МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 004.12:681.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____ к.т.н. Г.В. Шуклін
«____» _____ 2022 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: «ФУНКЦІОНАЛЬНІ МЕТОДИ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ»

студент групи СЗД-42 Яценко Валерій Сергійович _____
(підпис)

Науковий керівник: к.т.н., доцент Пепа Юрій Володимирович _____
(підпис)

Нормоконтроль: Гребенніков Асаді Болдхоядович _____
(підпис)

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»

Завідувач кафедри СІКЗ

_____ к.т.н. Г.В. Шуклін

(підпис)

«_____»_____ 2022 р.

ЗАВДАННЯ

на атестаційну роботу магістра

студенту: Яценку Валерію Сергійовичу

1. Тема роботи: «Функціональні методи оцінки ризиків кібербезпеки», затверджена наказом по університету від « ___ » _____ 2022 р. за № _____ .

2. Термін здачі студентом оформленої роботи « 01 » червня 2022 р.

3. Об'єкт дослідження: властивості інформації, які змінюються під впливом зовнішнього втручання.

4. Предмет дослідження: ризик та методи його оцінювання щодо безпеки даних.

5. Мета роботи: розробка методику функціонального оцінювання кібератак і протидії та оцінити економічну ефективність системи захисту.

6. Перелік питань, які мають бути розроблені:

1. Аналіз властивостей інформації, яка підлягає захисту на підприємстві.
2. Провести функціональне оцінювання ризиків втрати інформації та ефективної протидії.
3. Оцінити економічні ризики втрати інформації в залежності від вагових коефіцієнтів цінності інформації.

7. Перелік публікацій:

8. Перелік ілюстративного матеріалу: Презентація виконана на слайдах для подання за допомогою світлопроектору та комп'ютерних засобів.

9. Дата видачі завдання « 16 » лютого 2022 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «16» лютого 2022 р.

№ з/п	Назва етапів атестаційної роботи	Строк виконання етапів роботи	Примітка
1	Огляд літератури	20.03.22 р.	виконано
2	Написання першого розділу роботи	05.04.22 р.	виконано
3	Написання другого розділу роботи	30.04.22 р.	виконано
4	Написання третього розділу роботи	12.05.22 р.	виконано
5	Оформлення атестаційної роботи	14.05.22 р.	виконано
6	Підготовка демонстраційних матеріалів	20.05.22 р.	виконано

Студент: СЗД-42 Яценко В.С. _____
(підпис)

Науковий керівник: к.т.н., доц. Пепа Ю.В. _____
(підпис)

Нормоконтроль: Гребенніков А.Б. _____
(підпис)

РЕФЕРАТ

Атестаційна робота містить: 67 сторінок, 10 рисунків, 6 таблиць.

Важливість роботи полягає в дослідженні питань економічних ризиків втрати конфіденційної інформації на підприємстві від різних чинників, а також всебічному аналізі функціональних методів критеріальної оцінки вторгнень і протидії кібератакам. На основі цих досліджень проведено якісний та кількісний аналіз економічної ефективності вкладання коштів у побудову системи захисту інформації на виділеному об’єкті.

Метою роботи є розробка методику функціонального оцінювання кібератак і протидії та оцінити економічну ефективність системи захисту.

Завдання роботи:

1. Проаналізувати існуючі властивості інформації, яка підлягає захисту на підприємстві.

2. Провести функціональне оцінювання ризиків втрати інформації та ефективної протидії.

3. Оцінити економічні ризики втрати інформації в залежності від вагових коефіцієнтів цінності інформації.

Об’єктом дослідження є властивості інформації, які змінюються під впливом зовнішнього втручання.

Предметом дослідження є ризик та методи його оцінювання щодо безпеки даних.

Методи дослідження – аналіз, експертне оцінювання, систематизація, ймовірнісний підхід.

Галузь використання – кібербезпека та інформаційна безпека.

Ключові слова: ВТРАТИ, АТАКА, ПРОТИДІЯ, КІБЕРБЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ, КРИТЕРІЙ, ЕКОНОМІЧНИЙ РИЗИК, ЕФЕКТИВНІСТЬ.

ЗМІСТ

ВСТУП

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

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

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

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

В роботі увага приділялася аналізу функціональних підходів до аналізу ризику атак і їх протидіям, економічним ризикам втрати інформації та фінансовим збиткам, які несе підприємство у разі нападу або несанкціонованого перехоплення такої інформації.

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

1 СПОСОБИ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

1.1 Причини перехоплення інформації

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

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

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

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

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

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

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

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

2. Використання відомостей, розповсюджуваних службовцями конкуруючих фірм;

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

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

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

6. Безпосереднє спостереження, здійснюване потай;

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

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

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

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

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

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

13. Перехоплення телеграфних повідомлень;

14. Підслуховування телефонних переговорів;

15. Крадіжки креслень, зразків, документації й ін.;

16. Шантаж і вимагання.

