявним загрозам;

- бути розробленими з урахуванням можливих збитків від їх реалізації, вартості заходів та обмежень, які вони накладають;

- забезпечувати необхідну ефективність захисту інформації на визначеному рівні протягом часу, коли доступ до неї обмежений, або поки не буде здійснена загроза.

Рівень захисту інформації визначається за допомогою системи кількісних та якісних показників, що дозволяють вирішити завдання захисту інформації відповідно до норм і вимог ТЗІ. Мінімальний необхідний рівень захисту досягається шляхом обмеження доступу до інформації та

застосування фрагментарних заходів для протидії найбільш небезпечним загрозам. Підвищення рівня захисту можливе за допомогою розширення технічних заходів для протидії різноманітним загрозам.

Процедури розрахунку та інструментального визначення зон безпеки інформації, реалізації заходів ТЗІ, оцінки ефективності захисту та атестації технічних засобів для забезпечення інформаційної діяльності, а також робочих місць (приміщень) регулюються відповідними нормативними документами.

Реалізація плану захисту інформації. На третьому етапі необхідно реалізувати організаційні, первинні технічні та основні технічні заходи захисту ІзОД, впровадити необхідні засоби безпеки інформації, провести атестацію технічних засобів для забезпечення інформаційної діяльності, а також перевірити відповідність робочих місць (приміщень) вимогам безпеки інформації.

Технічний захист інформації забезпечується шляхом застосування захищених програм та технічних засобів для інформаційної діяльності, а також програмних і технічних засобів захисту інформації та засобів контролю, які мають сертифікат відповідності вимогам нормативних документів системи УкрСЕПРО або дозвіл на їх використання від органу, уповноваженого Кабінетом Міністрів України. Також використовуються спеціальні інженерно-технічні споруди, засоби і системи (засоби забезпечення ТЗІ).

Засоби ТЗІ можуть працювати як автономно, так і в складі технічних засобів забезпечення інформаційної діяльності, будучи самостійними пристроями або вбудованими в інші пристрої.

Склад засобів забезпечення ТЗІ, їх постачальники, а також послуги з їх установки, монтажу, налаштування і обслуговування визначаються особами, які володіють, користуються та розпоряджаються ІзОД самостійно або за рекомендаціями фахівців з ТЗІ відповідно до нормативних документів.

Надання послуг з ТЗІ, атестацію та сервісне обслуговування засобів забезпечення ТЗІ можуть здійснювати юридичні та фізичні особи, що мають ліцензію на проведення цих робіт, видану органом, уповноваженим Кабінетом Міністрів України.

Контроль функціювання та керування системою захисту інформації. На четвертому етапі необхідно провести аналіз функціонування системи захисту інформації, перевірити виконання заходів ТЗІ, оцінити ефективність захисту та підготувати основні дані для управління системою захисту інформації.

Управління системою захисту інформації полягає в адаптації заходів ТЗІ до актуальних завдань захисту інформації.

У разі зміни умов чи виявлення нових загроз, заходи ТЗІ повинні бути реалізовані в найкоротші терміни.

Якщо виникає необхідність підвищення рівня захисту інформації, слід виконати роботи, передбачені етапами 1, 2 та 3 для побудови системи захисту інформації.

Порядок проведення перевірок і контролю ефективності захисту інформації визначається нормативними документами з ТЗІ.

Нормативні документи з ТЗІ.

Нормативні документи розробляються в процесі виконання робіт зі стандартизації та нормування в галузі ТЗІ. Вони повинні забезпечувати:

- здійснення єдиної технічної політики;

- створення та розвиток єдиної термінологічної системи;

- функціонування багаторівневих систем захисту інформації на основі узгоджених положень, правил, методик, вимог і норм;

- діяльність систем сертифікації, ліцензування та атестації відповідно до вимог безпеки інформації;

- розвиток сфери послуг у галузі ТЗІ;

- встановлення порядку розроблення, виробництва та експлуатації засобів забезпечення ТЗІ;

- організацію проєктування будівельних робіт у частині забезпечення ТЗІ;

- підготовку та перепідготовку кадрів у системі ТЗІ.

Нормативні документи з ТЗІ поділяються на:

- нормативні документи зі стандартизації в галузі ТЗІ;

- державні стандарти та нормативні документи, прирівняні до них;

- нормативні акти міжвідомчого значення, які реєструються в Міністерстві юстиції України;

- нормативні документи міжвідомчого значення технічного характеру, що реєструються органом, уповноваженим Кабінетом Міністрів України;

- нормативні документи відомчого значення органів державної влади та органів місцевого самоврядування.

Коли відомі всі основні технічні канали витоку та класифікація способів зняття інформації, можна розглядати методи та засоби технічної протидії протиправним намаганням її отримання.

Серед основних загальних положень та визначень термінів захисту інформації особливе значення займає об’єкт захисту.

Слід зауважити, що об’єкт захисту може бути розміщений усередині іншого об’єкта, який не є об’єктом захисту інформації. Наприклад, спеціально виділені приміщення з обмеженим доступом, що знаходяться в будівлі з більш відкритим доступом, і призначені для роботи з конкретними видами інформації.

Основні технічні засоби – це пристрої, що використовуються для обробки, зберігання та передачі закритої інформації. Крім них, існують і допоміжні технічні засоби, які обробляють відкриту інформацію, але можуть створювати технічні канали для витоку закритої інформації. Тому, плануючи захист інформації на об’єкті, перш за все необхідно визначити, які види інформації потрібно захищати, а також, які приміщення або вся будівля підлягають захисту. Важливо також знати рівень секретності захищеної інформації та можливі загрози від потенційного зловмисника. Загроза для

інформації – це виток, можливість блокування або порушення цілісності інформації, яка може здійснюватися під час використання технічних засобів, недосконалих з точки зору захисту інформації, або інші канали витоку інформації.

Знаючі всі ці складові, можна розробляти систему захисту інформації на об’єкті. При цьому, слід пам’ятати, що для кожного виду інформації та кожного виду загроз існують цілком конкретні засоби захисту та способи їх застосування, отже треба користуватися тими системами та засобами захисту, що найбільш повно відповідають потенційним загрозам для кожного з видів інформації, яку слід захищати на конкретному об’єкті.

У випадку комплексного захисту необхідно розробляти підсистеми захисту для кожного окремого виду інформації, обов’язково пов’язавши їх у комплексну систему. При цьому, необхідно виявити всі потенційні канали витоку інформації та забезпечити їх блокування з рівнем технічного захисту, відповідним ступеню таємності інформації та рівню потенційних загроз.

Рівень технічного захисту інформації – це комплекс вимог, у тому числі нормативних, що визначаються умовами доступу до інформації та загрозами її безпеці.

У технічному захисті інформації зазвичай виділяють два основні методи: пасивний і активний.

Активний захист передбачає створення перешкод для зняття інформації шляхом випромінювання завад у канали витоку, рівень яких перевищує рівень небезпечних сигналів, що можуть бути отримані через ці канали. Крім того, до активного захисту належать методи, засновані на постійному моніторингу середовища поширення небезпечних сигналів з використанням спеціальних приладів і комплексів, які здатні виявляти спроби зняття інформації та активні заходи з нейтралізації засобів витоку.

Пасивний захист полягає в зниженні здатності технічних джерел витоку або середовища поширення небезпечних сигналів передавати

інформацію шляхом зміни їх властивостей, наприклад, екрануванням електромагнітного випромінювання.

У технічному захисті інформації застосовуються обидва методи. Водночас варто зазначити, що пасивні методи не використовують фізичних процесів, які можуть бути шкідливими для здоров'я людей або заважати їхній повсякденній діяльності. Однак, у багатьох випадках необхідне використання активних методів захисту, які в поєднанні з пасивними забезпечують потрібний рівень технічного захисту інформації.

Відповідно до ДСТУ 3396.2-97 (Захист інформації. Технічний захист інформації. Терміни та визначення) «Технічний захист інформації (ТЗІ) – діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (чи) витоку інформації технічними каналами». Тобто захист інформації необхідно здійснювати по кожному технічному каналу. Залежно від способу циркуляції інформації технічний захист інформації умовно можна розділити на два напрямки:

- технічний захист мовленнєвої інформації (мається на увазі інформація, яка циркулює у вигляді акустичних хвиль);
- технічний захист електронної інформації (інформація, яка циркулює у вигляді електричних сигналів та електромагнітних хвиль).

5.4. Методи пошуку радіозакладних пристроїв

Радіозакладні пристрої — це пристрої, які використовують радіоефір для передачі перехопленої інформації до засобів технічного захисту. Передача здійснюється шляхом перетворення (модуляції) перехоплених сигналів на електромагнітні хвилі, що розповсюджуються в ефірі.

Для виявлення радіозакладок, що випромінюють сигнали в ефір, необхідно визначити їх робочий діапазон, вид модуляції та методи захисту сигналу. Пошук закладних пристроїв ускладнюється завдяки використанню складних методів модуляції та шифрування (скремблювання, рандомізація, шифрування тощо), які постійно змінюються і вдосконалюються.

Методи пошуку радіозакладних пристроїв можна поділити на два основних підвиди, які доповнюють один одного:

- постійний радіомоніторинг ефіру:

- метод періодичних оглядів.

Постійний радіомоніторинг ефіру – найбільш ефективний метод. Він полягає в постійній перевірці радіовипромінювань для виявлення нових частот, що з'являються в спектрі, шляхом порівняння з попередніми даними. При появі в контрольованій області нових частотних складових проводиться пошук передавача за допомогою спеціальних приладів та методів пошуку, які становлять сутність другого підвиду.

Метод періодичних оглядів – застосовується на об'єктах, де немає можливості для постійного моніторингу. Цей метод може використовуватися автономно, без постійного контролю спектра.

Цю роботу повинні виконувати кваліфіковані фахівці, які добре володіють методиками радіотехнічних вимірювань та виявлення радіозакладок.

Основним приладом для радіомоніторингу є скануючий приймач (сканер), наприклад, моделі AR-2700, AR-3000A, AR-8000, AR-8200 (виробництво компанії AOR, Японія), або відповідні за характеристиками приймачі серії «Тантал» (виробництво компанії «Anna Design»). Найбільш удосконаленими серед них є сканери AR-8200 і AR-8600.

Ці приймачі мають вихід для підключення до персонального комп'ютера (який є другим елементом системи), де спеціальна програма (третій елемент системи) використовується для керування режимами роботи сканера. Сканер може налаштовуватись на задану частоту з визначеним кроком дискретизації.

Крім того, він може працювати з сигналами, які мають різний вид модуляції та в різній смузі частот прослуховування (широкій та вузькій), має зменшувач шуму, індикацію режиму. Взагалі, сканер може працювати

автономно від ПЕОМ, що і використовується при пошуку радіозакладок. Більш досконала апаратура використовується в професійній радіорозвідці.

Програма моніторингу побудована таким чином, що запам’ятовує спектр просканованої ділянки ефіру та використовує його як еталон при порівнянні з наступними вимірюваннями. Результати пошуку виводяться на монітор. У випадку виявлення нових частотних складових у контрольованій зоні ПЕОМ видає сигнал тривоги. Система може працювати і в автоматичному режимі.

Станом на сьогодні багатьма фірмами розроблено декілька таких програм. Принцип їх побудови однаковий, хоча вони мають відмінності в ціні і точності роботи.

Серед сучасних вітчизняних автоматизованих комплексів виявлення електромагнітних випромінювань слід відзначити комплекси «АКОР» (рис. 5.18) та PIAC-РДм «DigiScan EX».

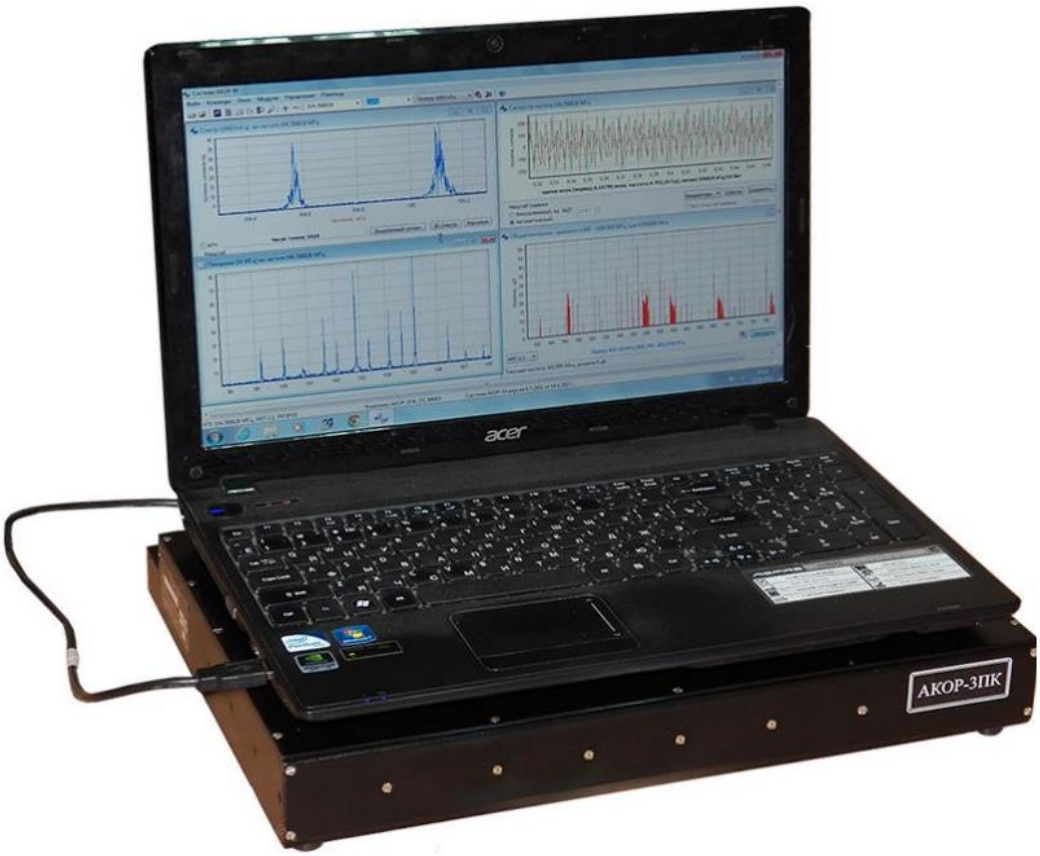


Рисунок 5.18 – Апаратно-програмний комплекс «АКОР»

Особливість цих комплексів полягає в тому, що вони: по-перше, здатні виявляти наявність радіозакладних пристроїв з шумоподібною та випадковою несівною частотою та по-друге, локалізувати місце знаходження радіозакладок.

Для цього в комплекси введено ряд додаткових пристроїв та програм.

Крім того, такі комплекси використовуються для перевірки відповідності рівня захисту об’єкту технічним вимогам та надійності блокування каналів витоку акустичної інформації. Ці комплекси розроблені в Україні та пройшли відповідну атестацію. Вони є офіційними приладами захисту інформації в нашій країні.

В якості прикладу також можна навести програмне забезпечення (з контролером) «DigiScan EX NEW Professional» (наведено на рис. 5.19), яке слід відмітити серед багатьох програм, розроблених для автоматичного сканування ефіру.

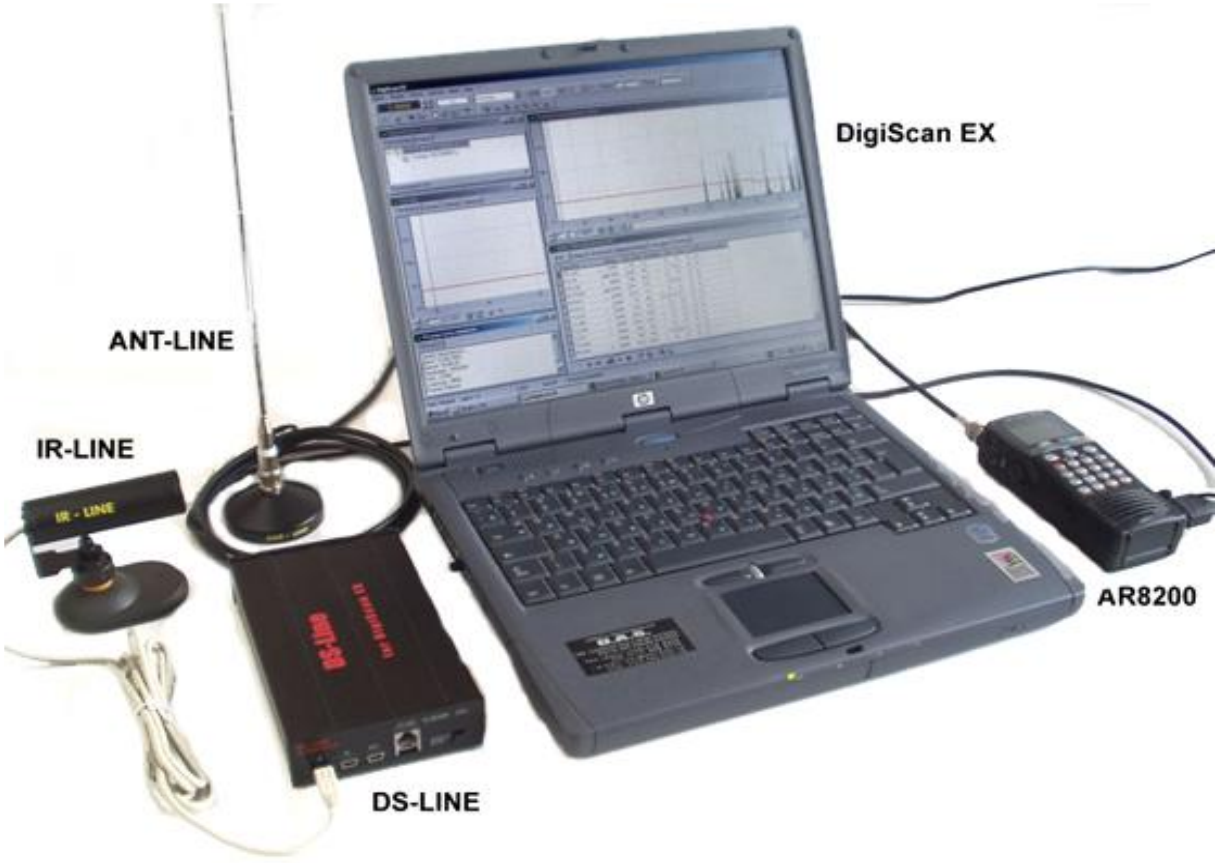


Рисунок 5.19 – Пошуковий комплекс на базі DigiScan EX

Це програмне забезпечення містить широкий набір алгоритмів пошуку та обробки сигналів та під час пошуку проводиться загальне і уточнююче сканування, що забезпечує точне вимірювання центральної частоти сигналу.

До комплекту постачання може входити: конвертор DS-LINE для перевірки телефонних ліній, комунікацій та мережі 220 В, зонд IR-LINE для перевірки ІЧ-діапазону, який підключається до DS-LINE, зовнішня широкосмугова антена ANT-LINE яка дозволяє уникнути перешкод від найближчого комп'ютера, та можливість підключення скануючих приймачів серій AR3000A, AR5000, IC-PCR1000, AR8600, IC-R8500. При використанні конвертору наднизьких частот DS-LINE програма може виявляти підслуховувальні пристрої, що використовують кабельні комунікації для передавання звукової інформації з приміщення в діапазоні частот від 5 кГц до 2 МГц (мережа 220 В, телефонні кабелі, дроти сигналізації).

Робота комплексу з цією програмою побудована за принципом порівняння параметрів акустичних сигналів та працює таким чином:

1. На першому етапі вимірюється та запам'ятовується спектр радіосигналів по всьому діапазону роботи сканера. Одночасно встановлюється вид модуляції для кожного сигналу, випромінювання якого зафіксовано.

2. На другому етапі на кожній з виявлених частот комплекс випромінює в повітря декілька складних акустичних сигналів, які сприймаються ним через ланцюг зворотного зв'язку, а саме – через радіоканал (приймач сканеру) на тій частоті, що перевіряється. Якщо в приміщенні є радіозакладка, то параметри сигналу, який продетектовано з ефіру, співпадатимуть з параметрами сигналу, що випромінювався в повітря приміщення. Для забезпечення однозначності сигналів, що сприймаються радіозакладкою, до сигналу, що випромінюється комплексом, додається акустичний сигнал з приміщення (шум, розмови тощо) через другий ланцюг зворотного зв'язку (мікрофон, підсилювач та змішувач сигналів).

Канали витоку інформації, що використовують закладні пристрої, є штучними технічними каналами, призначеними для несанкціонованого перехоплення даних. Для маскування таких пристроїв при їх установці застосовуються різні методи, що ускладнюють їх виявлення та захист від витоку інформації. Для захисту інформації від витоку через ці канали вживаються такі заходи:

- запобігання установці закладних пристроїв;

- виявлення та протидія роботі закладних пристроїв.

Ці заходи поділяються на організаційні та технічні.

Організаційні (глобальні) заходи включають:

- організація режиму роботи спеціально виділених приміщень;

- контроль за доступом відвідувачів та співробітників із обмеженим доступом;

- моніторинг роботи співробітників;

- перевірка приміщень та техніки, що знаходиться на об’єкті, на наявність закладних пристроїв, включаючи нову техніку, що надходить;

- аналіз методів установки закладних пристроїв, їх маскування, конструкцій та технологій.

Технічні (глобальні) заходи включають:

- створення системи технічних засобів охорони;

- впровадження системи охоронної сигналізації;

- організація телевізійного спостереження;

- впровадження системи контролю доступу;

- використання технічних засобів для виявлення підключення закладних пристроїв до ліній зв’язку, мереж живлення тощо;

- застосування технічних засобів для виявлення закладних пристроїв у техніці, що надходить, і в приміщеннях;

- використання технічних засобів для контролю радіовипромінювань та випромінювань у лініях зв’язку, живлення та управління;

- застосування технічних засобів для контролю інфрачервоних випромінювань;

- використання технічних засобів нелінійної радіолокації та підповерхневої локації;

- використання рентгенівських установок, тепловізорів, металодетекторів тощо.

Окрім глобальних організаційних заходів, які здебільшого є нормативами для діяльності підприємства чи організації, також розглядаються локальні організаційні заходи. Вони включають:

- аналітичну роботу з виявлення можливих місць для встановлення закладних пристроїв, з урахуванням особливостей їх функціонування;

- організацію роботи служби безпеки для контролю випромінювань в ефірі, мережах зв’язку та управління;

- аналіз частотних діапазонів та методів роботи закладних пристроїв.

Локальні технічні заходи включають різноманітні дії, спрямовані на виявлення закладних пристроїв та безпосередній захист:

- контроль сигналів у лініях зв’язку, керування, живлення та охоронних системах;

- моніторинг радіовипромінювань;

- контроль інфрачервоних випромінювань у зоні розташування об’єкта інформаційної діяльності;

- використання апаратури нелінійної радіолокації та підповерхневої локації;

- застосування рентгенівських установок, тепловізорів, металодетекторів;

- використання технічних засобів для сигналізації про підключення закладних пристроїв;

- застосування засобів візуального контролю;

- заходи для протидії роботі закладних пристроїв (використання електромагнітних засобів зашумлення, акусто-вібраційного зашумлення, демонтаж, руйнування та відключення закладних пристроїв).

Виявлення закладних пристроїв здійснюється через спеціалізовані обстеження та перевірки об'єктів ТЗПІ та виділених приміщень. Методи виявлення можна поділити на:

1. Пасивні методи:

- встановлення систем виявлення лазерного випромінювання (підсвітка скла на вікнах);

- встановлення стаціонарних детекторів диктофонів;

- пошук закладних пристроїв за допомогою індикаторів поля, інтерсепторів, частотомірів, скануючих приймачів та комплексів контролю;

- організація радіоконтролю побічних електромагнітних випромінювань ТЗПІ.

2. Активні методи:

- спеціальні перевірки виділених приміщень із використанням нелінійних локаторів;

- перевірка виділених приміщень, ТЗПІ та ДТЗІ з використанням рентгенівських комплексів.

Засоби радіоуправління приміщення використовуються для виявлення закладних пристроїв, які випромінюють радіохвилі під час пошуку. Для виявлення закладок, що не випромінюють сигналів, таких як дистанційно керовані пристрої або ті, що передають сигнали по дротах, застосовуються методи, які реагують не тільки на радіовипромінювання, а й на інші ознаки, що можуть вказувати на наявність закладок.

Методи та засоби виявлення не випромінюючих закладних пристроїв можна поділити на дві основні групи.

Перша група – методи, що базуються на пошуку закладних пристроїв як фізичних об’єктів з чіткими властивостями та компактними характеристиками. До неї належать:

- візуальний огляд потенційних місць розташування закладок, зокрема з використанням збільшувального скла, дзеркал та спеціального підсвічування;

- перевірка важкодоступних місць за допомогою відеоспостереження;

- використання металодетекторів.

Друга група – методи, що враховують електронні властивості закладних пристроїв. До цієї групи належать:

- застосування індикаторів поля, що реагують на випромінювання радіозакладок та дозволяють визначити їх місцезнаходження;

- використання спеціальних радіоприймальних пристроїв для пошуку сигналів за заданими параметрами та аналізу електромагнітного середовища;

- застосування комплексів радіоконтролю та виявлення закладних пристроїв;

- обстеження приміщень за допомогою нелінійних радіолокаторів, що здатні виявляти всі типи закладок.

Виявлення закладних пристроїв як фізичних об’єктів є найбільш загальним методом, що включає огляд приміщення або обстеження.

На основі вищевказаного розробляється методика та обираються засоби пошуку та знешкодження радіозакладних пристроїв.