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

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

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

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

1.2 Огляд методів одержання конфіденційної інформації

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

1. Акустичний контроль приміщення, автомобіля, безпосередньо людини;

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

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

4. Схована фото й відеозйомка, спеціальна оптика;

5. Візуальне спостереження за об'єктом;

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

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

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

Акустичний контроль.

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

У тому випадку, якщо є постійний доступ до об'єкта контролю, можуть бути використані найпростіші мініатюрні мікрофони, сполучні лінії які виводять у сусідні приміщення для реєстрації й подальшого прослуховування

акустичної інформації. Такі мікрофони діаметром 2.5 мм можуть уловлювати нормальний людський голос із відстані до 20 м.

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

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

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

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

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

1. По використовуваному діапазоні частот;

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

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

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

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

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

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

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

Мережні закладки, що використовують як канал передачі інформації електромережу, установлюються в електророзетки, подовжувачі, побутову апаратуру або безпосередньо в силову мережу. Їхнім недоліком є мала дальність передачі (у межах одного будинку до трансформаторної підстанції). Перевага мережної закладки – складність виявлення. Прийомна частина виконана у вигляді спецприймача.

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

Контроль і прослуховування телефонних переговорів.

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

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

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

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

1.3 Необхідність захисту інформації

Спроба заощадити на захисті інформації обходиться недешево. За даними опитування, проведеного «Ernst & Young LLP», що зневажають захистом інформації компанії зазнають незлічимих збитків від випадкових помилок, вірусів, а також вторгнень внутрішніх і зовнішніх хакерів.

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

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

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

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

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

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

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

замовлення продукції. Цього року лише 34 % респондентів повідомили, що застосовували Internet для подібних цілей; 87 % опитаних відзначили, що їхня компанія використовує мережу як електронну пошту й дослідницький інструмент.

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

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

Мета – це захист інформації. Основні причини збитків компаній, що зневажають захистом даних наведені в табл. 1.1.

Таблиця 1.1

Основні причини збитків компаній

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

В компаніях 71 % не впевнені в захищеності своїх мереж.

Наведемо 10 порад щодо захисту інформації:

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

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

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

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

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

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

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

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

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

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

1.4 Структура та режим роботи персоналу на об'єкті виробничої діяльності

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

Для нормального функціонування підприємства необхідно, щоб керівництво вело виважену кадрову політику, яку можна представити у

вигляді схеми (рис. 1.1), де містяться інструменти реалізації кадрової стратегії підприємства.

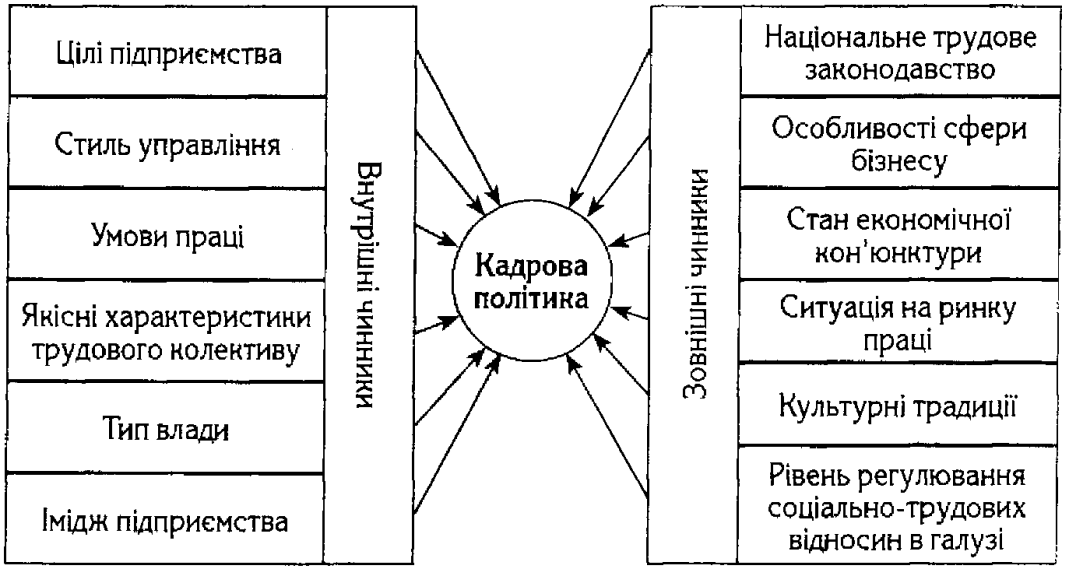


Рисунок 1.1 – Кадрова політика

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

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

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

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

1.5 Заходи захисту інформації на підприємстві

Організаційний захист – це регламентація виробничої діяльності та взаємовідносин виконавців на нормативній основі, що виключає або суттєво ускладнює неправомірне оволодіння конфіденційною інформацією та прояву

внутрішніх та зовнішніх загроз. Його можна представити у вигляді, що приведений на рис. 1.2.