У випадку наявності системи радіомоніторингу необхідно провести моніторинг ефіру. Якщо ж такого комплексу немає, можна здійснити контроль за допомогою сканера. Ці роботи зазвичай виконуються двома-трьома фахівцями і завжди починаються з опитування осіб, які використовують приміщення: чи отримували вони сувеніри, коли це сталося, і чи є вони в приміщенні на момент перевірки.

Наступним етапом є візуальний огляд приміщення, з особливою увагою до можливих місць для розміщення закладок. Для цього використовують ліхтарик. Крім меблів, перевіряють електричні та телефонні розетки, вентиляційні отвори, ніші для батарей опалення тощо. Особливу увагу приділяють рамкам картин, фотографій, портретів, естампів. При огляді таких предметів необхідно ретельно перевірити їх конструкцію, щоб

з’ясувати, чи не можуть вони створювати резонансний контур для високочастотного випромінювання.

Далі проводиться перевірка ефіру за допомогою сканера. Для активації закладок, які реагують на акустичні сигнали, використовуються спеціальні записи на магнітофоні, що містять мову та синусоїдальні сигнали з частотою 400 Гц та 1 кГц.

Одночасно можна почати перевірку в близькому полі, використовуючи індикатори або детектори поля. Ці пристрої виявляють джерела випромінювання на відстані до 25 см від антени, фіксуючи наявність електромагнітного поля. Зазвичай такі прилади оснащені світловими та звуковими сигналами, що попереджають про наближення до джерела випромінювання, а також мають вбудований частотомір для індикації частоти випромінювання. Ці прилади особливо корисні там, де візуальний огляд є складним або неможливим.

До таких приладів можна віднести детектор «D-006» виробництва компанії «СмерШ Техникс» та пошуковий пристрій «РТ-2» компанії «НОВО», який об’єднує функції детектора поля та частотоміра. Найбільш удосконаленими є прилади від компанії «Optoelectronics», зокрема модель «РТ-/025». Крім того, важливо провести комплексну перевірку електричних та телефонних мереж на наявність закладних пристроїв, які можуть живитися від цих мереж, а також перевірити наявність інфрачервоних джерел випромінювання, таких як телевізійні камери. Таку перевірку можна здійснити за допомогою приладу комплексного контролю «Акула» (модель СРМ – 700, виробництва США), наведеного на рис. 5.20.

Рисунок 5.20 – СРМ-700, «Акула»

Окрім виявлення радіозакладних пристроїв, їх можна також нейтралізувати шляхом установки активної радіотехнічної завади, яка може бути широкосмуговою або вузькосмуговою. Вузькосмугова завада застосовується у випадку, якщо точно відома частота, на якій працює радіозакладка. Однак цей метод використовується не часто і тільки коли передавач закладки має велику потужність.

Серед таких приладів варто виділити сучасні вітчизняні генератори завади, що працюють на основі випромінювання шумових електромагнітних коливань. Одним з найсучасніших таких пристроїв є прилад «Завада» (м. Київ), а також кілька моделей від компанії РІАС. Ці прилади оснащені генераторами випадкових сигналів, потужними підсилювачами та випромінювачами. Однак прилад «Завада» має кілька переваг перед зарубіжними аналогами. По-перше, він має високу потужність, що дозволяє ефективно захищати велику площу. По-друге, його генератор створює «білий» шум у широкому частотному діапазоні, значно ширшому, ніж у більшості інших приладів такого типу.

Крім того, прилади для постановки радіотехнічної завади виконують ще одну важливу функцію – блокування радіовибухових пристроїв під час розмінування. І в цьому випадку «Завада» має незаперечну перевагу,

оскільки його генератор працює на принципі шумової генерації, на відміну від псевдовипадкових послідовностей, що використовуються в багатьох інших подібних пристроях. Це виключає можливість випадкового збігу сигналу завади з кодом підриву вибухового пристрою.

Контрольні питання

1. Які існують способи несанкціонованого доступу до інформації?
2. Дайте короткий опис (не більше двох речень) кожного способу несанкціонованого доступу до інформації.
3. Як можна класифікувати пристрої для несанкціонованого добування інформації?
4. Як можна класифікувати програмні засоби для несанкціонованого добування інформації?
5. Наведіть головні ознаки основних програмних засобів добування інформації.
6. Що таке технічний канал витоку інформації?
7. Які існують технічні канали витоку інформації?
8. Як класифікуються види інформації?
9. Дайте характеристику акустичній інформації.
10. Які існують канали витоку інформації?
11. Назвіть комбіновані методи та засоби зняття акустичної інформації.
12. Назвіть методи та засоби зняття акустичної інформації з будівельних конструкцій.
13. Назвіть методи та засоби зняття акустичної інформації з засобів та ліній зв’язку.
14. Які використовуються радіомікрофони для зняття акустичної інформації?
15. Які існують канали та засоби зняття електромагнітної та електронної інформації?
16. Які існують шляхи отримання письмової інформації?

17. Опишіть призначення та основні можливості комплексу засобів лінійного захисту інформації РІАС–ЛЗ.

18. Назвіть функції підсистеми криптографічного захисту.

19. Які загрози повідомленням в автоматизованих системах попереджаються підсистемами криптографічного захисту?

20. Опишіть призначення та основні можливості комплексної системи захисту інформації ЛАВИНА-Е.

21. Які існують етапи технічного захисту інформації?

22. Якими нормативними документами регулюється технічний захист інформації?

23. Як можна виявити наявність радіозакладних пристроїв?

24. Яке обладнання використовується для виявлення радіозакладних пристроїв?

25. Які існують методи та засоби виявлення не випромінюючих закладних пристроїв?

26. Яке обладнання використовується для генерування завад?

6. МЕРЕЖЕВІ ПРИСТРОЇ ЗВ'ЯЗКУ

6.1. Інфраструктура забезпечення мережевої безпеки

У сучасному світі більшість людей щоденно використовує персональні стаціонарні комп'ютери, ноутбуки та інші цифрові пристрої для роботи або розваг, а також системи відеоспостереження для створення безпечної системи захисту оселі. Крім цього, комп'ютерна та цифрова техніка також застосовується для збереження та передачі великих обсягів даних працівниками різноманітних промислових, енергетичних, адміністративних, комерційних компаній та в багатьох інших сферах діяльності. Для того, щоб об'єднати декілька комп'ютерів в одну мережу, підвищити якість, швидкість та продуктивність з'єднання, а також для забезпечення ефективної, стабільної роботи та безпечної передачі даних слід використовувати мережеві комутатори локальної мережі.

Комп'ютерна мережа – найпоширеніший на сьогодні спосіб спілкування та обміну інформацією. «Всесвітня павутина» зберігає гігабайти персональної інформації про своїх користувачів. А персональні комп'ютери та сервери в локальній мережі – внутрішню інформацію компанії. Ці дані потребують захисту від стороннього втручання [23].

Мережева інфраструктура – це сукупність обладнання та програмного забезпечення, що формує середовище процесу передачі даних та забезпечує функціонування усіх необхідних бізнес-застосунків і сервісів. Вона повинна забезпечувати передачу будь-якого виду трафіку – дані, голос, відео, але з різними пріоритетами та якістю.

Основні принципи безпеки корпоративної мережі повинні забезпечувати:

1. Захист пристроїв, підключених до мережі. Для ефективного захисту пристроїв, що підключені до мережі, слід використовувати передові технології. Наприклад, для захисту комп'ютерів від вірусних атак необхідно

встановлювати надійне антивірусне програмне забезпечення та налаштувати автоматичне оновлення баз сигнатур, щоб знизити ймовірність атаки.

2. Стійкість мережевих пристроїв до відмов та швидке відновлення. Важливо забезпечити надійність пристроїв, а також регулярно проводити моніторинг інфраструктури для того, щоб мати чітке уявлення про стан різних елементів мережі (пристроїв, застосунків, сервісів) та оперативно застосовувати засоби захисту в разі необхідності.

3. Безперервний контроль пропускної здатності мережі. Потрібно постійно моніторити пропускну здатність мережі, оскільки атаки можуть спричинити значні витрати на відновлення роботи систем. Тому необхідно впроваджувати засоби захисту від цільових атак та заходи для попередження несанкціонованого доступу до інфраструктури, що допоможе зменшити ризики від успішних атак і знизить витрати на відновлення.

4. Стійкість локальної мережі до відмов. Повний захист мережі неможливий за жодних умов, однак можна реалізувати механізми швидкого переключення з одного ресурсу на інший у разі відмови першого, що дозволить користувачам мережі не помітити збоїв.

5. Комплексні заходи для забезпечення мережевої безпеки. Атаки на мережеву інфраструктуру можуть бути активними або пасивними, залежно від типу шкідливого програмного забезпечення, яке використовують зловмисники. Для ефективного забезпечення безпеки мережі необхідно застосовувати різноманітні методи і інструменти, які взаємодіють для зниження потенційних загроз.

Основні методи і інструменти для забезпечення безпеки в мережі:

1. **Міжмережеві екрани**. Міжмережеві екрани служать бар’єром між внутрішньою, захищеною мережею та зовнішніми, менш надійними мережами, такими як Інтернет. Вони застосовують набір правил для контролю доступу і фільтрації трафіку. Міжмережевий екран може бути реалізований у вигляді апаратного, програмного або комбінованого рішення. Інші назви міжмережевих екранів – брандмауер (Brandmauer), фаєрвол

(Firewall), Сучасні пристрої для уніфікованого управління загрозами (UTM) та міжмережеві екрани нового покоління забезпечують високий рівень захисту і профілактику загроз. Приклад мережевих екранів Fortinet FortiGate або Palo Alto Networks наведено на рис. 6.1.

а) Fortinet FortiGate 40F

б) Palo Alto Networks Enterprise Firewall PA-220

Рисунок 6.1 - Міжмережеві екрани

2. **Захист електронної пошти**. Шлюзи електронної пошти є основною ціллю для кіберзлочинців, які намагаються проникнути в мережу, використовуючи методи соціальної інженерії або фішинг. Для протидії таким загрозам використовуються спеціалізовані програми, що блокують шкідливі повідомлення. Сучасні рішення для захисту пошти аналізують вхідні повідомлення та контролюють вихідні, щоб запобігти витоку конфіденційної

інформації. Приклади: програмні та апаратні засоби Proofpoint або програмні продукти від Mimecast, для захисту від спаму та фішингових атак.

3. **Антивіруси та програми для захисту від шкідливого ПЗ**. Термін «шкідливе ПЗ» охоплює різні типи програм, включаючи віруси, черв'яки, троянські коні, шпигунські програми тощо. Шкідливе ПЗ може приховано заражати систему, не проявляючи себе протягом певного часу. Найкращі антивірусні рішення не тільки сканують трафік, а й постійно моніторять файли, виявляючи аномалії, усуваючи загрози і мінімізуючи збитки.

4. **Сегментація мережі**. Сегментація мережі дозволяє класифікувати мережевий трафік і застосовувати політики безпеки, що спрощує контроль доступу. Ключовим є розподіл доступу залежно від ролей, місця розташування чи інших параметрів, що дозволяє знижувати ризики від несанкціонованого доступу. Наприклад, впровадження програмно визначеної сегментації мережі SDN (Software-Defined Networking) дозволяє автоматично класифікувати пристрої та користувачів для забезпечення більшої безпеки.

5. **Управління доступом**. Не всі користувачі повинні мати доступ до всіх ресурсів мережі. Для забезпечення безпеки необхідно чітко ідентифікувати кожного користувача та пристрій і застосовувати відповідні політики доступу. Процес контролю доступу до мережі NAC (Network Access Control) дозволяє обмежити доступ до мережі для невідомих або ненадійних пристроїв. Наприклад, такі рішення, як Cisco Identity Services Engine (ISE), можуть реалізувати політики доступу на основі пристроїв і користувачів.

6. **Безпека застосунків**. Будь-яке програмне забезпечення, яке використовується в організації, може містити вразливості, що можуть бути використані зловмисниками для проникнення в мережу. Система безпеки застосунків забезпечує усунення цих вразливостей через апаратні та програмні засоби. Наприклад, веб-застосунки можна захищати за допомогою таких рішень, як OWASP (Open Web Application Security Project) для виявлення вразливостей або використання WAF (Web Application Firewall) таких як Imperva.

7. **Поведінкова аналітика**. Поведінкова аналітика дозволяє виявляти аномалії в мережі, спостерігаючи за типовим поведінковим профілем користувачів і пристроїв. Цей метод допомагає швидко реагувати на потенційні загрози, запобігаючи компрометації. Наприклад, використання таких інструментів як Darktrace для виявлення та реагування на незвичні дії в мережі.

8 **Запобігання витоку даних**. Технології запобігання витоку даних DLP (Data Leak Prevention) допомагають контролювати передавання конфіденційної інформації через електронну пошту, веб або інші канали, щоб запобігти її витоку за межі організації. Наприклад, за допомогою використання рішень Symantec DLP для контролю і обмеження доступу до чутливих даних.

9. **Безпека мобільних пристроїв**. З розвитком мобільних технологій, мобільні пристрої стають однією з основних цілей для атак. Для забезпечення їх безпеки необхідно контролювати доступ до мережі та налаштовувати підключення для збереження конфіденційності даних. Приклад організації безпеки мобільних пристроїв – впровадження рішень для мобільної безпеки, від MobileIron або Microsoft Intune, для керування мобільними пристроями та застосунками.

10. **Мережа VPN**. Віртуальні приватні мережі VPN (Virtual Private Network) забезпечують шифрування даних при підключенні до корпоративної мережі через мережу Інтернет. Це дозволяє захистити віддалений доступ до мережі за допомогою таких протоколів, як IPsec або SSL. Наприклад, використання OpenVPN або Cisco AnyConnect для створення захищених з’єднань між користувачами та мережею.

11. **Безпека веб-трафіку**. Рішення для безпеки веб-трафіку контролюють використання мережі Інтернет, блокують шкідливі вебсайти і захищають від загроз, пов’язаних із веб-трафіком. Вони також можуть захищати корпоративні сайти від атак. Наприклад, використання веб-

фільтрів, таких як Websense або Zscaler, для запобігання доступу до шкідливих сайтів і захисту від атак.

Мережева інфраструктура організації забезпечує обмін даними та інтеграцію всіх IT-ресурсів. Вона може значно варіюватися за такими характеристиками:

- розмір покритої території,
- кількість підключених користувачів,
- кількість і види доступних послуг.

Основні складові мережевої інфраструктури включають:

- активне обладнання (комутатори, маршрутизатори тощо);
- пасивні пристрої (кабелі, кабельні канали, монтажні шафи, комутаційні панелі, інформаційні розетки);
- периферійне обладнання та комп'ютери (ксерокси, робочі станції, сервери, принтери, сканери);
- програмне забезпечення для управління та моніторингу мережі.

Ефективність моніторингу мережевої інфраструктури безпосередньо залежить від наявності в адміністратора спеціалізованих інструментів. У разі їх відсутності, моніторинг часто здійснюється методом «випадкових перевірок» або інцидентного реагування, тобто усунення несправностей лише після їх виникнення.

Для своєчасного виявлення та усунення проблем необхідно проводити регулярний контроль мережевої інфраструктури. Наприклад, якщо не стежити за процесом щоденного резервного копіювання, то при його збої компанія може не мати доступу до актуальних бекапів, що призведе до серйозних фінансових та організаційних втрат.

Адміністратор, який має необхідні інструменти, здатен:

- передбачити потенційні проблеми, наприклад, з перевантаженням серверів через недостатні ресурси;
- завчасно визначити заходи для запобігання збоям;
- оперативно реагувати на інциденти в будь-який час доби;

- провести детальне розслідування інциденту для виявлення його причин.

Для цього вендори пропонують організаціям спеціалізовані рішення, такі як Aruba AirWave (від HPE), Cisco Prime, системи з відкритим вихідним кодом, наприклад Zabbix, та інші. Ці системи виконують централізований моніторинг і забезпечують управління мережею в режимі реального часу. Якщо виникає збій або інша проблема в мережі, інструмент негайно повідомляє про це адміністратора. Такі продукти перевіряють:

- доступність вебсайтів компанії;
- роботу серверів на різних операційних системах;
- функціонування серверних застосунків і служб;
- стан мережевого обладнання (комутатори, маршрутизатори тощо).

Після проведених перевірок зібрані дані автоматично оформлюються в звіт і надсилаються на електронну пошту або через SMS.

IT-відділ повинен постійно контролювати конфігурацію та технічну підтримку мережевої інфраструктури. Оскільки з часом складність інфраструктури зростає, організація повинна адаптуватися до змін, щоб мати можливість швидко і ефективно вирішувати завдання. Масштабованість і гнучкість мережі безпосередньо впливають на ефективність роботи інфраструктурних сервісів і продуктів.

Для успішного розвитку бізнесу компаніям важливо правильно управляти своєю мережею, яка може включати значну кількість апаратного та програмного забезпечення. Якщо діяльність компанії не пов’язана з IT-сферою, керування інфраструктурою може стати складним завданням. У такому випадку доцільно використовувати аутсорсинг мережевої інфраструктури.

Аутсорсинг мережевої інфраструктури дозволяє:

- зосередитися на важливіших завданнях. Адміністратор може не витрачати час на постійний моніторинг інфраструктури і переключитися на пріоритетні бізнес-цілі;

- знизити витрати на придбання обладнання та програмного забезпечення. Постачальники аутсорсингових послуг мають партнерські угоди з провідними вендорами, що дозволяє їм надавати необхідне обладнання та ПЗ за вигіднішими цінами;

- підвищити рівень безпеки мережі. Аутсорсингові компанії забезпечують відповідність інфраструктури вимогам безпеки та функціональності, впроваджуючи спеціалізовані сервіси та застосунки. Це знижує ймовірність помилок і дозволяє швидко виправляти їх у разі виникнення;

- покращити функціональність інфраструктури. Аутсорсинг дає можливість автоматизувати рутинні завдання та інтегрувати складні бізнес-процеси. Використання послуг аутсорсингової компанії допоможе стандартизувати і спростити обслуговування мережі, що дозволить ефективніше управляти внутрішніми процесами організації.

6.2. Забезпечення обміну даними мережевими пристроями

Комп'ютерна мережа – сукупність пристроїв, з'єднаних каналами передавання даних, для спільного користування апаратними, програмними та інформаційними ресурсами під керуванням спеціального програмного забезпечення.

Мережі можна поділити на кабельні (дротові) та бездротові залежно від способу передавання даних.

Кабельною (дротовою) мережею називають мережу, в якій для передавання даних використовується кабель. У таких мережах дані передаються через електричні або оптичні сигнали.

Застосовуються такі типи кабелів:

- кручена пара – це кілька пар скручених мідних проводів, покритих кольоровою пластиковою ізоляцією. Зовні вони обгорнуті захисним обплетенням. Такий кабель використовують у телефонії та більшості мереж Ethernet (пакетна технологія передачі даних для комп'ютерних мереж). Існує

неізольований (UTP) і ізольований (STP) варіанти даного типу кабелю. В останньому випадку скручені пари проводів мають мідне обплетення, яке заземляється. Характеризується кручена пара так званою категорією, зокрема для мереж на базі технології Ethernet допускається використання кабелю категорії 3 і вище. З кабелем цього типу використовуються вилки та розетки стандарту 8P8C. Він використовується для побудови мережі топології «зірка». Залежно від типу кабелю максимальна відстань передачі даних без підсилення сигналу варіюється від 15 до 100 м, а швидкість передачі може досягати 100 Гбіт/с;

- коаксіальний кабель – це кабель, що складається з мідного проводу, який оточений металевою оболонкою-екраном. Він використовується для підключення комп'ютерів до мережі та передавання телевізійних сигналів. Максимальна відстань без підсилення сигналу становить 500 м, а максимальна швидкість передачі даних може досягати 10 Мбіт/с.

- оптоволоконний кабель – це кабель, що складається з скляного або пластикового волокна, яке використовує принцип повного внутрішнього відображення для перенесення світлових сигналів. Застосовується в основному для побудови магістралей, тобто створення каналів зв'язку між віддаленими частинами мережі, а також для підключення серверів. Існують два різновиди даного кабелю: багатомодовий (допускається передача декількох пучків світла «модів» по одному світловоду, при цьому забезпечується дальність зв'язку до 2 км) і одномодовий (внаслідок меншого діаметра світловода можлива передача лише одного пучка світла, забезпечується дальність зв'язку до 80 км). Такий кабель забезпечує найшвидшу передачу даних. Відстань без підсилення сигналу досягає 50 км, а швидкість передачі може коливатися від 10 Гбіт/с до 4-8 Тбіт/с.

Бездротовою мережею називають таку мережу, в якій дані передаються через радіосигнали. Стандарти бездротових мереж:

- Wi-Fi (Wireless Fidelity) – стандарт для обладнання бездротових мереж, який підтримує Wi-Fi Alliance, об’єднання великих виробників комп’ютерної техніки та мережевого обладнання;

- WiMAX, Mobile WiMAX, Mobile-Fi – технології, що розширюють можливості бездротових мереж, забезпечуючи покриття на більших територіях і покращений доступ до мережі Інтернет порівняно з Wi-Fi;

- LTE (Long-Term Evolution, або 4G LTE) – стандарт для високошвидкісної передачі даних через мобільні телефони та інші пристрої;

- Bluetooth – стандарт для бездротових персональних мереж, що дозволяє обмінюватися даними між різними пристроями, такими як мобільні телефони, ноутбуки, принтери, фотоапарати тощо.

За іншими ознаками класифікація мереж може бути виконана таким чином:

1. Сфера застосування:

- офісні, промислові, побутові мережі.

2. Комплекс архітектурних рішень:

- Ethernet, Token Ring, Arcnet.

3. Топологія мережі:

- шинна або «спільна шина» (Bus) – загальний кабель (шина або магістраль), до якого приєднані всі робочі станції. На кінцях кабелю знаходяться термінатори, для запобігання відбивання сигналу. Шинна топологія має низьку надійність, оскільки у випадку обриву кабелю порушується працездатність всієї мережі. З’єднання за цією топологією не вимагає використання комунікаційних пристроїв;

- кільцева або «кільце» (Ring) – кожен комп’ютер з’єднаний лініями зв’язку тільки з двома іншими: від одного він тільки одержує інформацію, а іншому тільки передає;

- «подвійне кільце» (Dual Ring) – топологія, побудована на двох кільцях. Перше кільце – основний шлях для передачі даних; друге –

резервний шлях, що дублює основний. Це забезпечує високу надійність, гнучкість в експлуатації і обслуговуванні;

- зіркоподібна або «зірка» (Star) – базова топологія комп'ютерної мережі, в якій всі комп'ютери мережі приєднані до центрального вузла, у ролі якого може бути концентратор або комутатор. Має високу надійність, оскільки при обриві мережевого кабелю від'єднаним від мережі буде лише один пристрій;

- розширена зірка (Extended Star) – утворюється при об'єднанні декількох сегментів мережі, кожен з яких організовано за топологією «зірка». Зв'язок між сегментами здійснюється з використанням концентраторів, мостів та комутаторів. Один з пристроїв є центральним;

- ієрархічна (Hierarchical) або «деревоподібна» (Tree) – побудова мережі за схемою двійкового дерева, де кожен вузол більш високого рівня пов'язаний з двома вузлами наступного по порядку більш низького рівня. Ця топологія об'єднує різні зіркоподібні топології в одній шині, тому її називають ще топологією зіркоподібної шини;

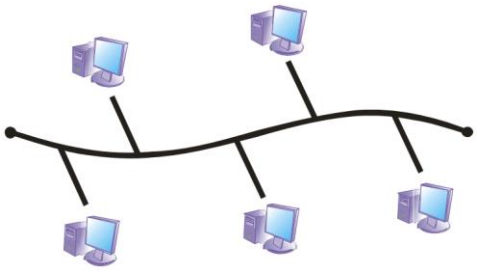
- повнозв'язна або «завершена» (Complete, Mesh) – базова повнозв'язна топологія комп'ютерної мережі, в якій кожна робоча станція мережі з'єднується з усіма іншими робочими станціями цієї ж мережі;

- нерегульована (Irregular) – не має чітко визначених правил, за якими з'єднуються мережеві пристрої;

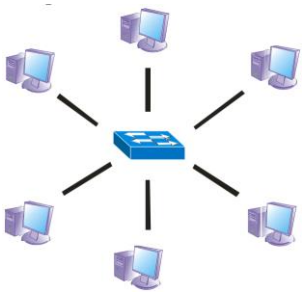
- комірчаста (Cells) – кожен комп'ютер з'єднано з іншим, переважно за допомогою радіомодемів, які входять у зону дії його зв'язку;

- гібридна (Hybrid) – поєднання простих топологій типу «зірка», «спільна шина», «кільце» між собою.

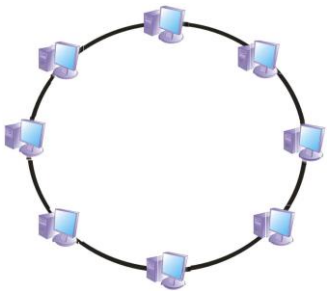
Графічне зображення варіантів побудови топології мереж наведено на рис. 6.2.



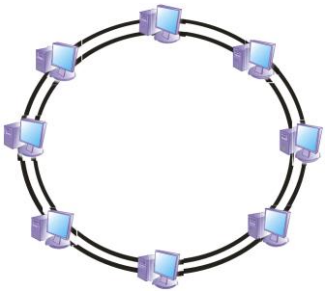
а) шинна



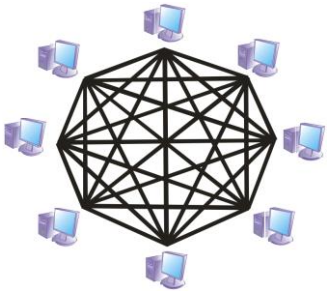
б) зіркоподібна



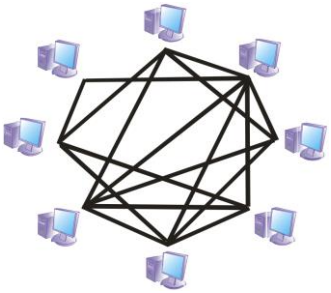
в) кільцева



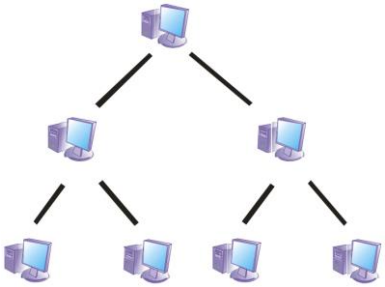
г) подвійне кільце



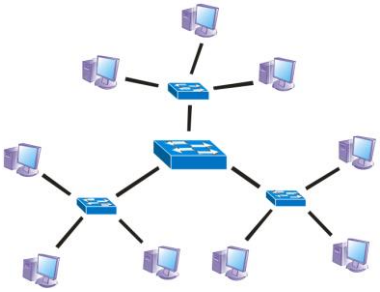
д) повнозв’язна



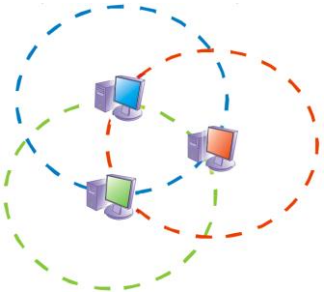
е) нерегульована



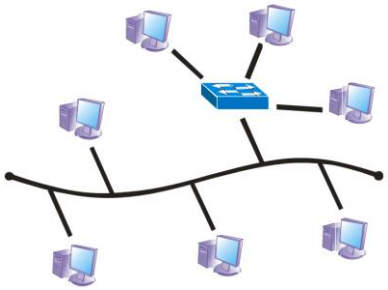
ж) ієрархічна



к) розширена зірка



л) комірчаста



м) гібридна

Рисунок 6.2 – Топологія мереж

4. Метод доступу до фізичного середовища:

- мережі з опитуванням, маркерним доступом, суперництвом, установленням регістра.

5. Набір протоколів (протокольний стек):

- мережі TCP/IP, SPX/IPX.

6. Ширина смуги каналу:

- вузькосмугові (Baseband) – передача одного повідомлення в будь-який момент часу без модуляції;

- широкосмугові (Broadband) – одночасна передача кількох повідомлень через частотно-розділені канали.

7. Розміри мережі (географічна площа):

- BAN (Body Area Network) – натільна комп'ютерна мережа пристроїв, які одягає користувач або мережа імплантованих пристроїв. Через шлюзи такі пристрої можуть з'єднуватись через мережу Інтернет (наприклад, для доступу медичними працівниками до даних про пацієнта онлайн, незалежно від місця розташування пацієнта);

- PAN (Personal Area Network) – комп'ютерна мережа, утворена навколо людини. Зазвичай складається з комп'ютера, мобільного телефону чи персонального цифрового помічника. PAN можна використовувати для встановлення зв'язку між цими персональними пристроями для підключення до цифрової мережі та мережі Інтернет. PAN дозволяє керувати з'єднанням IT-пристроїв в оточенні одного користувача. Техніка, яка використовується для PAN: бездротові миші, клавіатури та системи Bluetooth. Мережі PAN відносно безпечні;

- HAN (Home Area Network) – домашня мережа завжди будується за допомогою двох або більше взаємопов'язаних комп'ютерів, що утворюють локальну мережу (LAN) всередині будинку. Ця мережа дозволяє спільно використовувати файли, програми, принтери та інші периферійні пристрої;

- LAN (Local Area Network) – локальна мережа в межах одного офісу чи будівлі. Це група комп'ютерів та периферійних пристроїв,

підключених на обмеженій території з менш ніж 5000 взаємозалежних пристроїв у кількох будинках. Адміністратор локальної мережі може мати доступ до файлів особистих даних кожного користувача локальної мережі, тому це не забезпечує конфіденційність. Також неавторизовані користувачі можуть отримати доступ до критично важливих даних організації, якщо адміністратор локальної мережі не може захистити централізоване сховище даних;

- CAN (Campus Area Network) – мережа для об'єднання віддалених вузлів та локальних мереж без використання телефонних ліній. Наприклад, університетський кампус можна поєднати з різними будівлями кампусу, щоб об'єднати всі академічні факультети;

- MAN (Metropolitan Area Network) – територіальна мережа з радіусом десятки кілометрів, з високою швидкістю передачі даних. Мережа може охоплювати місто або невеликий регіон. Середовище, що використовується – оптичні волокна, кабелі;

- WAN (Wide Area Network) – мережа WAN може бути об'єднанням локальної мережі, яка з'єднується з іншими локальними мережами за допомогою телефонних ліній і радіохвиль. Найчастіше це обмежується підприємством чи організацією. Забезпечує нижчий рівень безпеки, ніж попередні типи комп'ютерних мереж;

- GAN (Global Area Network) – глобальна міжнародна мережа. Глобальні або всесвітні мережі GAN призначені для зв'язку абонентів, розташованих у різних географічних регіонах, і включають безліч мереж різної протяжності – материкові WAN, регіональні або міські MAN, і навіть локальні LAN та CAN;

- EWN (Enterprise Wide Network) – особливий вид мереж. Термін «корпоративна мережа» відбиває, з одного боку, величину мережі, оскільки корпорація – велике підприємство. З іншого боку, цей термін несе сенс об'єднання, тобто корпоративна мережа – мережа, отримана в результаті об'єднання кількох, зазвичай, різноманітних мереж. Ці мережі можуть

включати всі перелічені вище типи мереж, складно пов’язані і можуть покривати місто, регіон або навіть континент.

8. Співвідношення вузлів:

- одноранговi мережі (Peer-To-Peer) – мережі, де кожен вузол може бути як клієнтом, так і сервером;

- розподілені мережі (Distributed) – мережі без єдиного лідера, де сервери забезпечують сервіс, але не керують мережею;

- мережі з централізованим управлінням (Server-Based) – мережі, де сервери надають іншим вузлам доступ до спільних ресурсів.

9. Метод доступу:

- мережі з розподіленим середовищем передачі (Shared-Media Networks) – в яких на певний момент часу можуть взаємодіяти тільки два вузли;

- мережі з комутацією (Switching Networks) – де декілька пар вузлів можуть взаємодіяти одночасно через мультиплексування.

10. Спільність операційних систем:

- гомогенні мережі – всі вузли використовують однакові або схожі операційні системи;

- гетерогенні мережі – вузли використовують різні операційні системи.

Але будь-яка класифікація мереж є умовною, оскільки реальні мережеві конфігурації часто поєднують елементи кількох класифікацій одночасно.

Канало- та мережеутворювальне обладнання (або просто «мережеве обладнання») – це обладнання для сполучення кабельної системи інформаційної системи з обчислювальним пристроями, а також різних частин кабельної системи. Каналоутворювальне обладнання забезпечує функції канального рівня моделі OSI для організації мережі, а мережеутворювальне – функції канального та мережевого рівня моделі OSI.

Мережеве обладнання можна розділити на дві групи:

- кінцеве обладнання – мережні плати та модеми, які встановлюються в обчислювальні пристрої та забезпечують їх підключення до мережі;

- комутаційне обладнання – концентратори, мости, комутатори, маршрутизатори, які служать для об'єднання частин кабельної системи в єдину мережну інфраструктуру.

Лінія зв'язку – це обладнання, за допомогою якого здійснюється об'єднання комп'ютерів у мережу. Лінії зв'язку залежно від середовища передачі даних поділяються на:

- повітряні – традиційно по таких проводах передають телефонні або телеграфні сигнали, але за відсутності інших можливостей ці лінії використовуються також і для передачі комп'ютерних даних;

- кабельні – представляють складну конструкцію, яка складається із провідників; використовуються такі типи: кручена пара, коаксіальний кабель, волоконно-оптичний кабель;

- радіоканали наземного та супутникового зв'язку – створюються за допомогою передавача і приймача радіохвиль.

Комунікаційне або мережеве обладнання – це периферійні пристрої, що здійснюють перетворення сигналів, які використовуються в комп'ютері, на сигнали, що передаються через лінії зв'язку, і навпаки. Такими пристроями є мережеві адаптери, модеми та ін.

В описах мережевих пристроїв наводиться інформація про рівні, на яких ці пристрої працюють, згідно моделі ISO (Open Systems Interconnection). Модель ISO є стандартною моделлю, що визначає архітектуру комп'ютерних мереж і протоколів обміну даними. Ця модель складається з семи рівнів, кожен з яких відповідає за конкретні функції і завдання. Розуміння моделі OSI є ключовим для будь-якого інженера мереж, оскільки вона надає структурований підхід до розробки та управління мережевими протоколами. Рівні моделі наведені в табл. 6.1.

Використовуючи лінію зв'язку і мережевий адаптер можна побудувати найпростішу мережу, але надійність і продуктивність такої мережі буде

невисокою. Суттєво покращити характеристики мережі дозволять такі мережеві пристрої:

- комутатори (Switch) – обладнання, яке призначене для об'єднання декількох комп'ютерів комп'ютерної мережі в межах одного сегмента мережі. Комутатор може мати різну кількість портів (зазвичай від 8 до 32). Зазвичай комутатор працює на рівні каналу передачі даних або мережевому рівні (рівень 2 і рівень 3 еталонної моделі OSI) і підтримує різні пакетні протоколи. У даний час існує безліч типів комутаторів, таких як комутатори локальної мережі, комутатори Ethernet тощо. Серед них комутатор локальної мережі в основному використовується для обміну даними в комутованій локальній мережі, тоді як комутатор Ethernet в основному використовується для передачі даних в Ethernet. У мережі комутатор використовується для фільтрації та пересилання пакетів між сегментами локальної мережі;

Таблиця 6.1 – Рівні моделі ISO

	Одиниця даних	Рівень	Функція	Приклади протоколів
ОС	Дані	7. Прикладний	Користувацькі програми та сервіси, взаємодія з застосунками	HTTP SMTP DNS
		6. Подання	Перетворення та форматування даних, шифрування та декодування	MIME SSL
		5. Сеансовий	Керування сеансами зв'язку, синхронізація та керування взаємодією	NetBios
	Сегменти	4. Транспортний	Забезпечення надійної доставки даних, контроль передачі та потоку даних	TCP UDP
Мережа	Пакети	3. Мережевий	Маршрутизація пакетів даних, логічне адресування	IP ICMP
	Фрейми	2. Канальний	Керування доступом до мережі, виявлення та корекція помилок	IEEE 802.3 ARP DHCP
	Біти	1. Фізичний	Опис фізичних характеристик мережі, фізичне кодування та передача даних	IEEE 802.3

- концентратори або хаби (Hub) – об’єднуючі компоненти, до яких підключаються всі комп’ютери в мережі. Нині майже не використовуються – їх змінили комутатори, які виділяють кожен підключений пристрій в окремий сегмент. Зазвичай концентратор працює на фізичному рівні мережі (рівень 1 еталонної моделі OSI), який використовується для підключення сегменту локальної мережі. Концентратор має кілька портів. Коли один порт приймає сигнал, він формує і посилює послаблений сигнал, а потім передає посилений сигнал на всі інші порти, так що всі сегменти локальної мережі можуть бачити пакети. У мережі концентратор діє як загальна точка підключення пристроїв. Для таких пристроїв однією з причин непрацездатності є виникнення апаратної петлі. Проблема може виникнути при підключенні порту до комутатора, в якому утворилася петля. Петля утворюється внаслідок людської помилки, коли два порти комутатора виявляються з’єднаними одним кабелем. При розсиланні комутатором з петлею широкомовних повідомлень вони повертаються на комутатор і повторно ретранслюються знову і знову, викликаючи «шторм» (рис. 6.3);

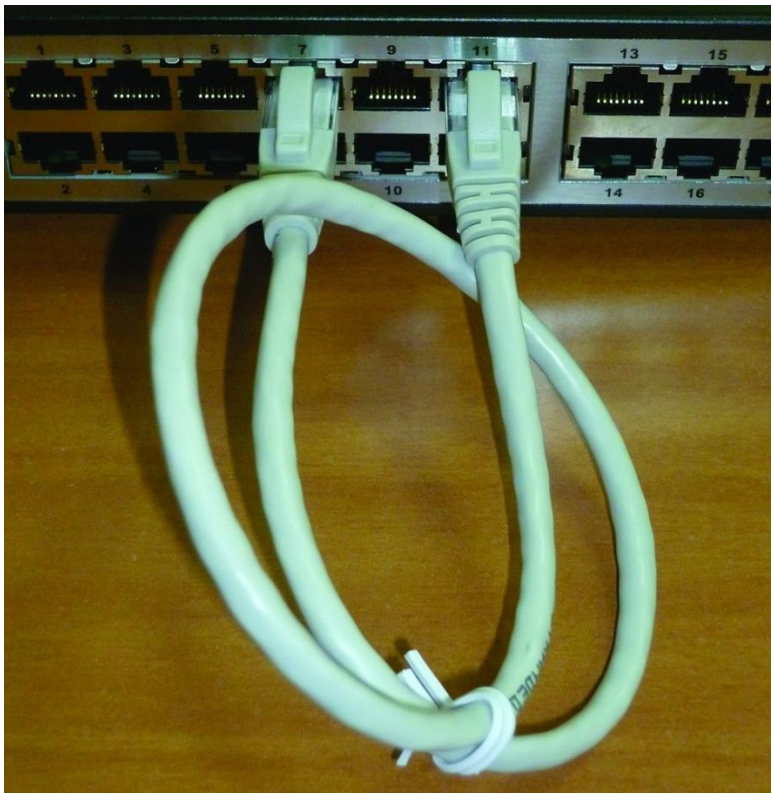


Рисунок 6.3 – Апаратна петля на концентраторі

- мости (Bridge) – це пристрої, що з’єднують дві мережі, які побудовані за різними технологіями. Міст працює на канальному рівні (рівень 2 еталонної моделі OSI). Міст виконує перерозподіл інформаційних потоків між мережами. Мости характеризуються слабким захистом від широкомовного «шторму» та неможливістю підтримки конфігурацій петлеподібних мереж. До переваг відноситься виконання сегментації, що зменшує навантаження мережі та підвищує її загальну продуктивність, та наявність фільтрації, що підвищує безпеку за рахунок запобігання несанкціонованому доступу до певних сегментів локальної мережі;

- повторювач або підсилювач сигналу (Repeater) являє собою мережевий пристрій, що використовується для посилення та регенерації мережевих сигналів. Він працює на фізичному рівні моделі OSI та допомагає розширити зону дії мережевих сигналів за рахунок підвищення їх потужності. Повторювачі зазвичай використовуються у випадках, коли мережеві кабелі необхідно подовжити за межі стандартних обмежень за довжиною. Існують аналогові повторювачі (посилюють аналогові сигнали, які зазвичай використовуються при передачі аудіо і відео) і цифрові ретранслятори (регенерують цифрові сигнали, зберігаючи цілісність даних, що передаються). Повторювачі – це прості пристрої з мінімальними вимогами до конфігурації, що спрощує їх розгортання. До недоліків можна віднести обмежену функціональність (повторювачі лише посилюють і регенерують сигнали, не надаючи додаткових функцій, таких як фільтрація або сегментація) та затримку сигналу (процес посилення та регенерації сигналів призводить до деякої затримки, хоча зазвичай нею можна знехтувати);

- маршрутизатор або роутер (Router) – мережеве обладнання, яке на основі інформації про топологію мережі і визначених правил приймає рішення про пересилання пакетів мережевого рівня між різними сегментами мережі. Маршрутизатор визначає оптимальний маршрут передачі даних. Він допомагає зменшити навантаження мережі, завдяки поділу на домени, а

також завдяки фільтрації пакетів. Зазвичай він розташований на шлюзі двох або більше мережевих з'єднань і працює на мережевому рівні (рівень 3 еталонної моделі OSI). Він використовується для реалізації мережевого зв'язку між двома локальними мережами або двома глобальними мережами або однією локальною мережею та постачальниками послуг мережі Інтернет. Зазвичай у маршрутизаторі є таблиця маршрутизації, яка автоматично вибирає та встановлює маршрут відповідно до умов каналу, а потім надсилає сигнал з найкращим шляхом. Крім того, маршрутизатор підтримує протокол керування повідомленнями мережі Інтернет (ICMP) та інші подібні протоколи, які можуть допомогти IP-хостам і маршрутизаторам передавати контрольні повідомлення та налаштовувати найкращий маршрут між будь-якими двома хостами. Апаратні маршрутизатори вразливі для кібер-зловмисників, оскільки вони містять програмне забезпечення (мікропрограму). Маршрутизатори без виправлень досить вразливі до кібератак. Оскільки маршрутизатори аналізують передачу даних від фізичного до мережевого рівня, вони повільніші, ніж повторювачі та мости;

- модем (Modem) – пристрій зв'язку для перетворення сигналу за допомогою процесів модуляції (зміна параметрів електромагнітного коливання за законом інформаційного повідомлення) та протилежному йому – демодуляції, що дозволяє комп'ютеру передавати дані по телефонній лінії; він є пристроєм узгодження в телекомунікаційних системах, системах автоматичного керування тощо. Стосовно застосування модемів у комп'ютерній техніці, то модеми поділяють на внутрішні (що встановлюються усередині системного блока) та зовнішні (що встановлюються ззовні системного блока). Модем працює на канальному рівні (рівень 2 еталонної моделі OSI). Недоліки модему: повільна швидкість порівняно з іншим обладнанням.

На підприємствах для установки телевізійного, електронного, серверного та мережевого обладнання зазвичай виділяють окрему кімнату. Всі комунікації розміщують у шафі, яка забезпечує зручність монтажу,

ремонту, збереження і безпеку. Залежно від конструкції, телекомунікаційні шафи та стійки можна поділити на такі види:

- підлогова – універсальний тип шаф, який дозволяє розмістити багато обладнання різного типу й потужності. Перевагами підлогових шаф є висока міцність, можливість розширення шляхом додавання модулів. Вони відрізняються наявністю знімних бічних стінок для доступу до обладнання;

- настінна – компактний тип шаф, що призначений для розміщення невеликої кількості обладнання з невисокою потужністю. Перевагами настінних шаф є малогабаритність, мобільність, можливість встановлення на вертикальну поверхню.

Окремий вид – захищена антивандальна телекомунікаційна шафа. Це спеціальний тип шаф, який призначений для захисту обладнання (серверів, маршрутизаторів, комутаторів, модемів, телефонних станцій, елементів оптичних кросових систем) від несанкціонованого доступу, злому або вандалізму в місцях загального доступу – коридорах, горищах, сходових клітинах під'їздів, підвалах – де можливо розкрадання, пошкодження або підміна обладнання сторонніми особами. Серверна шафа має посилені каркас та двері, замки.

Інформаційна система підприємства розпочинається із з'єднань між різними пристроями. Від якості цих каналів зв'язку не в останню чергу залежить стабільність і надійність роботи бізнес-застосунків.

Структурована кабельна система (СКС) – ієрархічна кабельна система, що містить всі необхідні пасивні компоненти для створення середовища передачі інформації: телекомунікаційні кабелі, з'єднувальні патч-корди (кросовери), пасивне комутаційне обладнання.

Вита, звита, скручена або кручена пара (Twisted Pair) – вид мережевого кабелю, з однією або декількома парами ізольованих провідників, скручених між собою (з невеликою кількістю витків на одиницю довжини) для зменшення взаємних наведень при передачі сигналу і покритих пластиковою оболонкою. Використовується для побудови мереж у багатьох технологіях,

наприклад, Ethernet, ARCNet і Token ring. Останнім часом, завдяки своїй дешевизні й легкості установки, є найпоширенішим для побудови локальних мереж.

Кабель приєднується до мережевих пристроїв за допомогою з'єднувача 8P8C (8 Position 8 Contact). Вилки 8P8C прийнято називати роз'ємами RJ-45, хоча це помилкове найменування. Спочатку так називалися вилки 8P2C – 8-позиційні, оснащені тільки центральними контактами 4, 5. Підтримує передачу даних на відстань до 100 метрів. На більших відстанях сигнал через загасання не розпізнається; якщо передача даних на більшу відстань все ж таки необхідна, потрібно скористатися повторювачем, або ж задіяти волоконно-оптичний або коаксіальний кабель.

Існує декілька категорій кабелю «кручена пара», які нумеруються від CAT1 до CAT8. Кабель вищої категорії зазвичай містить більше пар дротів і кожна пара має більше витків на одиницю довжини. Категорії неекранованої крученої пари описуються в стандарті ISO/IEC 11801-1 (Information technology – Generic cabling for customer premises):

- CAT1 – телефонний кабель, всього одна пара. У США використовувався раніше, і провідники були скручені між собою. Використовується тільки для передачі голосу або даних за допомогою модему;

- CAT2 – старий тип кабелю з 2-х пар провідників, підтримував передачу даних на швидкостях до 4 Мбіт/с, використовувався в мережах Token ring і ARCNet. Зараз іноді зустрічається в телефонних мережах;

- CAT3 – 2-парний кабель, використовувався для побудові локальних мереж 10BASE-T і Token ring, підтримує швидкість передачі даних тільки до 10 Мбіт/с. На відміну від попередніх двох, відповідає вимогам стандарту IEEE 802.3. Також дотепер зустрічається в телефонних мережах;

- CAT4 – кабель складається з 4-х скручених пар, використовувався в мережах Token ring, 10BASE-T, 10BASE-T4, швидкість передачі даних не перевищує 16 Мбіт/с, зараз не використовується;

- CAT5 – 4-парний кабель, це і є те, що зазвичай називають кабель «кручена пара». Завдяки високій швидкості передачі (до 100 Мбіт/с при використанні 2 пар і до 1000 Мбіт/с при використанні 4 пар) є найпоширенішим мережевим носієм, що використовується в комп'ютерних мережах дотепер. Для прокладки нових мереж користуються дещо вдосконаленим кабелем CAT5e, який краще пропускає високочастотні сигнали;

- CAT6 – застосовується в мережах Fast Ethernet і Gigabit Ethernet, складається з 4 пар провідників і здатний передавати дані на швидкості до 10000 Мбіт/с. Доданий до стандарту в червні 2002 року, пропускає сигнали частотою до 200 МГц. Існує категорія CAT6a, в якій збільшена частота сигналу, що пропускається, до 500 МГц. За даними IEEE, 70 % встановлених мереж у 2004 році використовували кабель категорії CAT6 (хоча кабелі CAT5 і CAT5e також використовуються в мережах 10GBASE-T);

- CAT7 – швидкість передачі даних – до 10000 Мбіт/с, частота сигналу, що пропускається, до 600–700 Мгц. Кабель категорії CAT7a – покращена версія CAT7, яка надає додатковий захист від перешкод та підтримує швидкість до 10000 Мбіт/с на більш довгих відстанях. Кабель категорії CAT7 екранований;

- CAT8 – Ethernet кабель, який сильно відрізняється від попередніх кабелів тим, що він підтримує частоту до 2000 Мгц, і обмежений 30-метровим каналом. CAT8 кабель також вимагає екранований кабель. Ethernet кабелі CAT8 можуть підтримувати швидкість 25000 Мбіт/с або 40000 Мбіт/с. Зовнішній вигляд кабелю CAT8 аналогічний кабелю нижньої категорії і він термінований роз'ємом 8P8C або іншим роз'ємом. CAT8 кабель також сумісний зі своїми попередніми версіями. Тому можна використовувати його зі стандартним роз'ємом CAT7. Канал класу I (кабель категорії CAT8.1 має конструкцію кабелю U/FTP або F/UTP з повною зворотною сумісністю і взаємодією з CAT6a за допомогою роз'ємів 8P8C. Канал класу II (кабель

категорії CAT8.2) – мінімум F/FTP або S/FTP, сумісний 3 із класом CAT7a за допомогою роз'ємів TERA або GG45 (рис. 6.4).

8P8C (RJ45) GG45 TERA

Рисунок. 6.4 – Роз'єми 8P8C (RJ45), GG45, TERA

У табл. 6.2 наведено основні характеристики крученої пари, яка використовується для з'єднання сучасного мережевого обладнання.

Таблиця 6.2 – Характеристики крученої пари категорій CAT5- CAT8

Атрибут	CAT5	CAT5e	CAT6	CAT6a	CAT7	CAT8
Макс. швидкість передачі	100 Мбіт/с	1 Гбіт/с		10 Гбіт/с		40 Гбіт/с
Тип роз'єму	8P8C				GG45/TERA	8P8C
Кабельна конструкція	UTP			UTP/STP	STP	
Частота	100 Мгц		250 Мгц	500 Мгц	600 Мгц	2000 Мгц
Стандарт зв'язку	100BASE-TX 1000BASE-T	1000BASE-T			10GBASE-T	40GBASE-T
Відстань	100 м					30 м з 40 Гбіт/с

У даний час більшість експлуатованих кабельних систем відносяться до категорії CAT5, яка допускає передачу даних по мережі зі швидкістю до 100 Мбіт/с. Категорія CAT5e вводить невеликі додаткові обмеження, які дозволяють використовувати канали передачі даних з гігабітними мережевими картами. На практиці акуратно виконана проводка на елементах категорії CAT5 дозволяє здійснювати передачу на швидкості до 1 Гбіт/с.

Довжина кабелю від одного елемента активного обладнання до іншого, наприклад від комп'ютера до комутатора, у мережі Ethernet не повинна перевищувати 100 м. Зазвичай стандартами передбачена максимальна довжина самого кабелю 90 м, а 10 м відводиться на сполучні кабелі. На практиці довжина патч-кордів зазвичай становить 1 м і більше. Не має сенсу застосовувати саморобні короткі патч-корди, наприклад, для підключення сервера до патч-панелі, якщо обидва ці елементи розташовані поруч («фірмові» кабелі не можуть бути коротше 60 см). При малій довжині кабелю зростає рівень перешкод, що виникають при відображенні високочастотних сигналів від точки з'єднання кабелю і розетки. Це може призвести до збільшення кількості помилок у лінії.

Для локальної 10-мегабітної мережі, побудованої на концентраторах, існує «правило 5/4»: між будь-якими двома мережевими пристроями повинно бути не більше 5 сегментів мережі з чотирма концентраторами (хабами). Ця вимога обмежує розмір мережі діаметром 500 м, побудованої на концентраторах і з використанням крученої пари.

Хоча в 100-мегабітній мережі зазвичай використовуються тільки комутатори, на практиці в ряді організацій експлуатуються і концентратори. Стандартом передбачено в цьому випадку використання максимум двох концентраторів з відстанню між ними не більше 5 м.

Кабельна система підприємства може бути виконана різними способами: за технологією прихованої проводки, у накладних каналах, у просторі під фальшстелею або над навісною стелею тощо. Власними силами прокладка кабелів зазвичай виконується без трудомістких будівельних

робіт – у накладних каналах, при цьому переходи між окремими приміщеннями здійснюються або через отвори в стінах, або над накладною стелею коридору.

До структурованої кабельної системи входять кабельні системи, що складаються з набору кабелів і телекомунікаційних шаф для різних цілей: комунікація, пожежна та охоронна сигналізація тощо.

У структурі наявні такі підсистеми:

- мережеві;
- підсистеми, що відповідають за безпеку;
- IP-телефонія, голосова пошта;
- системи, контролюючі доступ та авторизацію;
- моніторинг та управління;
- підсистеми зв'язку (аудіо, відео);
- бездротові мережі.

Стандарти структурованих кабельних систем не передбачають можливості складання мережевих ліній передачі даних з кількох ділянок. Це означає, що з'єднання комп'ютера з комутатором має складатися з патч-корду, інформаційної розетки, кабелю, комутаційної панелі (на яку «розшитий» кабель), патч-корду до роз'єму на комутаторі. Якщо з яких-небудь причин довжини кабелю недостатньо (кабель пошкоджений або співробітнику виділено інше місце), то нарощувати його не можна.

На практиці досить часто доводиться стикатися з необхідністю подовження кабелю та виконання його подовженням через скрутки (або, що краще – паяного з'єднання) двох частин. При цьому слід мінімізувати довжину ділянки кабелю, на якому порушений крок крученої пари. Оскільки якість контактів скрутки може істотно знизитися через деякий проміжок часу через вплив зовнішніх умов (наприклад, окислення під впливом вологи), слід подбати про надійну ізоляцію такого з'єднання.

Кожне робоче місце користувача повинно бути обладнане розеткою електроживлення із заземленням та інформаційними розетками. У невеликих організаціях зазвичай використовують розетки існуючої електропроводки.

При цьому, слід враховувати, що відстань між силовою та інформаційною розетками одного робочого місця за стандартом не повинна перевищувати 1 м. Крім того, з метою зниження рівня перешкод і підвищення пожежобезпеки в стандартах визначається мінімальна відстань між силовим та інформаційними кабелями: вона залежить від споживаної потужності, але зазвичай можна орієнтуватися на значення в 10-15 см.

На практиці лише інколи вдається витримати такі відстані, тому, щоб мінімізувати вплив силового кабелю, часто використовують спеціальні кабелі з екрануванням. При розміщенні великої кількості користувачів у приміщенні, не обладнаному достатньою кількістю силових розеток, часто здійснюється проводка силових та інформаційних кабелів до робочого місця в одному каналі.

Відповідно до стандарту, якщо обидва кабелі прокладаються в загальному каналі, то повинна бути передбачена суцільна перегородка між силовими та інформаційним відсіками.

При побудові кабельної системи підприємства часто виникає необхідність підключення пристроїв, рознесених на великі відстані (100 і більше метрів). У цьому випадку успішно застосовуються волоконно-оптичні лінії зв’язку. Зазвичай одне волокно кабелю використовується для передачі сигналу, інше – для прийому. Існує обладнання, що дозволяє за рахунок використання різних діапазонів випромінювання передавати і приймати дані по одному волокну, але воно застосовується не часто: зазвичай оптичні кабелі проєктуються з великим запасом по числу волокон.

Оптичні волокна можуть бути одномодовими і багатомодовими. Діаметр серцевини одномодових волоконне перевищує 10 мікрон. Багатомодові волокна відрізняються від одномодових діаметром серцевини,

який складає 50 мікрон в європейському стандарті і 62.5 мікрон у північноамериканському і японському стандартах.

При відстані 100-200 м застосовуються багатомодові оптичні кабелі. Вартість прокладки і експлуатації такої лінії практично порівнянна з вартістю лінії на крученій парі. У приймально-передавальній апаратурі застосовується простий світлодіод, що істотно здешевлює обладнання. Довжина хвилі переданого імпульсу становить 0.85 мкм, а величина затримки – 4-5 нс/м. При довжинах з'єднань понад 200 м використовується одномодовий оптичний кабель. Відповідне обладнання (приймачі і передавачі оптичного сигналу) за вартістю в кілька разів дорожче, ніж моделі для багатомодового кабелю (приймально-передавальна апаратура генерує сигнал виключно однієї довжини), і воно досить швидко виходить з ладу.

Якщо відстань, на яку передбачається передавати дані, вимірюється десятками кілометрів, то необхідно використовувати передавачі підвищеної потужності (вони присутні в лінійках продукції практично всіх виробників).

Експлуатація волоконно-оптичних каналів зв'язку вимагає підвищеної акуратності з боку користувачів. Не допускається різко згинати кабель, слід оберігати оптичні поверхні від засмічення (не чіпати їх руками, завжди закривати кінці кабелю і гнізда в модулі підключення спеціальними заглушками тощо). У випадку пошкодження кабелю зазвичай потрібне запрошення монтажних фірм, оскільки придбання обладнання для пошуку та визначення місць несправності доступно тільки спеціалізованим організаціям.

Основне застосування оптичні волокна знаходять як середовища передачі на волоконно-оптичних телекомунікаційних мережах різних рівнів: від міжконтинентальних магістралей до домашніх комп'ютерних мереж. Застосування оптичних волокон для ліній зв'язку обумовлено тим, що оптичне волокно забезпечує високу захищеність від несанкціонованого доступу, низьке загасання сигналу при передачі інформації на великі відстані і можливість оперувати з надзвичайно високими швидкостями передачі. Вже

до 2006-го року була досягнута частота модуляції 111 ГГц, у той час як швидкості 10 і 40 Гбіт/с стали вже стандартними швидкостями передачі по одному каналу оптичного волокна.

При цьому кожне волокно, використовуючи технологію спектрального ущільнення каналів може передавати до декількох сотень каналів одночасно, забезпечуючи загальну швидкість передачі інформації, яка обчислюється Терабітами в секунду. Так, до 2008 року була досягнута швидкість 10.72 Тбіт/с, а до 2012 – 20 Тбіт/с. Група вчених та інженерів з Японського національного інституту інформаційних та комунікаційних технологій (NICT) у 2021 р. встановила рекорд швидкості завдяки використанню експериментального фотонного чіпа і чотирьохжильного кабелю (замість стандартного одинарного) – їм вдалося розвинути найбільшу швидкість передачі даних до 319 Тбіт/с.

Коаксіальний кабель – електричний кабель із співвісними провідниками. Основне призначення коаксіального кабелю – передача сигналу в різних областях техніки. Сучасний кабель складається з центрального провідника, оточеного шаром діелектрика, зовнішня поверхня якого покрита обплетенням або фольгою (другим провідником) і захисною оболонкою з пластику, що захищає кабель від дії навколишнього середовища. Для підключення кабельної мережі Інтернет використовується коаксіальний телевізійний кабель, через який одночасно може передаватися відеосигнал і здійснюватися Інтернет-з’єднання. Останній стандарт Docsis 3.0 дозволяє збільшити швидкість мережі Інтернет до 150 Мбіт/с.

Сучасні пристрої для бездротової мережі випускаються на основі декількох стандартів, деякі параметри яких наведено в табл. 6.3.

Wi-Fi, WiFi (Wireless Fidelity) – мережа, що належить «Wi-Fi Alliance». Некомерційна організація «Wi-Fi Alliance» є всесвітнім, неприбутковим промисловим об’єднанням понад 300 компаній, створеним з метою сприяння росту бездротових локальних мереж (WLAN). Маючи на меті покращення роботи користувачів з бездротовими переносними, мобільними, та

розважальними пристроями, програми тестування та сертифікації «Wi-Fi Alliance» гарантують WLAN продукції на основі специфікації IEEE 802.11. З часу запровадження програми сертифікації «Wi-Fi Alliance» у березні 2000 року, понад 4000 продуктів отримали позначку «Wi-Fi CERTIFIED™», що стимулює ширше використання Wi-Fi продуктів та послуг на ринках для споживачів і підприємств. «Wi-Fi Alliance» володіє торговою маркою Wi-Fi. Виробники можуть використовувати цю торговельну марку для сертифікованої продукції, яка була протестована на сумісність.

Загальновживана назва для стандарту бездротового (радіо) зв'язку передачі даних, який об'єднує декілька протоколів і ґрунтується на сімействі стандартів IEEE 802.11 (Institute of Electrical and Electronic Engineers – міжнародна організація, що займається розробкою стандартів у сфері електронних технологій). Найвідомішим та найпоширенішим на сьогодні є протокол IEEE 802.11g, що визначає функціонування бездротових мереж. Починаючи зі стандарту 802.11n версіям були присвоєні назви (Wi-Fi 4 – 802.11n; Wi-Fi 5 – 802.11ac; Wi-Fi 6 – 802.11ax; Wi-Fi 7 – 802.11be; Wi-Fi 8 – 802.11bn). Назви Wi-Fi 0, 1, 2, 3 для попередніх версій є широковживаними, однак неофіційними.

Таблиця 6.3 – Стандарти Wi-Fi

Стандарт	Рік	Частота, ГГц	Макс. швидкість, Мбіт/с	Дальність (приміщення / ззовні)
802.11	1997	2.4	2	20 /100 м
802.11a	1999	5	54	35 / 5000 м
802.11b	1999	2.4	11	35 / 120 м
802.11g	2003	2.4	54	38 / 140 м
802.11n	2009	2.4/5	600	70 / 250 м
802.11ac	2013	5	6933	35 / 5000 м
802.11ax	2019	2.4 / 5 / 6	9608	30 / 120 м
802.11be	2024	2.4 / 5 / 6	46120	30 / 120 м
802.11bn	2028*	2.4 / 5 / 6	100000	немає даних

Стандарт Wi-Fi 8, відомий зараз як IEEE 802.11bn Ultra High Reliability, відноситься до зміни Wi-Fi 7 (802.11be), який станом на початок 2024 р. ще

офіційно не підтверджено. Остаточна специфікація Wi-Fi 8 очікується приблизно у вересні 2028 року.

Встановлення бездротових мереж було рекомендовано у випадках, коли прокладання кабельної системи було неможливим або економічно невигідним. Наразі Wi-Fi широко використовується в багатьох організаціях, оскільки в певних умовах швидкість мережі може перевищувати 100 Мбіт/с, і користувачі можуть вільно переміщатися між точками доступу в межах зони покриття.

Завдяки бездротовим технологіям можна здійснювати з'єднання між комп'ютерами (по типу «точка-точка»), а також між різними сегментами мережі. Найбільш часто в локальних мережах використовуються пристрої бездротового доступу, які виконують функцію точок доступу (AP – Wireless Access Point). У такому випадку персональні комп'ютери підключаються до цих точок, через які здійснюється доступ як до локальної мережі організації, так і до мережі Інтернет. Точка доступу в даному контексті виконує роль концентратора мережі.

Після вибору стандарту бездротової мережі важливо визначити зони покриття. Одна стандартна точка доступу забезпечує покриття на відстань близько 75-100 м, хоча ці показники можуть змінюватися залежно від умов приміщення, матеріалу стін тощо. Найкращим варіантом є проведення тестових вимірів на місцевості з використанням спеціалізованого обладнання.

На кількість точок доступу також впливає вимога до швидкості передачі даних. Швидкість передачі може знижуватися на великих відстанях, якщо рівень сигналу слабкий. Для підвищення швидкості обміну даними рекомендується встановлювати додаткові точки доступу, щоб рівномірно розподіляти навантаження серед користувачів. Зазвичай для оптимального покриття рекомендується встановлювати одну точку доступу на 10 клієнтів, хоча технічна межа кількості підключень бездротових пристроїв може досягати кількох сотень. Бездротові технології також можуть

використовуватися для з’єднання віддалених будівель за допомогою спеціалізованих бездротових мостів та спрямованих антен.

Точку доступу можна порівняти з концентратором локальної мережі, розташованим у загальнодоступному приміщенні, що дозволяє будь-кому підключитися до мережі та прослуховувати передану інформацію. Тому особлива увага повинна бути приділена налаштуванню підключення клієнтів для забезпечення безпеки.

Для захисту інформації, що передається по бездротовій мережі, використовується шифрування даних. Першим стандартом безпеки для Wi-Fi був протокол WEP (Wired Equivalent Privacy або Wireless Encryption Protocol), який передбачав шифрування за допомогою статичного ключа, відомого як користувачеві, так і адміністратору точки доступу. Проте, на практиці цей протокол виявився вразливим, оскільки зловмисники могли за кілька годин обчислити ключ шифрування.

Через це протокол WEP, навіть з подовженим ключем, не може бути визнаним надійним для корпоративних бездротових мереж. У випадку, якщо використовувані пристрої не підтримують новіші стандарти безпеки, адміністратори можуть застосувати віртуальні приватні мережі (VPN), щоб забезпечити захищений канал зв’язку поверх бездротової мережі.

Стандарти WPA і WPA2 (Wi-Fi Protected Access) забезпечують використання динамічних (змінюваних) ключів шифрування та аутентифікацію користувачів при підключенні до бездротової мережі. При проєктуванні бездротового сегмента мережі важливо обирати лише ті пристрої, які відповідають цим стандартам.

Аутентифікація може здійснюватися через перевірку MAC-адрес пристроїв, що підключаються до точки доступу. У цьому випадку адміністратор повинен вручну налаштувати список дозволених MAC-адрес для кожної точки доступу. Однак цей спосіб не забезпечує високий рівень безпеки, оскільки MAC-адреси легко визначити при прослуховуванні

бездротового сегмента, і «підміна» MAC-адреси є нескладною задачею навіть для новачка.

Для ефективного усунення несправностей у лініях зв’язку необхідно мати чітке уявлення про те, як з’єднане активне обладнання та до якого порту підключено кожен комп’ютер. Адміністратор повинен мати комплект документації, що містить описи ліній зв’язку, кабельні журнали (окрім стандартних таблиць на комутаційних шафах), результати приймальних тестів, відомості про проведені ремонти тощо.

Інформацію про топологію мережі, порти і підключене обладнання можна збирати автоматично, якщо структурована кабельна система побудована з використанням керованих комутаторів.

Інвентаризація кабельної інфраструктури є однією з найбільш складних задач в умовах розгалуженої мережі підприємства. В ідеалі адміністратор має кабельні журнали, де зафіксовані типи кабелів та списки з’єднань на комутаційних панелях. Однак часто ці записи виявляються застарілими, і фактичні підключення відомі лише адміністратору.

Якщо адміністратор не має повної інвентаризації, яка охоплює все – від розташування кабелів до призначення портів на комутаційних панелях і навіть списку встановленого програмного забезпечення, то усунення несправностей може затягнутися на значний час. Це, у свою чергу, призведе до збитків для підприємства через відсутність доступу до інформаційних послуг. Чим детальніше ведеться документація і чим уважніше вона оновлюється, тим легше буде орієнтуватися у випадку аварійної ситуації.

Існують спеціалізовані програми, які дозволяють обліковувати робочі місця, кабельні з’єднання та інше обладнання. Такі системи забезпечують швидкий доступ до інформації про шляхи з’єднання між точками «А» і «Б», включаючи номери розеток, кабелі, номери комутаційних панелей і портів, на яких розподілені кабелі, а також іншу важливу інформацію.

6.3. Забезпечення безпеки мережі пристроями та службами

Програмні засоби захисту інформації виконують логічні та інтелектуальні функції захисту і є частиною програмного забезпечення автоматизованих інформаційних систем або входять до складу апаратних засобів та комплексів контролю. Вони є найбільш поширеними засобами захисту завдяки таким перевагам, як універсальність, гнучкість, простота реалізації та можливість змінювати і розвивати їх. Однак, ці властивості роблять їх найбільш уразливими елементами системи захисту інформації підприємства.

Не менш важливим є захист інформації в мережі Інтернет. Раніше ця мережа використовувалась переважно для передачі файлів і електронної пошти, але сьогодні мережа Інтернет виконує набагато складніші функції, наприклад, такі як організація розподіленого доступу до ресурсів. Доступ до мережі Інтернет, що колись був доступний лише для наукових та освітніх груп, набуває дедалі більшого значення в бізнес-середовищі. Компанії використовують його через швидкість, доступність глобального зв’язку, зручність спільної роботи, доступ до програм та унікальних баз даних. Вони розглядають мережу Інтернет як доповнення до своїх локальних мереж.

До технічних заходів захисту можна віднести засоби боротьби з несанкціонованим доступом, резервування критичних комп’ютерних підсистем, організацію обчислювальних мереж з можливістю перенаправлення ресурсів при збоях, установку систем виявлення і гасіння пожеж, а також конструкційні заходи для запобігання крадіжкам, саботажу, диверсіям та вибухам. До того ж, важливим є встановлення резервних систем електроживлення, забезпечення приміщень замками, установка сигналізації та інші заходи.

Усі технічні засоби захисту поділяються на апаратні та фізичні.

Апаратні засоби – це пристрої, які інтегруються безпосередньо в обчислювальну техніку або підключаються до неї через стандартний інтерфейс.

Системи будь-якої складності, незалежно від їх рівня, використовують однакові технічні пристрої. При вирішенні технічних завдань, пов’язаних із захистом і безпекою, важливо правильно обрати основні параметри пристроїв, які забезпечать необхідну надійність виконання їх функцій. Наприклад, система охоронної сигналізації виявляє несанкціонований доступ на охоронювану територію, передає сигнал тривоги на пульт охорони та активує відповідні виконавчі пристрої. Такі системи містять: датчики, пульт-концентратор і виконавчі пристрої.

Апаратні пристрої, як правило, мають компактний розмір і можуть бути підключені між клавіатурою і комп’ютером або інтегровані безпосередньо в клавіатуру. Вони реєструють усі натискання клавіш, виконувані користувачем, і цей процес абсолютно непомітний для нього. Апаратні кейлоггери не потребують установки спеціальних програм на комп’ютері для збору інформації. Незалежно від того, вимкнений чи ввімкнений комп’ютер, вони продовжують працювати. Вони не потребують додаткового джерела живлення і можуть працювати без обмежень по часу.

Кількість даних, яку можуть зберігати ці пристрої, дозволяє реєструвати до 20 мільйонів натискань клавіш, з підтримкою кодування Unicode. Такі пристрої можуть бути виконані в різних формах, що ускладнює їх виявлення навіть під час аудиту інформаційної безпеки. Залежно від того, де вони розташовуються, апаратні кейлоггери поділяються на зовнішні та внутрішні.

Сучасні комп’ютерні системи використовують інтегральні схеми, в яких під час роботи відбуваються швидкі зміни рівнів напруги та струмів. Це призводить до виникнення електромагнітних полів і наведень, які можуть поширюватися в ланцюгах живлення, ефірі, в апаратурі поблизу та комп’ютерах мережі. Спеціальні пристрої, які умовно можна назвати

«шпигунськими», здатні перетворювати ці наведення в оброблювану інформацію. Тому, чим ближче приймач порушника до апаратних засобів, тим вища ймовірність зняття та розшифровки інформації. Це підвищує необхідність дотримання нормативних відстаней і встановлення захисних екранів і фільтрів.

Як приклад можна навести SunScreen від компанії Sun Microsystems (у 1996 р. розробка була визнана продуктом року по версії журнала «LAN Magazin») – апаратну систему для захисту локальних мереж, спеціально розроблену для вирішення завдань фільтрації пакетів, аутентифікації та забезпечення конфіденційності трафіку. Важливою особливістю SunScreen є те, що вона не має IP-адреси, що робить її «невидимою» для зовнішньої мережі і унеможливлює прямі атаки. Пристрій містить п’ять Ethernet-адаптерів, до яких можна підключити чотири незалежні сегменти локальної мережі та комунікаційного провайдера. Для кожного сегмента налаштовується індивідуальна політика безпеки за допомогою складного набору правил фільтрації пакетів, що враховують напрямок передачі, адреси відправника/одержувача, протоколи, час доби та інші параметри. Ще однією важливою особливістю SunScreen є підтримка протоколу SKIP (Simple Key-Management for Internet Protocol), який використовується для забезпечення безпеки роботи, управління та налаштування системи, а також для організації захисту користувацького трафіку. Використання SKIP у системах SunScreen відкриває додаткові можливості для забезпечення безпеки.

Screen-пристрої можуть забезпечити інкапсуляцію всього зовнішнього трафіку локальних мереж, які вони захищають, через SKIP (створюючи SKIP-тунелі). У цьому випадку початкові IP-пакети перетворюються на блоки даних SKIP-пакетів, а мережеві адреси всіх вузлів внутрішніх мереж замінюються на віртуальні адреси, що відповідають Screen-пристроям у зовнішній мережі (це називається адресною векторизацією). Таким чином, весь трафік між захищеними локальними мережами буде виглядати ззовні як зашифрований трафік між вузлами Screen-пристроїв. Для зовнішнього

спостерігача доступною буде лише інформація про динаміку і інтенсивність трафіку, що може бути приховано через стиснення даних або створення «порожнього» трафіку. Приклад вибіркових тунелів з шифруванням на базі пристроїв SunScreen наведено на рис. 6.5.

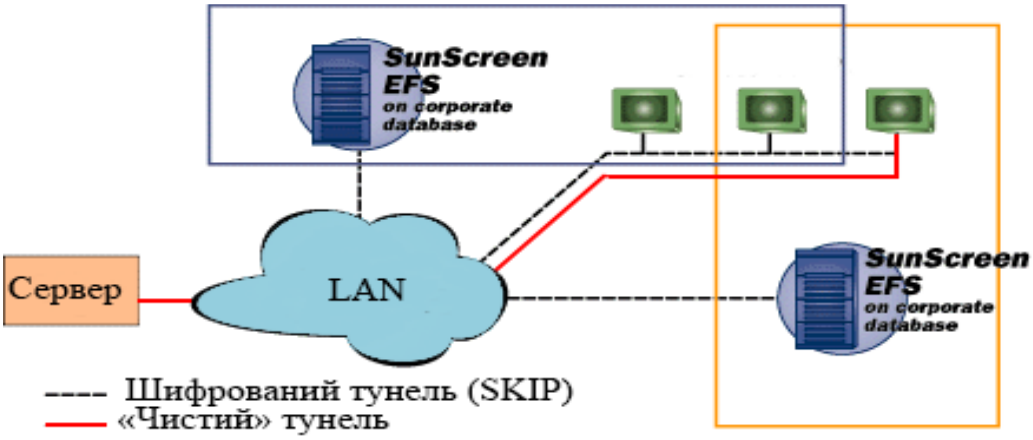


Рисунок 6.5 – Використання SunScreen

Програмно-апаратні засоби можна класифікувати таким чином:

- апаратно-незалежні – працюють без необхідності взаємодії з апаратними засобами захисту (наприклад, паролі, програми для шифрування, антивірусне ПЗ);

- апаратно-залежні – забезпечують інтеграцію апаратних засобів захисту з іншими програмами або операційними системами (наприклад, драйвери, безкоштовне ПЗ);

- автономні – функціонують як частина системи захисту, але можуть працювати незалежно;

- комплексні – кілька елементів системи безпеки використовують спільні ресурси і базу ідентифікації, або обмінюються інформацією між собою (наприклад, використання ключа під час завантаження комп'ютера, де параметри користувача ігноруються, якщо він не пройшов контроль);

- інтелектуальні – всі системи безпеки та управління безпекою об'єднані в єдину структуру.

Основним засобом захисту інформації при міжмережевій взаємодії є міжмережевий екран. Це напівпроникна мембрана, що знаходиться між

внутрішньою мережею (яка потребує захисту) і зовнішнім середовищем (зовнішніми мережами чи іншими сегментами корпоративної мережі). Екран контролює всі інформаційні потоки, що проходять у межах внутрішньої мережі та з неї. Контроль полягає у фільтрації цих потоків – вибірковому пропуску через екран, інколи з виконанням додаткових перетворень та інформуванням відправника про відмову в доступі до його даних.

Фільтрація здійснюється відповідно до набору правил, які попередньо завантажуються в екран і базуються на політиці безпеки організації.

Ситуації, коли корпоративна мережа має тільки один зовнішній канал, є рідкісними. Зазвичай корпоративні мережі складаються з кількох територіально відокремлених сегментів, кожен з яких підключений до мережі загального користування. У такому випадку кожне підключення повинно бути захищене окремим екраном. Насправді, корпоративний зовнішній міжмережевий екран є складеним, і це вимагає вирішення задачі злагодженого адміністрування (керування і аудиту) всіх його складових.

Серед усіх загроз, яким піддається інформація в автоматизованій системі, важливу роль займають загрози, що стосуються даних, переданих через канали і лінії зв’язку між різними територіально відокремленими частинами системи. На практиці, якщо захист відсутній, канали зв’язку є найбільш уразливими елементами автоматизованої системи, оскільки вони за своєю природою та умовами розташування відкриті для як пасивних, так і активних атак з боку порушника.

При розробці методів захисту передачі даних слід забезпечити:

- уникнення розкриття змісту інформації;
- перешкоджання аналізу потоку даних;
- виявлення змін у потоці повідомлень;
- виявлення переривання передачі повідомлень;
- виявлення спроби встановлення хибного з’єднання.

Існує два основні підходи до захисту передачі даних: канальні (лінійні) та абонентські (міжкінцеві). Канальні методи забезпечують захист потоку

даних для кожного окремого каналу, незалежно від того, хто є відправником і хто одержувач. Абонентські методи забезпечують захист кожного повідомлення під час його передачі від джерела до отримувача.

Канальні методи забезпечують захист усього потоку повідомлень, який передається через певний канал зв'язку між двома вузлами, незалежно від джерела і адресата. Основним їх недоліком є те, що компрометація одного з вузлів мережі передачі даних може призвести до розкриття великої частини потоку повідомлень, тому необхідно захищати всі вузли цієї мережі.

Абонентські методи забезпечують захист повідомлень під час їх передачі між джерелом і адресатом, так що розкриття одного з каналів зв'язку не призводить до витоку інформації з усього потоку. Цей метод забезпечує захист саме між парою користувачів або між користувачем і обчислювальним процесом.

Основною перевагою є те, що питання використання таких методів може вирішуватися окремими користувачами без порушення інтересів інших учасників. Одним із варіантів абонентських методів є методи, орієнтовані на з'єднання, при яких мережа передачі даних розглядається як середовище, що дозволяє користувачам встановлювати з'єднання або віртуальний канал від джерела до отримувача. У такому випадку кожне з'єднання захищається окремо. В абонентських методах захист потрібен тільки для обладнання джерела і адресата з'єднання.

Основними механізмами захисту повідомлень є:

1. Розкриття змісту повідомлень. Основним методом захисту від розкриття змісту повідомлень є шифрування, яке може бути канальним або абонентським.

Канальне шифрування виконується незалежно для кожного каналу зв'язку. Зазвичай для цього застосовуються симетричні потокові шифри, і між вузлами підтримується безперервний потік шифрованих бітів, при цьому використовуються довгострокові ключі шифрування. Вузли, де проводиться шифрування, мають бути захищені.

Абонентське шифрування передбачає, що кожне повідомлення, за винятком деяких даних заголовка, оброблюваних у проміжних вузлах, шифрується на джерелі і не розшифровується до моменту досягнення адресата. Для кожного з'єднання можна використовувати унікальний ключ або більш складне дроблення при розподілі ключів (наприклад, один ключ для кожної пари з'єднаних комп'ютерів або один для всієї захищеної підмережі). Часто застосовується комбінація канального та абонентського шифрування.

2. Аналіз потоку. Захист від аналізу потоку повідомлень містить маскування таких параметрів, як:

- частота передачі повідомлень;
- довжина повідомлень;
- джерела та адресати повідомлень.

Основні заходи захисту містять:

- генерацію фальшивих (надлишкових) повідомлень;
- доповнення блоку даних до фіксованої довжини;
- маскування адреси призначення;
- використання захищених протоколів передачі.

Контрольні питання

1. Що повинні забезпечувати основні принципи безпеки корпоративної мережі?
2. Назвіть основні методи і інструменти для забезпечення безпеки в мережі.
3. З чого складається мережева інфраструктура?
4. Що дозволяє отримати аутсорсинг мережевої інфраструктури?
5. Які типи кабелів застосовуються в кабельній мережі?
6. Які існують стандарти бездротових мереж?
7. Які існують варіанти топології мереж?
8. Як поділяються мережі за розміром?

9. Що таке канало- та мережеутворювальне обладнання?

10. Які існують лінії зв’язку?

11. На які рівні поділяється мережа згідно моделі ISO?

12. Які є основні мережеві пристрої та на яких рівнях моделі ISO вони працюють?

13. Яке призначення має телекомунікаційна шафа?

14. З чого складається структурована кабельна система?

15. Які типи крученої пари використовуються для побудови мережі?

16. Які характеристики мають оптичні кабелі?

17. Що описує сімейство стандартів IEEE 802.11?

18. Які існують протоколи безпеки для Wi-Fi?

19. Назвіть приклади пристроїв та служб для забезпечення безпеки мережі.

20. Яким чином можна класифікувати програмно-апаратні засоби забезпечення безпеки?

21. Які підходи використовуються для захисту передачі даних?

7. СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ ВІД ЗАГРОЗ КІБЕРТЕРОРИЗМУ

Інформаційні ресурси, що належать державі, суспільству, окремим організаціям чи фізичним особам, мають велику цінність, оскільки вони мають матеріальне вираження і потребують захисту від різноманітних загроз, які можуть знизити їх значущість. Загрози, що ведуть до зниження цінності інформаційних ресурсів, називаються небезпечними або несприятливими. Потенційно можливий несприятливий вплив називається загрозою [16].

Захист інформації в автоматизованих системах полягає в створенні та підтримці ефективної системи заходів, що включає як технічні (інженерні, програмно-апаратні), так і нетехнічні (правові, організаційні) заходи. Це забезпечує запобігання або ускладнення реалізації загроз, а також зниження можливих втрат. Тобто, захист інформації спрямований на забезпечення безпеки як інформації, що обробляється, так і самих автоматизованих систем, гарантуючи збереження їх властивостей. Така система заходів, що забезпечує захист, називається комплексною системою захисту інформації.

Багато проблем забезпечення захисту інформації в автоматизованій системі можна вирішити за допомогою організаційних заходів. Однак, із розвитком інформаційних технологій зростає потреба в застосуванні технічних засобів захисту.

Правову основу для забезпечення технічного захисту інформації в Україні складають Конституція України, закони України, такі як «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про науково-технічну інформацію», а також концепції національної безпеки, технічного захисту інформації та інші нормативно-правові акти. Крім того, на захист інформації впливають міжнародні угоди України в цій сфері.

Автоматизована система є організаційно-технічною структурою, що поєднує обчислювальні засоби, фізичне середовище, персонал і оброблювану інформацію. Основними напрямами технічного захисту інформації в таких системах є захист від несанкціонованого доступу та захист від витоку інформації через технічні канали (оптичні, акустичні, електромагнітні випромінювання).

Основні напрямки державної політики в сфері інформаційної безпеки включають [12]:

- забезпечення балансу між дотриманням прав людини, зокрема свободи слова, і виконанням державних функцій, спрямованих на виявлення та запобігання загрозам інформаційній безпеці громадян, суспільства та держави;

- розвиток нормативно-правової бази для регулювання інформаційного простору та його захисту від зовнішніх загроз, а також гармонізація з міжнародними стандартами;

- створення ефективної державної інформаційної політики, спрямованої на розвиток національного інформаційного простору, координацію з іншими державними органами та суб'єктами, які займаються інформаційною безпекою;

- розвиток співпраці між державними, приватними та громадськими секторами для реалізації державної інформаційної політики, а також для забезпечення інформаційної безпеки та підтримки національного інформаційного продукту;

- підтримку та поширення національного інформаційного продукту, зокрема за межі України, а також використання його для обміну досвідом щодо протидії викликам у сфері демократичних цінностей та свободи слова в глобальному інформаційному середовищі.

Для розгляду порядку проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі необхідно спочатку дати деякі визначення:

- інформаційна система – організаційно-технічна система, що реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки та програмного забезпечення;

- телекомунікаційна система – організаційно-технічна система, що реалізує технологію інформаційного обміну за допомогою технічних і програмних засобів шляхом передавання та приймання інформації у вигляді сигналів, знаків, звуків, зображень чи іншим чином;

- інтегрована система – сукупність двох або кількох взаємопов'язаних інформаційних та (або) телекомунікаційних систем, в якій функціонування однієї (кількох) з них залежить від результатів функціонування іншої (інших) таким чином, що цю сукупність у процесі взаємодії можна розглядати як єдину систему.

Під інформаційно-телекомунікаційною системою (ІТС) розуміється будь-яка система, яка відповідає одному з трьох наведених вище видів автоматизованих систем.

Комплексна система захисту інформації (КСЗІ) – це організаційні (обов'язкові) та технічні (при необхідності) заходи для захисту інформації від розголошення, витоку та несанкціонованого доступу (рис. 7.1).

Регулювання створення, впровадження та використання КСЗІ в Україні виконується відповідно до нормативних документів із технічного захисту інформації (НД ТЗІ).

Створення КСЗІ в Автоматизованій Системі або Інформаційно-Телекомунікаційній Системі здійснюється згідно з НД ТЗІ 3.7-003-05 «Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» на підставі технічного завдання, розробленого відповідно до вимог НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі».

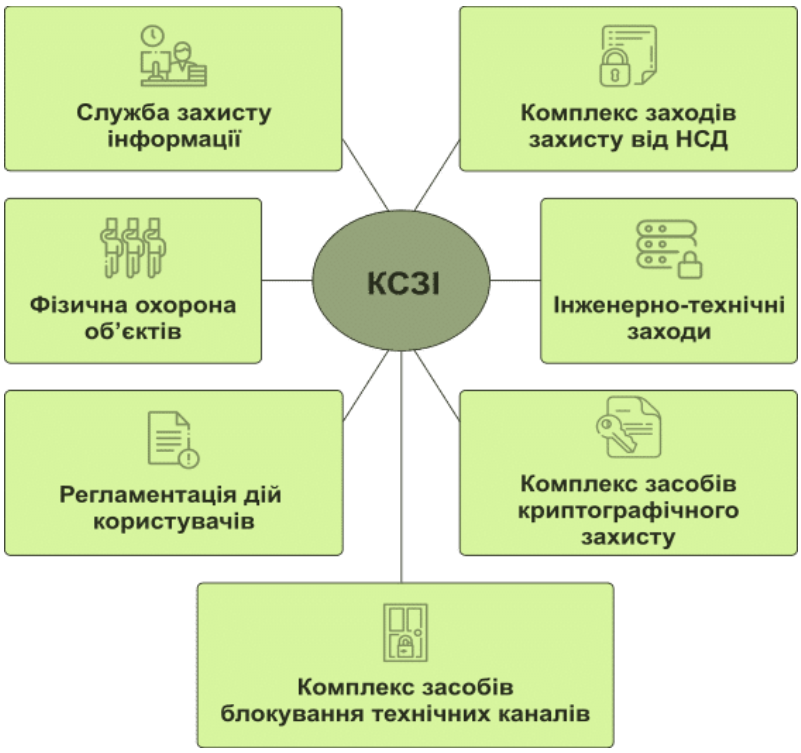


Рисунок 7.1 – Структура КСЗІ

До складу комплексної системи захисту інформації входять заходи та засоби, що реалізують різноманітні методи, механізми та технології для забезпечення захисту інформації від:

- витоку інформації через технічні канали, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні канали, а також інші канали, через які може здійснюватися несанкціонований вихід інформації;

- несанкціонованих дій та несанкціонованого доступу до інформації, які можуть бути здійснені шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, обхід систем захисту для неправомірного використання або маніпулювання інформацією, а також впровадження шкідливих пристроїв чи програм (наприклад, закладних пристроїв або комп'ютерних вірусів);

- спеціального впливу на інформацію, що може включати вплив на цілісність даних через формування електромагнітних полів або сигналів, з

метою порушення або руйнування систем захисту і компрометації інформації.

Ці заходи є критично важливими для забезпечення високого рівня конфіденційності, цілісності та доступності інформації в умовах постійно зростаючих загроз у кіберсередовищі.

7.1. Напрямки вдосконалення захисту інформаційного простору України від загроз кібертероризму

Основною метою створення системи захисту інформації є забезпечення її надійності. Система захисту інформації – це організована сукупність елементів, таких як об’єкти та суб’єкти захисту, методи й засоби захисту, а також заходи, що виконуються для забезпечення безпеки. Компоненти цієї системи, з одного боку, є її частинами, а з іншого – вони також формують систему, здійснюючи відповідні захисні функції. Оскільки система визначається як сукупність взаємопов’язаних елементів, завдання системи захисту інформації полягає в інтеграції всіх складових в єдине ціле. У такій системі кожен компонент, виконуючи свою задачу, одночасно підтримує функціонування інших складових, будучи логічно та технологічно пов’язаним з ними.

Надійність захисту інформації безпосередньо залежить від системного підходу. У разі відсутності узгодженості між окремими частинами системи ризик виникнення «проколів» у технології захисту зростає.

По-перше, потреба в комплексних рішеннях полягає в необхідності об’єднання різних локальних систем захисту інформації в єдину структуру, в якій усі частини повинні працювати як єдине ціле. Наприклад, це може стосуватися різних видів захисту, таких як правовий, організаційний, інженерно-технічний захист.

По-друге, потреба в комплексних рішеннях обумовлена самим призначенням системи. Система повинна об’єднати всі складові захисту з логічною та технологічною точки зору. Однак вона не охоплює всі питання

щодо повноти цих складових і не враховує всі фактори, які можуть впливати на ефективність захисту. Наприклад, система може включати певні об’єкти захисту, але питання того, чи всі вони потрапляють до її сфери, виходить за межі системи.

Отже, якість і надійність захисту інформації залежать не лише від видів складових системи, але і від їх повноти, яка забезпечується з урахуванням усіх чинників і обставин, що впливають на захист. Повнота складових системи захисту, що базується на аналізі цих факторів і обставин, є другим аспектом комплексного підходу. Необхідно враховувати всі параметри уразливості інформації, можливі загрози її безпеці, охоплювати всі об’єкти, що потребують захисту, використовувати всі доступні методи, засоби та ресурси для захисту, а також реалізувати заходи, які відповідають цілям і завданням захисту.

По-третє, лише комплексний підхід дозволяє забезпечити безпеку всіх елементів інформації, що потребують захисту, у будь-яких умовах. Це означає, що повинні бути захищені всі носії інформації в усіх точках її збору, зберігання, передачі та використання, безперервно і в будь-яких режимах функціонування систем обробки інформації. Однак комплексний підхід не виключає, а навпаки, передбачає диференційований захист залежно від типу носіїв інформації, рівня її секретності, ступеня конфіденційності, засобів її зберігання і обробки, форм уразливості, а також каналів і методів несанкціонованого доступу.

Отже, важливість комплексного підходу до захисту інформації полягає в:

- інтеграції локальних систем захисту;
- забезпеченні повноти всіх складових системи захисту;
- забезпеченні всебічного захисту інформації.

На рис. 7.2 наведено перелік головних етапів впровадження КСЗІ.

Рисунок 7.2 – Етапи впровадження КСЗІ

Повний перелік кроків створення КСЗІ ІТС включає такі роботи:

- обстеження середовищ функціонування ІТС;
- розробка моделі загроз та моделі порушника;
- формування політики безпеки;
- розробка технічного завдання на створення КСЗІ та погодження його з Держспецзв'язком України;
- розробка і реалізація проєкту КСЗІ;
- введення КСЗІ в дію та оцінка захищеності;
- попередні випробування;
- дослідна експлуатація;
- державна експертиза КСЗІ;
- супроводження КСЗІ.

Кожний етап дозволяє виконати певний перелік робіт і є необхідним для початку робіт щодо наступного етапу.

Для виконання завдань із захисту інформації, які необхідно вирішувати в ІТС, повинен бути створений підрозділ захисту інформації в ІТС – служба захисту інформації ІТС. У підрозділах організації також можуть бути

створені позаштатні підрозділи захисту інформації або призначені окремі відповідальні особи.

По завершенні державної експертизи і наявності атестату відповідності починається експлуатація створеної КСЗІ в складі ІТС у штатному режимі, відповідно до плану захисту в ІТС і експлуатаційної документації на складові частини КСЗІ.

Розкриття змісту головних етапів:

1. Визначення загальних вимог до КСЗІ в інформаційно-телекомунікаційних системах.

Обґрунтування потреби в створенні КСЗІ.

Підставою для визначення необхідності створення КСЗІ є вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певної інформації або забезпечення її захисту (цілісності чи доступності). Якщо підприємство працює з конфіденційними даними, такими як фінансова звітність чи персональні дані співробітників, законодавство може вимагати їхнього захисту. Тоді керівництво підприємства має прийняти рішення щодо створення КСЗІ для виконання цих вимог. Також важливим фактором є рішення власника інформації, якщо нормативно-правові акти надають йому право визначати, як діяти в конкретній ситуації.

Після прийняття рішення що створення КСЗІ виконується збір вихідних даних для обґрунтування необхідності створення КСЗІ на основі:

- аналізу нормативно-правових актів – це можуть бути державні закони, відомчі правила або внутрішні політики організації, що визначають, які дані повинні бути захищені або обмежені в доступі;

- ідентифікації чутливої інформації – процес визначення, які типи даних, що обробляються в ІТС, потребують особливого захисту (фінансові звіти, медичні записи тощо);

- оцінки переваг впровадження КСЗІ – оцінюється, яку користь принесе розробка КСЗІ з точки зору економії витрат, підвищення безпеки чи покращення репутації організації. Впровадження КСЗІ може знизити ризики

витоку даних, що в свою чергу покращить довіру клієнтів і забезпечить відповідність вимогам регуляторів.

Після всебічного аналізу організація приймає рішення про необхідність розробки та впровадження КСЗІ. Якщо результати аналізу вказують на високу вартість або ризик відсутності належного захисту, компанія приймає рішення про розробку КСЗІ для забезпечення захисту критичних даних.

Огляд середовищ функціонування ІТС також є важливим на даному етапі. Під час проведення огляду ІТС аналізується як комплексна організаційно-технічна система, що об'єднує обчислювальні ресурси, фізичне середовище, середовище користувачів, оброблену інформацію та технології її обробки – середовище функціонування ІТС.

Метою цього огляду є збір базових даних для формування вимог до КСЗІ шляхом опису кожного середовища функціонування ІТС і виявлення елементів, які можуть впливати на безпеку інформації, як безпосередньо, так і опосередковано. Під час цього етапу також визначаються взаємозв'язки між елементами різних середовищ, а результати обстеження документуються для подальшого використання в наступних етапах. Вже під час обстеження ІТС може бути виявлено, що певні пристрої користувачів або програмне забезпечення мають вразливості, які можуть бути використані для несанкціонованого доступу до даних.

Огляд проводиться після того, як концепція ІТС (основні принципи її побудови) розроблена, визначено основні завдання і характеристики ІТС, а також описані функціональні комплекси системи й варіанти їх реалізації.

Перш ніж розпочати детальне обстеження ІТС, необхідно мати план її архітектури і структури, наприклад, чи використовуються в системі хмарні технології або локальні сервери.

При огляді обчислювальної системи ІТС слід провести аналіз і описати:

- загальну структуру і склад (перелік і характеристики обладнання, технічних і програмних засобів, їх взаємозв'язки, конфігурацію, архітектуру та топологію, а також засоби захисту інформації, їх розташування);

- види і характеристики каналів зв’язку;

- особливості взаємодії окремих компонентів і їх взаємний вплив;

- можливі обмеження у використанні засобів.

Важливо виявити компоненти обчислювальної системи, що містять або не містять засобів захисту інформації, оцінити їх можливості і характеристики, у тому числі налаштування за умовчанням. Огляд може показати, що деяке обладнання не має вбудованих засобів шифрування або засобів захисту від несанкціонованого доступу, що вимагає додаткових заходів захисту для забезпечення безпеки інформації.

Метою проведеного аналізу є створення загального уявлення про наявні можливості для забезпечення захисту інформації, а також виявлення компонентів ІТС, що потребують посилених заходів безпеки і додаткових засобів захисту.

Під час **огляду інформаційного середовища** аналізується вся інформація, яка обробляється та зберігається в ІТС, включаючи як дані, так і програмне забезпечення. Всі ці дані повинні бути класифіковані за різними аспектами, такими як режим доступу та правовий статус. Крім того, для кожного виду інформації і типу об’єкта, де вона зберігається, потрібно визначити й описати властивості захисту інформації, такі як конфіденційність, цілісність і доступність, а також безпека комп’ютерної системи, зокрема спостережуваність. Для кожної інформації та компонентів ІТС необхідно чітко визначити, які засоби захисту застосовуються, щоб зберегти ці властивості. Наприклад, якщо в ІТС зберігаються фінансові звіти компанії, ця інформація повинна мати високий рівень конфіденційності, а доступ до неї має бути обмежений лише для конкретних користувачів з відповідними правами.

Аналіз технології обробки інформації включає виявлення особливостей обігу електронних документів, визначення інформаційних потоків, а також місця їх призначення і принципи керування цими потоками. Фіксується також порядок використання носіїв інформації під час функціонування ІТС.

Для електронних документів необхідно точно описати, як ці документи передаються між різними відділами і чи є належні заходи безпеки для їхнього захисту під час передавання.

При **огляді фізичного середовища** проводиться аналіз розміщення засобів обробки інформації ІТС на об'єктах, які пов'язані з інформаційною діяльністю, комунікаціями та системами життєзабезпечення. Оцінюються такі характеристики фізичного середовища:

- розташування компонентів ІТС на території (генеральний план, ситуаційний план);
- наявність охорони та перепускного режиму;
- наявність спеціально обладнаних приміщень для розміщення компонентів ІТС;
- режими доступу до фізичних компонентів ІТС;
- захист від технічної розвідки та впливу навколишнього середовища;
- технічні характеристики систем заземлення та умови зберігання носіїв інформації.

Для серверів, які обробляють чутливу інформацію, повинно бути забезпечено спеціально захищене приміщення з контролем доступу та протипожежною системою. Також, якщо є ризик витоку інформації через канали зв'язку, потрібно звернути увагу на використовувані заходи для захисту цих ліній.

Під час **обстеження середовища користувачів** вивчаються такі аспекти:

- функціональний склад користувачів, їхні обов'язки і кваліфікація;
- повноваження користувачів щодо доступу до відомостей та компонентів ІТС;
- повноваження користувачів щодо управління КСЗІ;
- можливості різних категорій користувачів щодо доступу до ресурсів ІТС;
- наявність засобів захисту інформації в ІТС.

Якщо в організації є кілька категорій користувачів – від адміністраторів до звичайних працівників – кожна категорія повинна мати чітко визначені права доступу. Адміністратор може мати доступ до всіх функцій системи, а звичайний користувач – лише до певних розділів інформації.

Усі результати обстеження середовищ функціонування ІТС оформлюються у вигляді акта, який, у разі необхідності, включається до відповідних розділів плану захисту інформації в ІТС.

Якщо в результаті обстеження було виявлено слабкі місця в захисті фізичного середовища, ці пункти описують в акті і включають до плану, щоб запланувати заходи для їх усунення.

Наприкінці етапу формується завдання на створення КСЗІ. Визначаються основні завдання захисту інформації в ІТС, зокрема мета створення КСЗІ, обраний спосіб вирішення завдань захисту та ключові напрямки забезпечення безпеки. Якщо ІТС обробляє конфіденційну інформацію про клієнтів, завдання захисту може полягати в забезпеченні конфіденційності та цілісності цих даних, а також обмеженні доступу тільки для авторизованих користувачів.

Проводиться аналіз ризиків, який включає оцінку можливих загроз (модель загроз і модель порушника), наслідків реалізації цих загроз, потенційних збитків та інших факторів, і на основі цього складається перелік основних загроз для ІТС. При суттєвій загрозі витоку інформації через технічні канали оцінюються можливі збитки від витоку конфіденційних даних або їх підробки.

Визначаються загальна структура та склад КСЗІ, а також конкретні вимоги до методів, засобів та заходів захисту інформації. Окремо встановлюються допустимі обмеження на застосування певних методів захисту (наприклад, обмеження на використання засобів активного захисту від витоку через електромагнітні канали, які можуть вимагати спеціалізованого обладнання, яке забезпечує належний рівень захисту).

Також обговорюються обмеження щодо функціонування ІТС, використання її ресурсів для задач захисту та припустимі витрати на створення КСЗІ.

Визначаються умови створення, введення в дію та функціонування КСЗІ (або її підсистем і компонентів), а також загальні вимоги щодо інтеграції різних заходів захисту (організаційних, технічних, криптографічних та інших) в ІТС, залежно від функціональних особливостей системи та вимог безпеки. Для забезпечення криптографічного захисту в ІТС може бути встановлено, що всі передавання чутливих даних повинні бути зашифровані, і використовувані ключі повинні відповідати певним стандартам.

На завершенні етапу оформлюється звіт про виконану роботу, який може містити технічні характеристики КСЗІ, опис основних функцій системи, вимоги до безпеки та специфікації для постачальників обладнання, а також вартість розробки та впровадження. Також готується заявка на розробку КСЗІ (наприклад, тактико-технічне завдання або інший документ, що містить всі вимоги та етапи створення КСЗІ).

2. Розробка політики безпеки інформації в ІТС.

Виконується вивчення об’єкта, на якому створюється КСЗІ, та проведення науково-дослідних робіт. На цьому етапі розробник КСЗІ проводить глибоке вивчення об’єкта, на якому буде реалізована система захисту. Він уточнює моделі загроз і аналізує можливість управління ризиками, що були визначені на попередніх етапах. Якщо необхідно, проводяться додаткові науково-дослідні роботи, що допомагають знайти найбільш ефективні способи реалізації завдання на створення КСЗІ. Результати цих робіт оформлюються у вигляді звітів і затверджуються.

Якщо в організації впроваджується нова система для обробки персональних даних, розробник аналізує потенційні загрози (наприклад, витік даних через канали зв’язку) і вивчає нові методи захисту, які допоможуть мінімізувати ці ризики. За результатами науково-дослідних

робіт можуть бути розроблені нові протоколи шифрування або методи контролю доступу.

Далі робиться вибір варіанту КСЗІ – на основі попередніх етапів розробляються кілька альтернативних варіантів концепції КСЗІ і планів їх реалізації. Після цього проводиться детальна оцінка переваг і недоліків кожного варіанту, і вибирається оптимальний шлях. Концепція обраного варіанту оформлюється у вигляді звіту, що містить всі важливі деталі щодо вибору найбільш ефективного рішення.

Наприклад, може розглядатись кілька варіантів захисту для системи: один – з використанням апаратних засобів для шифрування, інший – з програмним шифруванням. Після оцінки витрат і ефективності обирається найбільш оптимальний варіант.

Для оформлення політики безпеки здійснюється вибір основних рішень для протидії всім суттєвим загрозам. Формулюють загальні вимоги, правила, обмеження та рекомендації, що регламентують використання захищених технологій обробки інформації, окремих засобів і заходів захисту інформації, а також діяльність користувачів усіх категорій. Виконана робота з оформлення політики безпеки формується в документальному вигляді.

Політика безпеки може бути розроблена для ІТС у цілому або для окремих її компонентів, якщо мають місце особливості функціонування різних частин КСЗІ, чи для окремих функціональних задач, або технологій обробки інформації. Якщо система містить декілька підсистем (наприклад, базу даних та систему управління доступом), то політика безпеки може бути розроблена окремо для кожної підсистеми, враховуючи специфіку її функціонування.

Політика безпеки розробляється згідно з вимогами національних стандартів, таких як НД ТЗІ 1.1-002 (нормативний документ технічного захисту інформації, який визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп’ютерних системах і створення нормативних і методологічних документів, регламентуючих питання:

визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу; оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача), та рекомендаціями НД ТЗІ 1.4-001 (поради / рекомендації щодо створення КСЗІ в ІКС, які використовуються для надання послуг доступу до мережі Інтернет).

Зазвичай політику безпеки оформлюють як окремий документ у рамках плану захисту інформації. Тому політика безпеки для системи може бути оформлена у вигляді окремого документа, який буде частиною загального плану захисту ІТС, і містити конкретні приписи щодо захисту даних та взаємодії з іншими системами.

3. Розробка технічного завдання на створення КСЗІ.

Технічне завдання на створення КСЗІ в ІТС є основним організаційно-технічним документом, що визначає вимоги до захисту інформації, яку обробляє ІТС. У ньому вказується порядок створення КСЗІ, а також правила проведення всіх видів випробувань та введення системи в експлуатацію в складі ІТС.

Наприклад, технічне завдання на створення КСЗІ для системи обробки фінансової інформації містить вимоги до захисту даних, опис методів тестування системи безпеки та порядок її запуску в роботу після тестувань.

Розробка технічного завдання на створення КСЗІ здійснюється на відповідній стадії робіт зі створення ІТС, враховуючи комплексний підхід до її побудови. Це передбачає інтеграцію всіх необхідних заходів і засобів захисту інформації на всіх етапах життєвого циклу ІТС. Технічне завдання розробляється як для нових ІТС, так і для модернізації існуючих.

У випадку, якщо організація впроваджує нову інформаційну систему для управління персоналом, технічне завдання на створення КСЗІ включатиме заходи по захисту персональних даних на всіх етапах – від збору до зберігання та обробки.

Оформлення технічного завдання на створення КСЗІ може бути виконано кількома варіантами:

- як окремий розділ технічного завдання на створення ІТС;

- як окреме (часткове) технічне завдання;

- як доповнення до технічного завдання на створення ІТС.

Вибір варіанту не обмежується жорсткими правилами. Наприклад, для нової інформаційної системи можуть створити окреме технічне завдання для КСЗІ, а для модернізації існуючої – як додаток до основного технічного завдання на ІТС, що описує тільки зміни в системі захисту.

Для інтегрованих ІТС, що будуються за модульним принципом (наприклад, ІТС складається з кількох модулів, таких як обробка замовлень і обробка даних клієнтів), рекомендується розробляти вимоги до КСЗІ кожної складової частини окремо. Також дозволяється створити один документ на кілька схожих складових, зазначивши між ними відмінності. У цьому документі повинні бути визначені загальні вимоги до безпеки взаємодії між складовими частинами системи.

Єдиним обмеженням при розробці технічного завдання на КСЗІ чи доповнення до технічного завдання на ІТС є необхідність дотримання єдиної термінології, позначень і методів ідентифікації об’єктів, що застосовуються в технічному завдання на створення ІТС.

Для будь-якого з варіантів оформлення технічного завдання на КСЗІ його зміст, порядок погодження та затвердження мають відповідати національним стандартам НД ТЗІ 3.7-001 (встановлює вимоги до порядку розробки, складу і змісту технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, призначеній для оброблення, зберігання і передачі інформації з обмеженим доступом або інформації, захист якої гарантується державою. Положення цього документа розповсюджуються на державні органи, Збройні Сили, інші військові формування, МВС, Раду Міністрів Автономної Республіки Крим і органи місцевого самоврядування, а також підприємства, установи і організації всіх

форм власності, які володіють, користуються і розпоряджаються інформацією, яка належить до державних інформаційних ресурсів, або інформацією, вимога щодо захисту якої встановлена законом. Власники або користувачі іншої інформації, положення цього документа застосовують на свій розсуд) та ГОСТ 34.602 (стандарт поширюється на автоматизовані системи для автоматизації різних видів діяльності (управління, проєктування, дослідження тощо), включаючи їх поєднання, і встановлює склад, зміст, правила оформлення документа «Технічне завдання на створення, розвиток або модернізацію системи»).

4. Розробка проєкту КСЗІ.

Проєкт КСЗІ розробляється відповідно до технічного завдання на створення ІТС або доповнення до нього, а також окремого технічного завдання, яке конкретно стосується КСЗІ.

Під час розробки проєкту КСЗІ формулюють та приймають проєктні рішення, які дозволяють виконати вимоги технічного завдання, забезпечити сумісність і взаємодію різних складових частин КСЗІ, а також інтеграцію різних методів і засобів захисту інформації. Проєкт КСЗІ реалізується на таких етапах створення ІТС: ескізний проєкт, технічний проєкт і робочий проєкт.

Для кожного етапу розробки проєкту КСЗІ склад документації визначається технічним завданням на КСЗІ, а види та зміст документації регулюються ГОСТ 34.201 («Інформаційна технологія. Комплекс стандартів на автоматизовані системи. Види, комплектність і позначення документів при створенні автоматизованих систем», чинний згідно з наказом від 09.01.2024 № 9), НД ТЗІ 2.5-004 (установлює критерії оцінки захищеності інформації, оброблюваної в комп’ютерних системах, від несанкціонованого доступу; документ призначено для постачальників або розробників, споживачів, замовників та користувачів комп’ютерних систем, які використовуються для обробки, збирання, зберігання, передачі тощо критичної інформації, а також для органів, що здійснюють функції

оцінювання захищеності такої інформації та контролю за її обробкою). Документація на програмні засоби повинна відповідати стандартам ЄСПД, а на технічні засоби – стандартам ЄСКД.

Ескізний проєкт КСЗІ. На цьому етапі розробляються попередні проєктні рішення для КСЗІ та її складових частин. При необхідності здійснюється розробка документації, яка описує ці рішення, узгодження та затвердження документації. Зміст документації має бути достатнім для повного опису проєктних рішень на рівні ескізного проєкту.

Визначаються такі аспекти:

- функції КСЗІ в цілому та її окремих складових частин;

- склад комплексів технічного захисту інформації від витоку через технічні канали та спеціальні впливи;

- склад заходів протидії технічним розвідкам, а також організаційних, правових та інших заходів захисту;

- склад комплексів захисту засобами (КЗЗ);

- узагальнена структура КСЗІ та схема взаємодії її складових частин.

Під час виконання ескізного проєкту пропонуються попередні технічні рішення, які дозволяють реалізувати завдання і функції КСЗІ.

Технічний проєкт КСЗІ. Спочатку виконується розробка проєктних рішень КСЗІ, які містять:

- загальні проєктні рішення, необхідні для реалізації вимог технічного завдання на КСЗІ;

- рішення щодо структури КСЗІ, включаючи організаційну структуру, структуру технічних і програмних засобів, алгоритми функціонування та умови використання засобів захисту;

- рішення щодо архітектури засобів захисту інформації та механізмів їх реалізації відповідно до функціонального профілю послуг безпеки інформації.

Також проводяться організаційно-технічні заходи для забезпечення послідовності розробки КЗЗ, архітектури, середовища розробки,

випробувань, а також середовища функціонування та документації експлуатації КЗЗ відповідно до встановлених вимог гарантій щодо надання послуг.

Розробляється, оформлюється, узгоджується та затверджується документація, яка відповідає обсягу, визначеному технічним завданням на КСЗІ. Зміст і формат документації мають бути достатніми для повного опису проєктних рішень на етапі технічного проєкту.

Під час виконання цього етапу готується документація для постачання засобів захисту інформації або продукції, що містить їх у складі, для комплектування КСЗІ. Якщо необхідна продукція відсутня на ринку засобів захисту, то розробляються технічні вимоги або технічні завдання для розробки відповідних засобів.

Також розробляються, оформлюються та затверджуються завдання на проєктування, що стосуються суміжних питань, пов’язаних зі створенням КСЗІ або що впливають на умови її функціонування. Це можуть бути завдання щодо будівельних, електротехнічних, санітарно-технічних та інших підготовчих робіт.

Робочий проєкт КСЗІ починається з розробки та затвердження робочої і експлуатаційної документації. На цьому етапі здійснюється створення, оформлення та затвердження робочої та експлуатаційної документації КСЗІ, а також, за потреби, документації для окремих складових частин системи. Робоча документація повинна містити детальний опис рішень, необхідних для реалізації технічного проєкту, а також визначати способи управління КСЗІ та взаємодії її компонентів. Крім того, вона охоплює документацію, яка необхідна для проведення тестувань, пусконалагоджувальних робіт та випробувань системи.

На етапі робочого проєкту виконується розробка або адаптація засобів захисту: розробляються нові засоби захисту інформації або адаптується наявна продукція до умов функціонування КСЗІ.

Робоча документація для технічного захисту інформації від витоку інформації через технічні канали складається зі схем розміщення засобів технічного захисту в ІТС, а також схем кабельних мереж, мереж живлення та систем заземлення, що виконуються згідно з вимогами відповідних нормативних актів.

Документація для комплексу засобів захисту повинна містити опис процедур інсталяції та ініціалізації комплексу, налаштування механізмів розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, моніторингу дій користувачів, формування і актуалізації баз даних захисту, а також контролю цілісності програмного забезпечення та баз даних. Вона також повинна включати вихідні дані для внесення в бази даних захисту.

Експлуатаційна документація, яка складається, містить опис порядку функціонування КСЗІ, а також інструкції для обслуговуючого персоналу і користувачів щодо забезпечення належного функціонування системи. Вона також визначає порядок супроводження КСЗІ протягом усього життєвого циклу ІТС.

5. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС.

При підготовці організаційної структури та розпорядчих документів проводиться формування цієї структури та розроблюються внутрішні документи, які регламентують процеси забезпечення захисту інформації в ІТС. Наприклад, можуть бути створені накази та інструкції для визначення відповідальних осіб та процедур щодо моніторингу безпеки інформації в системі.

Якщо на попередніх етапах не було призначено відповідальних осіб або не була сформована система захисту інформації, ці дії мають бути завершені на цьому етапі. Визначаються особи, відповідальні за моніторинг доступу до конфіденційної інформації в ІТС, а також за впровадження засобів захисту.

Основна частина документів, що входять до плану захисту, має бути вже розроблена та затверджена. Це включає всі нормативні документи та

інструкції щодо забезпечення безпеки, за винятком тих, які потребують завершення наступних етапів робіт для їх розробки. Можуть бути завершені інструкції щодо управління доступом і забезпечення цілісності даних, хоча документи щодо моніторингу стану безпеки можуть бути розроблені лише після тестування КСЗІ.

Процес створення системи захисту інформації та розробки плану захисту має виконуватись згідно з вимогами нормативних документів, таких як НД ТЗІ 1.4-001, що визначають загальні принципи створення і впровадження КСЗІ в рамках ІТС.

На цьому етапі проводиться навчання всіх категорій користувачів ІТС (технічного персоналу, звичайних користувачів, а також осіб, відповідальних за управління КСЗІ). Навчання охоплює основні положення плану захисту, зокрема політику безпеки інформації та методи експлуатації засобів захисту. Технічний персонал може навчатися налаштуванню антивірусних засобів, а звичайні користувачі – правилам безпеки при використанні електронної пошти тощо. Після навчання проводиться перевірка їхніх знань і реєстрація результатів.

Також не менш важливим є виконання комплектування КСЗІ – забезпечується отримання необхідної продукції для КСЗІ, включаючи засоби захисту інформації, матеріали та обладнання, від постачальників. Наприклад, можуть бути отримані сервери для шифрування даних або спеціалізовані мережеві пристрої для захисту від атак. Також приймається рішення щодо підготовки до проведення оцінки відповідності цих засобів захисту вимогам нормативних документів ТЗІ, якщо на момент проєктування КСЗІ деякі засоби не мали необхідних сертифікатів або експертних висновків. Якщо певне мережеве обладнання ще не має сертифікації, потрібно буде організувати процедуру їх сертифікації перед впровадженням у систему.

Під час реалізації етапу будівельно-монтажних робіт виконуються роботи з реконструкції існуючих або будівництва нових спеціалізованих приміщень, призначених для розміщення технічних засобів ІТС, персоналу, а

також сховищ для матеріальних носіїв інформації. На цьому етапі можуть бути зведені нові серверні кімнати або встановлені спеціальні сейфи для зберігання захищених носіїв даних, що відповідають вимогам безпеки. Всі роботи проводяться з урахуванням технічного завдання на створення КСЗІ, яке визначає вимоги до безпеки приміщень і облаштування.

Будівельні роботи виконуються або самою організацією, що є власником ІТС, або залученими будівельно-монтажними компаніями відповідно до затвердженої проєктної документації. Ця документація розробляється спеціалізованою проєктною організацією з урахуванням вимог державних будівельних норм (ДБН), таких як ДБН А.2.2-2 (технічний захист інформації: загальні вимоги до організації проєктування і проектної документації для будівництва), ДБН 2.2-3-2004 (склад, порядок розроблення, погодження та затвердження проєктної документації для будівництва). Наприклад, для будівництва спеціального приміщення для серверів, з урахуванням вимог до захисту від несанкціонованого доступу та забезпечення належного клімат-контролю може бути розроблений окремий проєкт.

Приймання робіт виконується після завершення будівельних робіт створеною комісією, до складу якої входять представники замовника, проєктної організації та будівельно-монтажної компанії. Комісія здійснює перевірку виконаних робіт на відповідність технічним вимогам і стандартам, визначеним у технічному завданні на КСЗІ, перевіряється, чи відповідають нові приміщення вимогам безпеки, чи правильно виконано заземлення та електричні підключення тощо. За результатами приймання складається акт, який містить оцінку відповідності виконаних робіт вимогам ТЗІ. Цей акт затверджується керівником організації-замовника.

Основною метою пусконалагоджувальних робіт є:

- монтування обладнання і атестація комплексу технічного захисту інформації від витоку через технічні канали;

- встановлення та налаштування комплексних засобів захисту;

- перевірка працездатності засобів захисту як в автономному режимі, так і при їх взаємодії в складі комплексу.

Після монтажу засобів захисту інформації від витоку через акустичні або електронні канали, проводиться перевірка їх роботи в ізольованому режимі (кожен окремо) і в комплексному використанні (як частина єдиної системи).

Монтаж обладнання, включаючи обладнання для захисту інформації, кабельні системи, мережі живлення та заземлення, здійснюється згідно з проєктною документацією, розробленою в рамках робочого проєкту. Якщо до складу КСЗІ входять засоби, які не мають сертифікатів відповідності, необхідно визначити мінімальні безпечні відстані між цими засобами та іншими технічними засобами захисту після проведення спеціальних досліджень.

Ефективність вжитих заходів захисту повинна бути підтверджена інструментальними перевірками під час тестування комплексу технічного захисту інформації. Під час випробувань перевіряється, чи правильно функціонує система захисту від витоку інформації через канали, наприклад, за допомогою спеціальних датчиків, які оцінюють рівень витоку сигналів.

Для виконання спеціальних досліджень та інструментальних вимірювань рівня побічних електромагнітних випромінювань і наводок повинні залучатися підрозділи ТЗІ організації або сторонні організації, які мають ліцензію або дозвіл на виконання таких робіт.

Після завершення робіт складається акт приймання виконаних робіт, який містить:

- категорії приміщень, де встановлено обладнання ІТС, межі контрольованих зон;

- перелік технічних засобів захисту, їх типи, заводські номери;

- оцінку відповідності монтажних робіт вимогам експлуатаційних та нормативних документів;

- пропозиції щодо застосування додаткових заходів захисту в разі, якщо певні вимоги не були виконані під час монтажу.

Додаткові заходи захисту впроваджуються, якщо це було вказано в акті, та відповідно коригується проєктна, робоча та експлуатаційна документація.

Оцінка повноти та якості виконаних робіт здійснюється через атестацію впровадженого комплексу технічного захисту від витоку інформації, за результатами якої видається акт атестації (документ встановленого зразка – «Акт атестації комплексу технічного захисту інформації»), що підтверджує відповідність системи вимогам безпеки.

Інсталяція, ініціалізація та перевірка працездатності комплексних засобів захисту інформації проводиться відповідно до документації робочого проєкту. На етапі налаштування КЗЗ можуть бути виконані спеціальні перевірки працездатності програмного забезпечення, яке відповідає за контроль доступу до інформації, щоб забезпечити належну роботу всієї системи.

Основною метою попередніх випробувань є перевірка ефективності роботи КСЗІ та визначення, чи можна її прийняти для дослідної експлуатації. Під час цих випробувань перевіряється не тільки працездатність КСЗІ, але й її відповідність вимогам технічного завдання. Перевіряється, чи працюють засоби захисту інформації відповідно до специфікацій і чи забезпечують належний рівень безпеки.

Попередні випробування проводяться згідно з затвердженою програмою та методиками. Програму і методики розробляє постачальник КСЗІ, а погоджує їх замовник ІТС. Методики повинні бути заздалегідь погоджені сторонами і відповідати вимогам технічного завдання.

Організацію попередніх випробувань здійснює замовник ІТС, а безпосереднє проведення робіт покладається на розробника КСЗІ разом із замовником. Для цього створюється спеціальна комісія (фахівці з безпеки,

системні адміністратори, представники розробника та ін.), яку очолює представник замовника.

Результати попередніх випробувань оформляються у вигляді «Протоколу випробувань», в якому міститься висновок про можливість використання КСЗІ в дослідній експлуатації, а також перелік виявлених недоліків, заходи для їх усунення і терміни виконання цих робіт.

Після виправлення виявлених недоліків і внесення змін до проєктної, робочої та експлуатаційної документації, КСЗІ приймається в дослідну експлуатацію шляхом оформлення відповідного акта.

Під час дослідної експлуатації КСЗІ відпрацьовуються такі аспекти, як обробка інформації, обіг носіїв інформації, управління засобами захисту, контроль доступу до ІТС та моніторинг дій користувачів. Співробітники СЗІ та користувачі отримують практичні навички з використання програмно-апаратних засобів захисту (наприклад, користувачі можуть навчитися правильно налаштовувати і використовувати систему управління доступом, а співробітники служби безпеки – здійснювати контроль за діями користувачів у системі), а також ознайомлюються з вимогами нормативних документів з питань безпеки.

За результатами дослідної експлуатації складається підсумковий акт, в якому наводиться висновок про можливість або неможливість подальшого представлення КСЗІ на державну експертизу.

Державна експертиза КСЗІ є важливою частиною процесу приймальних випробувань ІТС.

Державна експертиза проводиться з метою перевірки того, чи відповідає КСЗІ технічному завданню та вимогам нормативних документів у сфері захисту інформації, а також для визначення можливості введення КСЗІ в експлуатацію.

Якщо під час державної експертизи виявляються недоліки, вони повинні бути усунуті до завершення експертизи. Якщо це неможливо,

складається акт, в якому вказується перелік необхідних доопрацювань, а після їх виконання проводиться повторна експертиза.

Для інтегрованих ІТС може проводитись окрема експертиза кожної частини КСЗІ. Це означає, що спершу оцінюються окремі модулі, а потім перевіряється їх взаємодія в рамках загальної системи.

Якщо інтегрована КСЗІ включає стандартні модулі, які були розроблені за єдиним технічним завданням, експертиза здійснюється в два етапи: на першому перевіряється один обраний типовий модуль, а на другому – відповідність умов експлуатації для всіх подібних модулів.

Якщо в існуючу КСЗІ додається новий модуль, для його інтеграції не проводиться повторна експертиза всієї системи. Оцінюється тільки взаємодія нового модуля зі вже існуючими компонентами.

Державну експертизу КСЗІ можна проводити паралельно з етапами проектування. Це дозволяє більш швидко виявляти проблеми та забезпечити відповідність системи до вимог на всіх етапах її створення.

Приймальні випробування ІТС проводяться лише після того, як КСЗІ почне функціонувати в складі ІТС.

6. Супроводження КСЗІ.

На цьому етапі проводяться роботи, пов’язані з організаційним забезпеченням функціонування КСЗІ та управлінням засобами захисту інформації відповідно до плану захисту. Це також включає технічне обслуговування, як у гарантійний, так і в післягарантійний періоди, для забезпечення безперебійної роботи засобів захисту. Під час супроводження КСЗІ проводяться регулярні перевірки на відповідність новим вимогам безпеки, а також оновлення програмного забезпечення та апаратних засобів для забезпечення максимальної ефективності системи захисту.

Контрольні питання

1. Що є правовою основою для забезпечення технічного захисту інформації в Україні?

2. Назвіть основні напрямки державної політики в сфері інформаційної безпеки.

3. Що таке комплексна система захисту інформації? Яка її структура?

4. У чому полягає важливість комплексного підходу до захисту інформації?

5. Які основні етапи впровадження комплексної системи захисту інформації?

6. Які основні дії виконуються на першому етапі впровадження комплексної системи захисту інформації?

7. Що робиться під час огляду інформаційного середовища?

8. Що робиться під час огляду фізичного середовища?

9. Що робиться під час обстеження середовища користувачів?

10. Які основні дії виконуються на другому етапі впровадження комплексної системи захисту інформації?

11. Які основні дії виконуються на третьому етапі впровадження комплексної системи захисту інформації?

12. З чого складається виконання четвертого етапу впровадження комплексної системи захисту інформації?

13. Які основні дії виконуються на п’ятому етапі впровадження комплексної системи захисту інформації?

14. Що виконується під час супроводження комплексної системи захисту інформації?

8. СТРАТЕГІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ (2021 – 2025 РОКИ)

Перша Стратегія кібербезпеки України була затверджена Указом президента України № 96/2016 15 березня 2016 р. Однак цей документ містив низку недоліків, що вплинули на ефективність досягнення поставлених цілей, прогрес у реалізації яких становив лише 40 % [17]. По-перше, пріоритети державної політики в кіберсекторі були не до кінця визначені. По-друге, основна увага була зосереджена на діяльності органів безпеки та оборони, без належної уваги до моделі державно-приватного партнерства та мінімального залучення академічної спільноти і громадськості. По-третє, не була створена система індикаторів для оцінки виконання стратегії і стану кібербезпеки.

Однак за цей час були досягнуті деякі позитивні зміни в розвитку системи кібербезпеки України:

- у 2017 році був прийнятий Закон України «Про основні засади забезпечення кібербезпеки України», який визначив повноваження державних органів, підприємств та осіб у цьому секторі;
- у 2020 році було ухвалено Постанову КМУ № 943, яка затвердила порядок формування переліку об’єктів критичної інформаційної інфраструктури, хоча відповідний список так і не був сформований;
- у ряді структур, зокрема в Національному банку, Міністерстві інфраструктури, Державній службі спеціального зв’язку та СБУ, були створені спеціалізовані підрозділи, а також утворено робочий орган РНБО – Національний координаційний центр кібербезпеки, що має на меті координувати діяльність різних учасників державного кіберсектору;
- налагоджено міжнародне галузеве партнерство, зокрема започатковано кібердіалог зі Сполученими Штатами.

Метою Стратегії кібербезпеки України на 2021–2025 роки є створення умов для безпечного функціонування кіберпростору та його ефективного використання на користь громадян, суспільства і держави. Цей документ

(«Стратегія кібербезпеки України», що затверджено Указом Президента України від 26 серпня 2021 року № 447/2021) ґрунтується на принципах стримування, кіберстійкості та співпраці.

Стратегія кібербезпеки України визначає основні пріоритети, цілі та завдання в сфері кібербезпеки, щоб забезпечити безпечне функціонування кіберпростору та сприяти його використанню в інтересах особи, суспільства і держави.

Кібербезпека є одним з ключових пріоритетів у системі національної безпеки України [12]. Для досягнення цього пріоритету планується зміцнення можливостей національної системи кібербезпеки для ефективної протидії кіберзагрозам в умовах сучасного безпекового середовища.

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку і захисту інформації України, Національна поліція, СБУ, Міноборони і Генштаб Збройних Сил, розвідувальні органи, Нацбанк (рис. 8.1).

Рисунок 8.1 – Система кібербезпеки в Україні

Стратегія охоплює період з 2021 по 2025 роки. Координатором реалізації Стратегії є Національний координаційний центр кібербезпеки, що діє в рамках Ради національної безпеки і оборони України.

Складові системи кібербезпеки України наведені на рис. 8.2.

Рисунок 8.2 – Складові системи кібербезпеки в Україні

Основним критерієм успішності Стратегії є досягнення її мети та стратегічних цілей через виконання визначених завдань.

Національний координаційний центр кібербезпеки відповідає за планування заходів для реалізації Стратегії, їх координацію та моніторинг виконання, а також оцінку ефективності.

Розроблений Національним координаційним центром план заходів, схвалений Радою національної безпеки і оборони України, є основою для Кабінету Міністрів України для формування щорічних планів з реалізації Стратегії, а також для здійснення ефективного контролю за виконанням цих завдань і заходів.

Ефективність виконання Стратегії оцінюється через проведення оглядів стану, які здійснюються у встановленому порядку, зокрема щодо:

- національної системи кібербезпеки;

- кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, що підлягає захисту згідно з законодавством.

Результати цих оглядів можуть стати підставою для коригування загального плану та/або щорічних планів заходів з реалізації Стратегії, що обумовлено необхідністю адаптації до змін у безпековому середовищі та для усунення негативних тенденцій у сфері кібербезпеки.

Стратегія є основою для розробки інших нормативно-правових актів у галузі кібербезпеки України та для обґрунтування розподілу необхідних матеріальних, кадрових та інших ресурсів.

Фінансування заходів щодо реалізації Стратегії здійснюється в межах видатків, передбачених Державним бюджетом України для сектору безпеки та оборони, які розглядаються Радою національної безпеки і оборони України відповідно до Бюджетного кодексу України. Згідно з чинним законодавством, державні органи, підприємства та установи повинні передбачати фінансування на кібербезпеку в своїх планах. Також, у рамках державно-приватного партнерства та міжнародної технічної допомоги залучаються інвестиції для розвитку національної системи кібербезпеки.

Щороку Національний координаційний центр кібербезпеки публікує звіт про стан реалізації Стратегії, з підсумковими оцінками її виконання.

Процес реалізації Стратегії має бути максимально відкритим і прозорим, з можливістю демократичного цивільного контролю. Для цього основні учасники національної системи кібербезпеки, у межах своїх повноважень, зобов’язані щорічно інформувати громадськість через офіційні вебсайти про хід виконання Стратегії та фінансування відповідних заходів.

Ключовим завданням для України є розробка та впровадження індикаторів стану кібербезпеки, які базуються на системному моніторингу виявлення та прогнозування кіберзагроз. Це дозволяє оцінювати як досягнення, так і недоліки в роботі системи кібербезпеки. Крім того, створена інтегрована система оцінки новітніх технологій, що впливають на

кіберстійкість країни, а також розроблено інструменти (стандарти, протоколи, сертифікати тощо) для оцінки ефективності застосування новітніх технологій у протидії кібератакам.

Ефективність виконання Стратегії оцінюється через постійний моніторинг і базується на чіткій системі індикаторів стану кібербезпеки.

Індикатори визначають прогрес у виконанні Стратегії за такими аспектами:

- виконання стратегічних завдань, визначених Стратегією, для кожного завдання;

- досягнення стратегічних цілей Стратегії, для кожної з цілей;

- оцінка впливу заходів, що реалізуються в рамках Стратегії, на національну систему кібербезпеки та цифрову трансформацію держави.

Перелік індикаторів розташовано на вебсайті Державної служби спеціального зв'язку та захисту інформації України [21].

Впровадження індикаторів стану кібербезпеки сприяє покращенню моніторингу виконання Стратегії в реальному часі із застосуванням сучасних веб-ресурсів (онлайн-платформ), забезпечуючи прозорість вжитих заходів для суспільства та держави.

Посилення впливу національної системи кібербезпеки на суспільний розвиток оцінюється за такими критеріями:

- збільшення рівня довіри населення до держави в питаннях безпеки кіберпростору;

- формування безпечного інформаційного суспільства, в якому, крім державних органів, активно залучені приватні суб'єкти та громадяни;

- позитивний вплив на захист національних інтересів у галузі кібербезпеки, наприклад, у контексті впливу на розвиток ситуації, пов'язаної з агресією рф проти України.

За допомогою системи індикаторів оцінюється стан досягнення умов для безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства і держави.

Система індикаторів охоплює основні показники стану кібербезпеки, індикатори розвитку національної системи кібербезпеки, а також показники стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, захист якої визначено законом. Це дозволяє здійснювати комплексну оцінку результативності та ефективності реалізації Стратегії.

Стратегія 2021 року визначає три пріоритети: безпечний кіберпростір, захист прав громадян у цифровому просторі та європейську і євроатлантичну інтеграції, а також передбачає досягнення важливих цілей, як-то:

- Для формування потенціалу стримування (С):

С1. Дієва кібероборона. Для цього в структурі Міноборони було заплановане створення кібервійська в першому півріччі 2023 року.

С2. Протидія розвідувально-підривній діяльності та кібертероризму.

С3. Протидія кіберзлочинності шляхом завершення імплементації в українське законодавство положень Конвенції про кіберзлочинність та залучення відповідних практик США.

С4. Розвиток асиметричних інструментів стримування.

- Для набуття кіберстійкості (К):

К1. Національна кіберготовність та надійний кіберзахист (таким чином документ обіцяє створення національної системи управління інцидентами).

К2. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки.

К3. Безпечні цифрові послуги.

- Для вдосконалення взаємодії (В):

В1. Зміцнення системи координації.

В2. Формування нової моделі відносин у сфері кібербезпеки, де за державою закріплюватиметься роль партнера.

В3. Прагматичне міжнародне співробітництво.

Індикатори виконання стратегії кібербезпеки України відповідно до наведених стратегічних цілей:

Стратегічна ціль С1:

- створити в системі Міністерства оборони України кібервійська, забезпечивши їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії в кіберпросторі та надання відсічі агресору. Виконання: перше півріччя 2023 року; кібервійська Збройних Сил України забезпечено ресурсами за відповідними показниками: персонал, озброєння та військова техніка, запаси, навченість. Кібервійська набули спроможностей до виконання завдань за призначенням;

- запровадити ефективні механізми взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони. Виконання: друге півріччя 2023 року; Міністерством оборони України внесено на розгляд Кабінету Міністрів України проект акта Уряду про затвердження механізму (порядку) взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони (політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі);

- розробити та забезпечити виконання плану кібероборони як складової частини плану оборони України. Виконання: розробка – друге півріччя 2022 року, реалізація – постійно; План кібероборони України розроблено та затверджено, забезпечено скоординоване виконання його заходів, забезпечено щорічне (за необхідності) уточнення Плану кібероборони України з метою оновлення політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі;

- забезпечити проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами держав – членів НАТО задля досягнення оперативної сумісності. Виконання: постійно; проведено

щонайменше двічі на рік тематичні навчання, учасниками кожного з яких були представники держав-членів НАТО;

- створити MIL.CERT-UA в інтересах Міністерства оборони України та Збройних Сил України, налагодивши на постійній основі співпрацю із європейською військовою CERT-мережею. Виконання: перше півріччя 2024 року; у Міністерстві оборони України створено MIL.CERT-UA, укладено угоди (меморандуми) щодо співпраці з європейською військовою CERT-мережею;

- забезпечити оцінку спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів, оглядів національної системи кібербезпеки та оглядів стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Виконання: щороку, починаючи з 2023 року; кожний із проведених оглядів (оборонних оглядів; оглядів національної системи кібербезпеки; оглядів стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом) містить окремий розділ, в якому надано оцінку спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони;

- запровадити в системі військово-патріотичного виховання та системі територіальної оборони навчальні програми підготовки та проводити практичні навчання в сфері кібербезпеки. Виконання: запровадження – перше півріччя 2022 року, реалізація – постійно; до кінця першого півріччя 2022 року в навчальних програмах систем військово-патріотичного виховання та територіальної оборони закріплено вимоги до знань слухачів у частині питань кібербезпеки. У подальшому щорічно не менше 25 % учасників цих систем мають бути охоплені такими курсами і здобути практичні навички в сфері кібербезпеки.

Стратегічна ціль С2:

- створити загальнодержавну систему виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об’єктів критичної інформаційної інфраструктури. Виконання: друге півріччя 2024 року; розроблено, погоджено із зацікавленими сторонами та впроваджено загальнодержавну систему виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об’єктів критичної інформаційної інфраструктури;

- удосконалити аналітичне і криміналістичне забезпечення контррозвідувального захисту кібербезпеки держави за рахунок впровадження інноваційних методик обробки та оцінки цифрових даних, формування електронних доказів. Виконання: перше півріччя 2023 року; розроблено, погоджено із зацікавленими сторонами та затверджено методики обробки та оцінки цифрових даних, формування електронних доказів;

- посилити спроможності в проведенні негласних перевірок стану готовності об’єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, поступово охопивши такими заходами всі такі об’єкти. Виконання: друге півріччя 2025 року; удосконалено нормативно-правову базу щодо проведення негласних перевірок, забезпечено необхідний технічний, апаратно-програмний інструментарій, кадрові спроможності для їх проведення;

- посилити контррозвідувальний захист сфери електронних комунікацій, ІТ-сфери, афілійованого з ними середовища, спрямований на виявлення, попередження і припинення розвідувально-підривних посягань спецслужб іноземних держав на національну безпеку України в сфері кібербезпеки. Виконання: постійно; забезпечено попередження та своєчасне реагування на потенційні загрози національній безпеці, пов’язані із розвідувально-підривною діяльністю спецслужб іноземних держав, спрямованих на сферу електронних комунікацій та ІТ-сферу;

- створити технологічні можливості для автоматичного виявлення кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем та на окремих об’єктах критичної інфраструктури, їх блокування та визначення пріоритетності. Виконання: друге півріччя 2023 року; розроблено та затверджено необхідну нормативно-правову базу, інтегровано апаратно-програмні засоби для автоматичного виявлення кібератак у режимі реального часу та їх блокування в загальнодержавні інформаційно-комунікаційні системи та на окремі об’єкти критичної інфраструктури, забезпечено автоматизований інформаційний обмін щодо отриманих даних між відповідальними державними органами, формалізовано механізм блокування кібератак;

- вдосконалити нормативно-правове, організаційне та кадрове забезпечення загальнодержавної системи боротьби з тероризмом у частині, що стосується залучення правоохоронних органів до здійснення заходів з попередження, виявлення і припинення актів кібертероризму. Виконання: перше півріччя 2024 року; протидія та реагування на кібератаки, що створювали небезпеку для життя чи здоров’я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об’єднаннями громадян, юридичними особами, міжнародними організаціями, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій з тією самою метою здійснюється в рамках правового режиму боротьби з тероризмом.

Стратегічна ціль С3:

- завершити імплементацію в законодавство України положень Конвенції про кіберзлочинність. Виконання: друге півріччя 2025 року; всі положення Конвенції про кіберзлочинність імплементовано в українське законодавство;

- забезпечити унормування в установленому порядку питання щодо електронних доказів, використовуючи кращі практики з цих питань Сполучених Штатів Америки, держав – членів ЄС та враховуючи сучасні виклики і тенденції в сфері кібербезпеки. Виконання: друге півріччя 2024 року; законодавство забезпечує можливість ефективно використовувати електронні докази в цивільному, адміністративному та кримінальному судочинстві відповідно до кращих практик Сполучених Штатів Америки, держав – членів ЄС;

- розробити концептуальні підходи щодо реалізації державної політики в сфері забезпечення прав громадян у кіберпросторі. Виконання: друге півріччя 2022 року; розроблено та впроваджено ефективні механізми захисту персональних даних громадян, забезпечення права на повагу до гідності людини і громадянина, свободи слова, недопущення булінгу та використання кіберпростору для сексуальної експлуатації дітей, доведення до самогубства, а також здійснення інших злочинів проти волі, честі та гідності особи, інших прав і свобод людини і громадянина;

- запровадити практику проведення загальнонаціональної інформаційної роз’яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами. Виконання: запровадження – друге півріччя 2022 року, реалізація – постійно; створено нормативні і організаційно-технічні умови для проведення загальнонаціональних інформаційних роз’яснювальних кампаній, інформація щодо алгоритму таких дій є загальнодоступною та розміщена на сторінках офіційних представництв основних суб’єктів національної системи кібербезпеки в мережі Інтернет;

- розробити методику збору кіберстатистики та щороку оприлюднювати статистичну інформацію щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних сайтах. Виконання: розробка – друге півріччя 2023 року, реалізація – щороку; розроблено та затверджено Методику збору кіберстатистики, на офіційних сайтах публікується інформація щодо кіберінцидентів, кібератак та заходів протидії;

- розробити методику проведення щорічних соціологічних досліджень щодо кіберзагроз, з якими стикається населення України, з оцінками ефективності діяльності державних органів у протидії ним і забезпечити проведення таких досліджень. Виконання: розробка – друге півріччя 2024 року, реалізація – щороку; методика розроблена та затверджена, Кабінетом Міністрів України організовано щорічне проведення таких досліджень, починаючи з 2024 року;

- розробити методику комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам, створити необхідні умови для її практичної реалізації. Виконання: друге півріччя 2022 року; розроблено та затверджено методику комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам, зазначена методика використовується на практиці;

- запровадити механізми ідентифікації суб'єктів електронної комерції в кіберпросторі, забезпечивши внесення відповідних змін до законодавства України. Виконання: друге півріччя 2025 року; чинні організаційно-правові механізми забезпечують ідентифікацію суб'єктів електронної комерції в кіберпросторі;

- забезпечити в установленому порядку врегулювання правового статусу криптовалют. Виконання: друге півріччя 2023 року; розроблено та винесено на розгляд Верховної Ради України законопроект щодо врегулювання правового статусу криптовалют, а також підготовлено відповідні зміни до інших законів та підзаконних нормативно-правових актів;

- проводити спільні з ЄС та НАТО заходи, спрямовані на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність та реагувати на кіберзагрози. Виконання: постійно; представники України беруть участь не менш ніж у 90 % міжнародних заходів ЄС та НАТО у сфері кібербезпеки, Україна виступає ініціатором та організатором не менш ніж 7 міжнародних заходів у сфері кібербезпеки щорічно спільно з ЄС та НАТО;

- забезпечити підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем та засобів. Виконання: друге півріччя 2022 року; організовано не менш ніж 5 програм підвищення кваліфікації щорічно, проведено оцінку потреб щодо необхідного апаратно-програмного та іншого забезпечення в інтересах проведення судових експертиз за вказаними напрямами та здійснено його подальше отримання;

- забезпечити підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів. Виконання: постійно; організовано не менш ніж 7 програм підвищення кваліфікації щорічно із охопленням не менш ніж 60 % співробітників, які працюють у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів;

- залучати приватних експертів до проведення комп'ютерно-технічних і телекомунікаційних досліджень та експертиз, досліджень програмного забезпечення, які необхідні для швидкого реагування на кіберінциденти та ефективного розслідування кіберзлочинів. Виконання: постійно; у щонайменше 50 % випадках проведення розслідувань комп'ютерно-технічних і телекомунікаційних досліджень та експертиз, досліджень програмного забезпечення було залучено приватних експертів.

Стратегічна ціль С4:

- удосконалити систему розвідувального забезпечення кібербезпеки держави в частині створення, розвитку сил, засобів та інструментів упередження загроз національній безпеці в кіберпросторі. Виконання: друге півріччя 2023 року; посилено кадрові та технічні спроможності структурних підрозділів розвідувальних органів;

- посилити заходи щодо забезпечення кібербезпеки інформаційної інфраструктури та кіберзахисту інформаційних ресурсів закордонних дипломатичних установ України та об'єктів державної власності України за кордоном. Виконання: перше півріччя 2024 року; впроваджено централізовану систему управління кіберінцидентами в структурі МЗС, орієнтовану на забезпечення кіберзахисту інфраструктури та інформаційних ресурсів закордонних дипломатичних установ України та об'єктів державної власності України за кордоном;

- створити технологічні можливості підключення постачальниками електронних комунікаційних мереж та/або послуг технічних засобів для здійснення оперативно-розшукових, контррозвідувальних та розвідувальних заходів. Виконання: перше півріччя 2024 року; налагоджено взаємодію з постачальниками електронних комунікаційних мереж та послуг, забезпечено інтероперабільність наявного в розвідувальних та контррозвідувальних органів технічного обладнання з обладнанням та відповідними протоколами обміну інформацією систем для підключення технічних засобів для здійснення оперативно-розшукових, контррозвідувальних та розвідувальних заходів;

- запровадити гармонізований з євроатлантичною спільнотою підхід до застосування санкцій у відповідь на підривну діяльність у кіберпросторі, розроблення та узгодження з іноземними партнерами механізму спільних дипломатичних та економічних дій і заходів, зокрема запровадження обмежувальних заходів у вигляді економічних санкцій, у відповідь на деструктивну кіберактивність. Виконання: друге півріччя 2022 року;

запроваджено санкції у відповідь на деструктивну кіберактивність проти України, країн ЄС та США;

- застосовувати усі доступні інструменти дипломатії та міжнародного права задля протидії зловмисній діяльності в кіберпросторі проти України. Виконання: постійно; забезпечено застосування санкцій євроатлантичною спільнотою на рф, юридичних та фізичних осіб рф за зловмисну діяльність у кіберпросторі проти України, ініційовано виключення рф з усіх груп та підгруп з кібербезпеки ключових міжнародних організацій;

- налагодити систематичний обмін інформацією про деструктивну діяльність у кіберпросторі з міжнародними партнерами, насамперед США, державами – членами ЄС та державами – членами НАТО, створити платформи такого обміну. Виконання: постійно; автоматизований обмін інформацією в режимі наближеному до реального часу між НКЦК і CERT-UA з боку України та компетентними органами країн ЄС і НАТО щодо кібератак, виявлених вразливостей систем кіберзахисту національного значення, планів та намірів зловмисників щодо реалізації кібероперацій;

- забезпечити розроблення законопроекту, спрямованого на врегулювання питань щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі. Виконання: друге півріччя 2024 року; законопроект розроблено та винесено на розгляд Верховної Ради України;

- розробити дієві механізми залучення фахівців приватного сектору з кібербезпеки до участі в стримуванні та протидії агресії проти України в кіберпросторі. Виконання: друге півріччя 2022 року; декриміналізовано несанкціоноване втручання в роботу інформаційно-комунікаційних систем з боку фахівців приватного сектору, створено кіберрезерв та відпрацьовано механізм його мобілізації, створено спільноту українських ІТ-спеціалістів, для нейтралізації ворога в кіберпросторі.

Стратегічна ціль К1:

- розробити Національний план реагування на надзвичайні (кризові) ситуації в кіберпросторі, який визначить механізми реагування на кібератаки загальнонаціонального масштабу щодо об'єктів критичної інформаційної інфраструктури та заходи з подальшого відновлення. Виконання: друге півріччя 2023 року; розроблено та затверджено Національний план реагування на надзвичайні (кризові) ситуації в кіберпросторі;

- створити національну систему управління інцидентами, розробити та впровадити стандартні операційні процедури для реагування на різні види подій у кіберпросторі з визначенням критеріїв для оцінки критичності подій та пріоритетності реагування залежно від визначеного рівня критичності. Виконання: друге півріччя 2023 року; створено національну систему управління інцидентами, розроблено та впроваджено стандартні операційні процедури для реагування на різні види подій у кіберпросторі;

- забезпечити постійний моніторинг національних електронних комунікаційних мереж та інформаційних ресурсів, аналіз вторгнень щодо цих мереж і ресурсів, а також виявлення в режимі реального часу аномалій їх функціонування. Виконання: постійно; створено нормативні, організаційні та технологічні умови для проведення постійного моніторингу, забезпечено на постійній основі обмін інформацією про виявлені в режимі реального часу аномалії функціонування національних електронних комунікаційних мереж та інформаційних ресурсів;

- передбачати в проекті закону про Державний бюджет України на відповідний рік видатки на кібербезпеку за окремими бюджетними програмами. Виконання: щороку; передбачено видатки на кібербезпеку за окремими бюджетними програмами;

- розробити базові вимоги та рекомендації з питань забезпечення кібербезпеки для державного і приватного секторів з урахуванням кращих світових практик. Виконання: друге півріччя 2024 року; затверджені базові вимоги та рекомендації з питань забезпечення кібербезпеки;

- налагодити на основі взаємної довіри системний обмін інформацією про кібератаки, кіберінциденти та індикатори кіберзагроз між усіма суб'ктами забезпечення кібербезпеки, насамперед на базі технологічної платформи Національного координаційного центру кібербезпеки, уніфікувати формати обміну інформацією. Виконання: перше півріччя 2023 року; уніфіковано формати обміну інформацією, обмін інформацією відбувається раз на тиждень;

- впровадити ризик-орієнтований підхід у частині заходів забезпечення кібербезпеки об'єктів критичної інфраструктури та державних органів, зокрема, розробити методики ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави, забезпечити нормативне врегулювання питань щодо впровадження обов'язковості здійснення періодичної оцінки кіберризиків на підставі розроблених методик. Виконання: друге півріччя 2025 року; розроблено та затверджено методику ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави;

- впровадити систему сертифікації продукції, яка використовується для функціонування та кіберзахисту інформаційно-комунікаційних систем, насамперед об'єктів критичної інформаційної інфраструктури. Виконання: друге півріччя 2024 року; змінено перелік сфер діяльності, створено та акредитовано орган з сертифікації продукції, процесів та послуг, орган оцінки відповідності в сфері електронних довірчих послуг та орган з оцінки відповідності в сфері криптографічного захисту інформації, розширено сфери акредитації органу з сертифікації продукції в сфері кіберзахисту;

- забезпечити розвиток організаційно-технічної моделі кіберзахисту. Виконання: постійно; розроблено перелік нормативно-правових актів, необхідних для розвитку організаційно-технічної моделі кіберзахисту, визначено необхідні заходи, етапи їх реалізації та відповідальні суб'єкти, які забезпечують розвиток елементів організаційно-технічної моделі кіберзахисту в різних інфраструктурах та їх рівнях, забезпечено

впровадження складових частин організаційно-технічної моделі кіберзахисту;

- завершити процеси визначення об’єктів критичної інфраструктури та об’єктів критичної інформаційної інфраструктури, створити і забезпечити функціонування державного реєстру об’єктів критичної інформаційної інфраструктури, постійно переглядати та оновлювати вимоги до їх кіберзахисту з урахуванням сучасних міжнародних стандартів з питань кібербезпеки. Виконання: друге півріччя 2022 року; затверджено Перелік об’єктів критичної та критичної інформаційної інфраструктури, введено в експлуатацію програмне та апаратне забезпечення реєстру об’єктів критичної інформаційної інфраструктури, переглянуто та оновлено вимоги до кіберзахисту об’єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів;

- запровадити на постійній основі оцінку стану захищеності об’єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість, встановити обов’язковість та періодичність проведення такої оцінки з урахуванням категорій критичності об’єктів, стимулювати участь у цих заходах фахівців з кібербезпеки приватного сектору. Виконання: розробка – друге півріччя 2022 року, реалізація – постійно; визначено обов’язковість та періодичність проведення оцінки стану захищеності об’єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість, а також порядок залучення до таких заходів фахівців з кібербезпеки приватного сектору;

- впровадити систему аудиту інформаційної безпеки, насамперед на об’єктах критичної інфраструктури, визначити механізми та базові методики проведення аудитів, встановити вимоги до аудиторів інформаційної безпеки, їх сертифікації, атестації, навчання та підвищення кваліфікації, а також щодо обов’язковості та періодичності проведення аудитів, надання узагальненої інформації про результати аудитів до Національного координаційного центру кібербезпеки. Виконання: друге півріччя 2022 року; прийнято постанову

Кабінету Міністрів України «Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури»;

- забезпечити розвиток систем технічного і криптографічного захисту інформації, пріоритетність використання засобів технічного і криптографічного захисту інформації вітчизняного виробництва для кіберзахисту державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури. Виконання – постійно; прийнято нормативний документ, що створює передумови пріоритетності використання засобів технічного і криптографічного захисту інформації вітчизняного виробництва, кількість засобів ТЗІ/КЗІ вітчизняного виробництва з підтвердженою відповідністю збільшується;

- впровадити вітчизняні рішення із захисту інформації. Виконання: постійно; в органах державної влади та на об’єктах критичної інформаційної інфраструктури пріоритетність вітчизняним рішенням з захисту інформації;

- проводити командно-штабні кібернавчання стратегічного рівня, а також тематичні кібернавчання та тренінги за участю представників державного та приватного секторів. Виконання: постійно; проводяться командно-штабні кібернавчання стратегічного рівня та тематичні кібернавчання та тренінги за участю представників державного та приватного секторів;

- забезпечити розвиток мережі центрів реагування на кібератаки та кіберінциденти. Виконання: друге півріччя 2025 року; щорічно вводиться в роботу щонайменше один новий центр;

- завершити розгортання Національної телекомунікаційної мережі, збільшити її пропускну здатність, передбачити під час її функціонування використання виключно вітчизняних засобів криптографічного захисту інформації. Виконання: друге півріччя 2022 року; завершено розгортання Національної телекомунікаційної мережі, збільшено пропускну здатність;

- забезпечити функціонування та розвиток Національного центру резервування державних інформаційних ресурсів, провести модернізацію

системи захищеного доступу державних органів до мережі Інтернет. Виконання: постійно; забезпечено функціонування та розвиток Національного центру резервування державних інформаційних ресурсів;

- створити національний сервіс доменних імен (DNS). Виконання: перше півріччя 2023 року; Створено та введено в експлуатацію національний сервіс доменних імен.

Стратегічна ціль К2:

- забезпечити координацію наукового співтовариства під час проведення наукових досліджень і розробок у сфері кібербезпеки та залучення його до заходів з реалізації державної політики в сфері кібербезпеки. Виконання: створення механізму координації – друге півріччя 2022 року, реалізація – постійно; створено та реалізовано на практиці координаційний механізм;

- визначити довгострокові напрями проведення досліджень і розробок у сфері кібербезпеки, а також розробити дієву програму державної підтримки (на основі проектного підходу) стратегічно важливих для кібербезпеки держави наукових установ і організацій, проведення наукових досліджень у цій сфері для потреб національної безпеки і оборони. Виконання: перше півріччя 2023 року; розроблено Концепцію;

- забезпечити стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням розвитку новітніх інформаційно-комунікаційних технологій, зокрема, технологій хмарних та квантових обчислень, 5G-мереж, Інтернету речей, штучного інтелекту, а також появи нових засобів реалізації кіберзагроз з метою створення вітчизняних систем, платформ і продуктів у сфері кібербезпеки. Виконання: розроблення механізму стимулювання – друге півріччя 2022 року, реалізація – постійно; щорічно механізм забезпечує стимулювання мінімум одного нового дослідження чи розробки;

- удосконалити систему підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки. Виконання: реалізація концепції – друге півріччя 2025 року; концепція офіційно прийнята, має затверджений план реалізації;

- розробити Загальнонаціональну програму кіберграмотності, спрямовану на підвищення рівня цифрової грамотності населення України, зокрема, шляхом включення питань стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії ним до навчальних програм загальної середньої, професійної (професійно-технічної), фахової передвищої та вищої освіти. Виконання: розробка програми – перше півріччя 2023 року, реалізація – постійно; щорічно програма охоплює щонайменше на 10 % цільових аудиторій більше, ніж у попередньому році;

- утворити центри, що будуть здійснювати узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій та вітчизняних розробок у цій сфері. Виконання: друге півріччя 2025 року; створено щонайменше 3 центри;

- забезпечити матеріальне стимулювання фахівців у сфері кібербезпеки, які перебувають на військовій, державній службі, у тому числі на державній службі особливого характеру, службі в правоохоронних органах або працюють за трудовим договором у державному секторі і безпосередньо виконують функції із забезпечення кібербезпеки та кіберзахисту, з урахуванням рівнів оплати праці таких фахівців у приватному секторі. Виконання: перше півріччя 2022 року; розроблено та прийнято акти Кабінету Міністрів України, що забезпечать матеріальне стимулювання фахівців у сфері кібербезпеки;

- залучити суб’єктів національної системи кібербезпеки до міжнародних програм навчання і підвищення кваліфікації персоналу. Виконання: постійно; щорічно щонайменше 5 представників основних суб’єктів національної системи кібербезпеки та операторів критичної інфраструктури проходять навчання/підвищення кваліфікації за міжнародними програмами.

Стратегічна ціль К3:

- Зміцнювати довіру приватного сектору та громадян до цифрових послуг, які надаються державою, безумовно виконуючи вимоги щодо забезпечення кібербезпеки та кіберзахисту під час їх надання та інформуючи громадськість про їх безпечність та надійність. Виконання: постійно; щорічне проведення роз'яснювальних інформаційних кампаній, що охоплюють до 20 % представників цільових аудиторій;

- забезпечити впровадження цифрових послуг для населення та розвиток національної інформаційної інфраструктури. Виконання: постійно; щорічно впроваджується щонайменше 5 нових цифрових послуг, 95 % закладів соціальної інфраструктури та органів місцевого самоврядування підключені до широкосмугового доступу до мережі Інтернет із швидкістю не менше 100 Мбіт/с;

- розробити національні стандарти в сфері кібербезпеки, організаційні та технічні вимоги, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, з урахуванням європейських та міжнародних стандартів. Виконання: друге півріччя 2025 року; розроблено та прийнято національні стандарти, гармонізовані із європейськими/міжнародними стандартами в сфері кібербезпеки;

- створити органи з оцінки відповідності надавачів електронних довірчих послуг вимогам для кваліфікованих надавачів кваліфікованих електронних довірчих послуг. Виконання: перше півріччя 2023 року; створено щонайменше два органи з оцінки відповідності надавачів електронних довірчих послуг;

- створити необхідні передумови (нормативні, організаційні, технологічні) для автентифікації користувачів сервісів цифрових послуг (там, де це потрібно) за допомогою інтегрованої системи електронної ідентифікації з використанням технологій електронної ідентифікації та/або електронних

довірчих послуг. Виконання: друге півріччя 2022 року; створено та впроваджено інтегровану систему електронної ідентифікації;

- підвищити ефективність системи захисту персональних даних громадян шляхом гармонізації законодавства України з відповідним законодавством ЄС та посилення відповідальності за порушення встановлених вимог. Виконання: друге півріччя 2023 року; до національного законодавства імплементовано положення GDPR (General Data Protection Regulation) – регламенту, прийнятого в межах законодавства ЄС, що спрямований на забезпечення захисту персональних даних громадян ЄС та врегулювання процесу обробки таких даних компаніями.

Стратегічна ціль В1:

- розробити та затвердити порядок проведення огляду національної системи кібербезпеки, забезпечивши його проведення не менше ніж раз на рік протягом реалізації Стратегії. Виконання: затвердження порядку – друге півріччя 2022 року, проведення огляду – щороку, починаючи з 2023 року; затверджено порядок проведення огляду національної системи кібербезпеки, організовано щорічне проведення такого огляду;

- запровадити обов’язкове негайне, без невиправданої затримки, надання інформації про кіберзагрози, кібератаки та кіберінциденти всіма відомчими та галузевими (секторальними) центрами кібербезпеки (кіберзахисту) до Національного координаційного центру кібербезпеки. Виконання: встановлення вимог та відповідальності щодо інформування – друге півріччя 2022 року, реалізація – постійно; усі відомчі та галузеві центри кібербезпеки повідомили про 100 % кібератак, які були виявлені ними протягом всього періоду виконання Стратегії;

- забезпечити розгляд найважливіших питань у сфері кібербезпеки України на засіданнях Національного координаційного центру кібербезпеки, системний контроль за станом виконання його рішень. Виконання: постійно; засідання Національного координаційного центру кібербезпеки, а також його робочих груп проводяться на системній основі;

- запровадити скоординоване виявлення та розкриття вразливостей інформаційно-комунікаційних систем. Виконання: впровадження системи управління вразливостями – друге півріччя 2023 року, реалізація – постійно; створено нормативно-правову базу та організаційні механізми щодо скоординованого виявлення та розкриття вразливостей інформаційно-комунікаційних систем, впроваджено систему управління вразливостями;

- розробити та запровадити механізми заохочення приватного сектору, наукового співтовариства, громадських організацій та окремих громадян до участі у формуванні та реалізації заходів із забезпечення кібербезпеки. Виконання: перше півріччя 2024 року; розроблено та впроваджено організаційно-правові механізми заохочення;

- забезпечити щорічне оприлюднення основними суб'єктами національної системи кібербезпеки публічних звітів про стан кібербезпеки за сферами відповідальності. Виконання: щороку з 2022 року; публічні звіти про стан кібербезпеки за сферами відповідальності щорічно оприлюднюються на офіційних вебсайтах.

Стратегічна ціль В2:

- забезпечити розроблення законопроекту, спрямованого на врегулювання питань державно-приватного партнерства в сфері кібербезпеки, визначивши форми і методи здійснення такого партнерства, зміцнивши взаємну довіру та передбачивши можливість запровадження експериментальних проектів у цій сфері. Виконання: перше півріччя 2023 року; розроблено та внесено на розгляд Верховної Ради України законопроект;

- запровадити проведення на регулярній основі консультацій заінтересованих сторін та надання методичної допомоги з питань утворення підрозділів кіберзахисту, галузевих (секторальних) центрів забезпечення кібербезпеки та команд реагування на кіберінциденти, всебічно сприяти їх розвитку. Виконання: постійно; створено механізм проведення консультацій, який застосовується на постійній основі;

- залучати на регулярній основі представників наукових установ, громадських організацій та незалежних експертів у сфері кібербезпеки до розроблення проектів нормативно-правових актів, нормативних документів та стандартів у цій сфері. Виконання: постійно; щорічно до розробки проектів нормативно-правових актів, нормативних документів та стандартів у цій сфері залучається мінімум один новий представник;

- підвищити ефективність залучення громадськості до прийняття рішень у сфері кібербезпеки шляхом проведення відповідних опитувань (анкетувань) та розміщення їх результатів на інформаційних ресурсах Національного координаційного центру кібербезпеки та основних суб'єктів національної системи кібербезпеки. Виконання: постійно; щорічно на сайті Національного координаційного центру кібербезпеки розміщується щонайменше одна нова анкета (опитування) з актуальних питань кібербезпеки;

- стимулювати розроблення вітчизняних програмних продуктів, зокрема програмного забезпечення з відкритим кодом, що пріоритетно використовуватимуться для обробки та захисту державних інформаційних ресурсів, а також на об'єктах критичної інформаційної інфраструктури. Виконання: постійно; запроваджено механізм стимулювання розроблення вітчизняних програмних продуктів, зокрема програмного забезпечення з відкритим кодом, щорічно надається підтримка щонайменше трьом вітчизняним програмним продуктам;

- впровадити програму розвитку ринку товарів і послуг у сфері кібербезпеки, що включатиме стимулювання його розвитку та міжнародного визнання. Виконання: друге півріччя 2024 року; розроблено та впроваджено програму розвитку ринку товарів і послуг у сфері кібербезпеки;

- продовжити практику щорічного проведення місяця кібербезпеки в Україні із залученням широкого кола профільних фахівців та експертів державних органів, закладів освіти та наукових установ, а також громадських об'єднань та приватного сектору. Виконання: щороку в жовтні; щорічно

проводяться заходи, присвячені місяцю кібербезпеки в Україні та готується інформаційна довідка, яка відображає: коло залучених профільних фахівців та експертів державних органів, закладів освіти та наукових установ, а також громадських об'єднань та приватного сектору;

- запровадити систему страхування від кіберризиків, зокрема механізм оцінки втрат суб'єктів господарювання внаслідок кібератак для можливості їх відшкодування. Виконання: друге півріччя 2025 року; розроблено та прийнято нормативно-правовий акт, що дозволяє реалізувати в Україні систему страхування від кіберризиків, запроваджено щонайменше один пілотний проект;

- розробити фінансові та нефінансові механізми для сприяння впровадженню сучасних технологій кібербезпеки в державному і приватному секторі, включаючи страхування, лізинг, пільги тощо. Виконання: перше півріччя 2025 року; розроблені та запроваджені фінансові та нефінансові механізми, хоча б один з механізмів функціонує в пілотному режимі.

Стратегічна ціль В3:

- забезпечити участь України в міжнародних заходах ООН щодо заохочення відповідальної поведінки держав у кіберпросторі. Виконання: постійно; щорічно забезпечується участь представників України в 100 % заходів ООН, щорічно надається перелік заходів із зазначеного питання, які відбувались під егідою ООН та хто і в якому статусі приймав у них участь від України;

- забезпечити участь України в доопрацюванні Другого додаткового протоколу до Конвенції про кіберзлочинність щодо вироблення заходів та гарантій для вдосконалення міжнародної співпраці між правоохоронними та судовими органами, а також між органами влади та постачальниками послуг в інших державах. Виконання: постійно; представники України постійно приймають участь у заходах, щорічно надається інформація про кількість заходів, а також хто і в якому статусі приймав у них участь від України;

- розширити шляхом діалогу з міжнародними партнерами доступ правоохоронних органів України до ресурсів Європейського центру боротьби з кіберзлочинністю, до телекомунікаційної системи Інтерполу I-24/7. Виконання: перше півріччя 2023 року; правоохоронні органи України, з числа основних суб'єктів національної системи кібербезпеки, мають постійний доступ до ресурсів Європейського центру боротьби з кіберзлочинністю та до телекомунікаційної системи Інтерполу;

- продовжити співробітництво з Агентством Європейського Союзу з питань мережевої та інформаційної безпеки, зокрема з питань скоординованого розкриття вразливостей та імплементації Директиви Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу як елементу євроінтеграції України. Виконання: постійно; щорічно проводяться щонайменше одні консультації між представниками України та Агентства Європейського Союзу;

- поглибити співпрацю з Міжнародним союзом електрозв'язку в сферах кібербезпеки та електронних комунікацій, зокрема з питань стандартизації в цих сферах. Виконання: друге півріччя 2022 року; забезпечено участь у заходах Міжнародного союзу електрозв'язку в сферах кібербезпеки та електронних комунікацій щодо питань стандартизації і удосконалення національної системи електронних комунікацій;

- розвивати практичне співробітництво з НАТО щодо питань кібероборони, налагодити тісну взаємодію з цих питань із відповідними структурами Альянсу, зокрема Радою управління з кібероборони (NATO Cyber Defence Management Board), Центром операцій у кіберпросторі (Cyberspace Operations Centre), Центром можливостей з реагування на комп`ютерні інциденти (NATO Computer Incident Response Capability), Об'єднаним центром передових технологій з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence). Виконання: постійно;

Україна має офіційне представництво у всіх вказаних структурах (або підписані угоди (меморандуми) про співробітництво);

- поглибити співпрацю з міжнародними організаціями в сфері захисту дітей від сексуального онлайн-насильства. Виконання: постійно; спільно з міжнародними партнерами щорічно проводиться не менше 5 заходів, щорічно реалізується щонайменше один пілотний проект;

- забезпечити розвиток міжнародного співробітництва в сфері кібербезпеки шляхом підтримки міжнародних ініціатив у цій сфері, які відповідають національним інтересам України. Виконання: постійно; щорічно Україна підтримує щонайменше одну міжнародну ініціативу;

- продовжити практику проведення двосторонніх кібердіалогів з державами – партнерами з метою обміну передовим досвідом у сфері кібербезпеки, інформацією про кіберзагрози, розвитку комунікації між заінтересованими державними органами України та іноземних держав, розширити коло держав – партнерів, з якими проводяться кібердіалоги, ініціювати питання щодо укладення двосторонніх договорів про співпрацю в сфері кібербезпеки. Виконання: постійно; щорічно проводяться кібердіалоги з наявними партнерами, а також щорічно додається щонайменше одна країна для таких діалогів;

- створити постійно діючу робочу групу з питань взаємодії із провідними IT-компаніями, світовими провайдерами цифрових послуг, соціальними мережами з метою протидії гібридним загрозам, поширенню дезінформації, можливості застосування санкцій відповідно до законів України. Виконання: перше півріччя 2023 року; створено постійно діючу робочу групу, проведено щонайменше одне засідання робочої групи;

- визначити та затвердити перелік пріоритетних напрямів залучення міжнародної технічної допомоги в сфері кібербезпеки України. Виконання: друге півріччя 2022 року; підготовлено та затверджено список пріоритетних напрямів, проведено щонайменше одні консультації щодо їх підтримки за рахунок міжнародної технічної допомоги.

Напрями зовнішньої політики України в сфері кібербезпеки.

Основним зовнішньополітичним пріоритетом України в сфері кібербезпеки є поглиблення процесів євроінтеграції через узгодження підходів, методів і засобів кібербезпеки з європейськими та натовськими стандартами, а також реалізацію заходів, погоджених з ключовими міжнародними партнерами, з метою підвищення кіберстійкості України, розвитку національної системи кібербезпеки та захисту національних інтересів у кіберпросторі [10].

Україна активно працює над спільною протидією міжнародному тероризму з партнерами, виявленням, попередженням і припиненням злочинів, які порушують міжнародний правопорядок і загрожують безпеці людства. Розвивається співпраця з органами безпеки і спецслужбами країн ЄС і НАТО, включаючи обмін інформацією та досвідом у сфері національної безпеки кіберпросторі, а також активне впровадження світових кращих практик і спільних заходів для зміцнення науково-технічної бази і кадрового потенціалу кібербезпеки.

Україна прагне співпрацювати з міжнародними партнерами та організаціями, що підтримують спільне бачення майбутнього кіберпростору як глобального, відкритого, вільного, стабільного і безпечного, де поважають права людини, основні свободи та демократичні цінності, що є основою для соціально-економічного та політичного розвитку країни.

Україна продовжує активну участь у міжнародному діалозі з питань відповідальної поведінки держав у кіберпросторі, ґрунтуючись на міжнародному праві, Статуті ООН і добровільних нормах, що регулюють поведінку держав. Це вимагає посиленої координації та співпраці зацікавлених сторін на міжнародних форумах, де Україна є не лише учасником, а й ініціатором та організатором.

Оскільки мережа Інтернет стала суспільним надбанням і виходить за межі національних інтересів, Україна активно підтримує багатосторонню модель управління мережею Інтернет, сприяючи міжнародним, регіональним

та національним дискусіям з цієї теми, залучаючи приватний сектор, наукові кола та громадянське суспільство. Спроби деяких авторитарних держав обмежити мережу Інтернет суперечать інтересам України і її соціально-економічній моделі розвитку.

Україна сприяє дотриманню міжнародного права і стандартів у сфері прав людини, заохочуючи застосування кращих практик і активно працюватиме над запобіганням зловживанню новими технологіями. Для цього розширено участь у міжнародних процесах стандартизації та сертифікації в сфері кібербезпеки, а також збільшено представництво в органах стандартизації та сертифікації.

Що стосується розробки стандартів для нових технологій, таких як штучний інтелект, хмарні технології, квантові обчислення та квантові комунікації, Україна наполягає на тому, що мережа Інтернет має залишатися глобальною та відкритою, а технології повинні сприяти захисту основних прав людини, забезпечувати її свободи і конфіденційність у кіберпросторі. Будь-які обмеження мають бути законними та обґрунтованими. Водночас, з огляду на зростаючі загрози в кіберпросторі, Україна займає активну позицію на міжнародних форумах ООН та інших платформах, щоб просувати свої інтереси та знижувати ризики мілітаризації кіберпростору.

Зважаючи на взаємозв’язок між віртуальним простором та співпрацею між державою, приватним сектором, науковими колами та громадянським суспільством, Україна активно розвиває національний кіберпростір як глобальний, відкритий, вільний, стабільний і безпечний, що є важливою умовою успішного розвитку країни.

Протягом реалізації Стратегії Україна робить кібербезпеку одним із основних напрямів своєї міжнародної діяльності, посилюючи потенціал зовнішньополітичних структур та кіберпотенціал держави. Для цього розвивається мережа партнерств у сфері кібербезпеки, зокрема через нові формати і механізми міжнародного співробітництва.

Контрольні питання

1. Які позитивні зміни розвитку системи кібербезпеки України були досягнуті до 2021 року?

2. Що є основними суб'єктами національної системи кібербезпеки?

3. Що входить до складу системи кібербезпеки України?

4. Чим являються індикатори стану кібербезпеки?

5. Які цілі визначено в Стратегії кібербезпеки України 2021 року?

6. Які складові цілі С1 Стратегії кібербезпеки України?

7. Які складові цілі С1 Стратегії кібербезпеки України вже виконано?

8. Які складові цілі С2 Стратегії кібербезпеки України?

9. Які складові цілі С2 Стратегії кібербезпеки України вже виконано?

10. Які складові цілі С3 Стратегії кібербезпеки України?

11. Які складові цілі С3 Стратегії кібербезпеки України вже виконано?

12. Які складові цілі С4 Стратегії кібербезпеки України?

13. Які складові цілі С4 Стратегії кібербезпеки України вже виконано?

14. Які складові цілі К1 Стратегії кібербезпеки України?

15. Які складові цілі К1 Стратегії кібербезпеки України вже виконано?

16. Які складові цілі К2 Стратегії кібербезпеки України?

17. Які складові цілі К2 Стратегії кібербезпеки України вже виконано?

18. Які складові цілі К3 Стратегії кібербезпеки України?

19. Які складові цілі К3 Стратегії кібербезпеки України вже виконано?

20. Які складові цілі В1 Стратегії кібербезпеки України є та які з них вже виконано?

21. Які складові цілі В2 Стратегії кібербезпеки України є та які з них вже виконано?

22. Які складові цілі В3 Стратегії кібербезпеки України є та які з них вже виконано?

23. Які основні напрями зовнішньої політики України в сфері кібербезпеки?

СПИСОК ЛІТЕРАТУРИ

1. Macedo F., Mira da Silva M. Comparative Study of Information Security Risk Assessment Models. Instituto Superior Técnico, Universidade Técnica de Lisboa, 2009. 106 p.

2. Nair A. Introduction to Information Security Risk Assessment using FAIR (Factor Analysis of Information Risk). Aujas, 2021. 15 p.

3. Балджи М. Д. Економічний ризик та методи його вимірювання. Навчальний посібник. Харків : Промарт, 2015. 300 с.

4. Березуцький В. В., Адаменко М. І. Небезпечні виробничі ризики та надійність : навчальний посібник для студентів за напрямком підготовки 6.170202 «Цивільна безпека». Харків : ФОП Панов А. М., 2016. 385 с.

5. Бурячок В. Л., Гулак Г. М., Толубко В. Б. Інформаційний та кіберпростори : проблеми безпеки, методи та засоби боротьби. Підручник. Київ : ТОВ «СТК ГРУП Україна», 2015. 449 с.

6. Бурячок В. Л., Толубко В. Б., Хорощко В. О., Толюпа С. В. Інформаційна та кібербезпека : Соціотехнічний аспект. Підручник. Львів : «Магнолія 2006», 2018. 320 с.

7. Гончар С. Ф. Методологія оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури : автореф. дис. ... докт. техн. наук : спец. 05.13.21. Київ, 2020. 38 с.

8. Гуменюк В. Я., Міщук Г. Ю., Олійник О. О. Управління ризиками. Навчальний посібник. Рівне : НУВГП, 2009. 156 с.

9. Гур’єв В. І., Мехед Д. Б., Ткач Ю. М., Фірсова І. В. Інформаційна безпека держави : навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека». Ніжин : ФОП Лук’янченко В. В., ТПК «Орхідея», 2018. 166 с.

10. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони : підручник. Одеса : ОНАЗ ім. О.С. Попова, 2019. 320 с.

11. Кармінська-Бєлоброва М. В., Ігнатова М. В. Управління ризиками у підприємництві : навч. посібник. Харків : «Слово», 2014. 169 с.

12. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній : практичний посібник. Київ : Консалтингова компанія «СІДКОН», 2021. 372 с.

13. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах : навч. посібник / В. Д. Козюра [та ін.]. Ніжин: ФОП Лук'яненко В. В., ТПК «Орхідея», 2019. 144 с.

14. Корченко О. Г., Казмірчук С. В., Ахметов Б. Б. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія. Київ : ЦП «Компринт», 2017. 435 с.

15. Кравченко М. О., Бояринова К. О., Копішинська К. О. Управління ризиками : навч. посіб. для студ. спеціальності 073 «Менеджмент». Київ : КПІ ім. Ігоря Сікорського, 2021. 432 с.

16. Лісовська Ю. П. Кібербезпека : ризики та заходи : навч. посібник. Київ : Видавничий дім «Кондор», 2019. 272 с.

17. Мануілов Я. С. Огляд новел вітчизняного законодавства у сфері забезпечення кібербезпеки (на прикладі Стратегії кібербезпеки України на 2021 – 2025 роки). Інформація і право № 4(39). Київ, 2021. С. 98-105.

18. Машина Н. І. Економічний ризик і методи його вимірювання. Навчальний посібник. Київ : ЦНЛ, 2003. 188 с.

19. Мохор В. В., Гончар С. Ф., Дибач О. М. Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури. Ядерна та радіаційна безпека 2(82). Київ, 2019. С. 4-8.

20. Рибальський О. В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. Київ : Вид. Національної академії внутріш. справ, 2012. 104 с.

21. Стратегія кібербезпеки України. Державна служба спеціального зв'язку та захисту інформації України. URL :

https://cip.gov.ua/ua/news/strategiya-kiberbezpeki-ukrayini (дата звернення : 16.12.2024).

22. Терентьєв О. М., Зайченко С. В., Клешов А. Й., Шевчук Н. А. Технічні ризики. Теорія та практикум : навч. посібник. Київ : Інтерсервіс, 2020. 164 с.

23. Технології забезпечення безпеки мережевої інфраструктури. Підручник / В. Л. Бурячок [та ін.]. Київ : КУБГ, 2019. 218 с.

24. Яцків В. В., Кулина С. В. Технічні засоби захисту інформації : опорн. консп. лекцій. Тернопіль : ЗУНУ, 2023. 88 с.

Навчальне видання

КОЛОМІЙЦЕВ Олексій Володимирович
ПАНЧЕНКО Володимир Іванович
ЛИСИЦЯ Дмитро Олександрович

ТЕОРІЯ РИЗИКІВ

Навчальний посібник
для студентів спеціальності 123 «Комп’ютерна інженерія»
денної та заочної форм навчання

Відповідальний за випуск проф. Заковоротний О. Ю.

Роботу до видання рекомендував проф. Заполовський М. Й.

В авторській редакції

План 2025 р., поз. 9

Гарнітура Times New Roman. Ум. друк. арк. 14,1.

Видавничий центр НТУ «ХПІ».
Свідоцтво про державну реєстрацію ДК № 5478 від 21.08.2017 р.
61002, м. Харків, вул. Кирпичова, 2.

Електронне видання