Організаційний захист забезпечує:

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

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

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

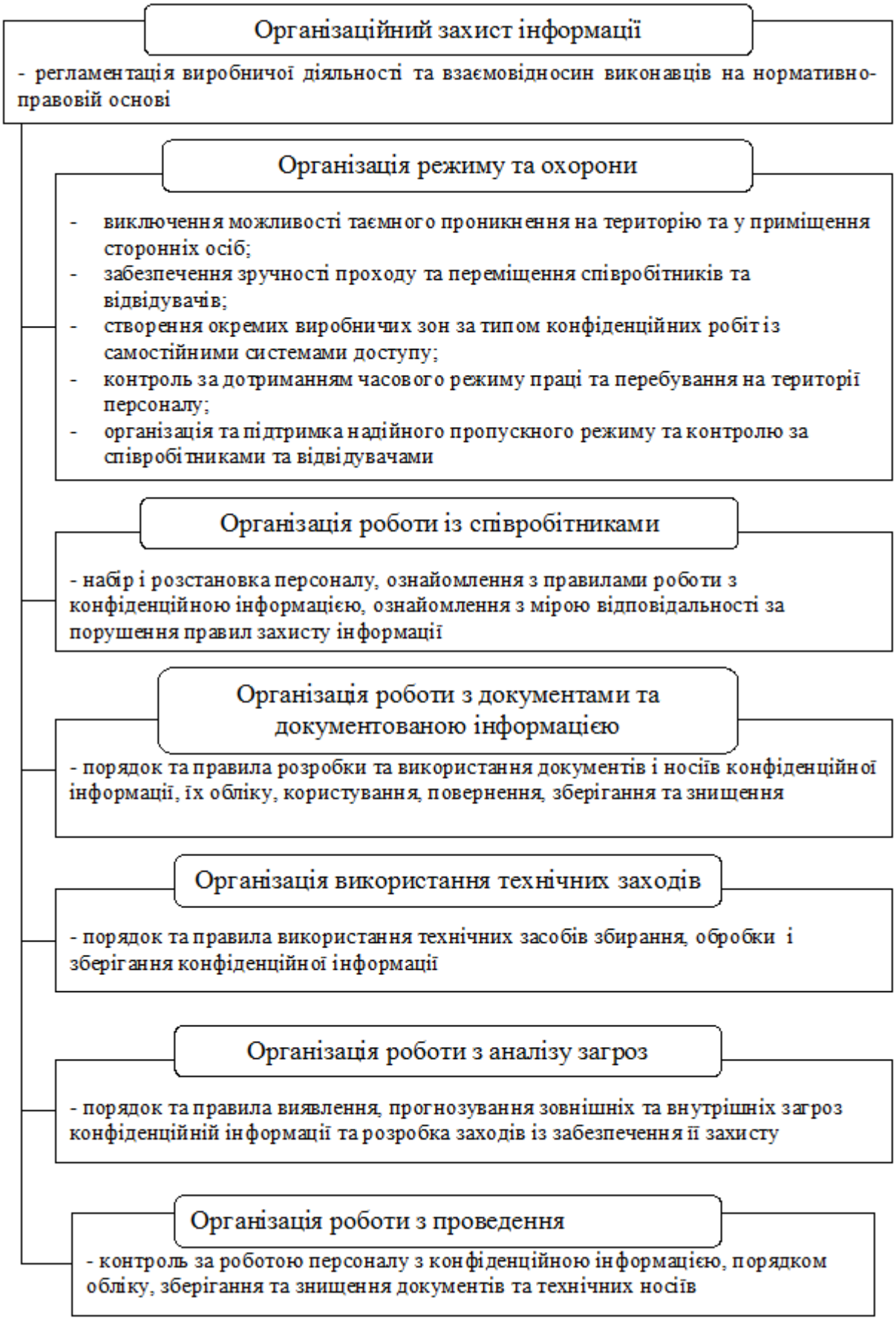


Рисунок 1.2 – Організаційний захист інформації

До основних організаційних заходів відносять наступні:

1) організація режиму та охорони їх позначка:

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

- забезпечення зручності проходу та переміщення співробітників та відвідувачів;

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

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

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

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

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

4) організація використання технічних засобів збирання, обробки, нагромадження та зберігання конфіденційної інформації;

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

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

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

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

- визначення технологічних процесів обробки інформації;

- обґрунтування та вибір завдань захисту;

- розробку та впровадження правил реалізації заходів;

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

- вибір засобів забезпечення;

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

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

- визначення зон безпеки інформації;

- обґрунтування структури та технології функціонування систем;

- розробка правил та порядку контролю функціонування систем захисту;

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

Організаційні заходи щодо захисту інформації полягають у розробці й реалізації адміністративних та організаційно-технічних заходів при підготовці та експлуатації системи, методів відбору всіх працівників (рис. 1.3).

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

урядовими постановами, більшість проблем вирішується в самій організації в конкретних умовах.

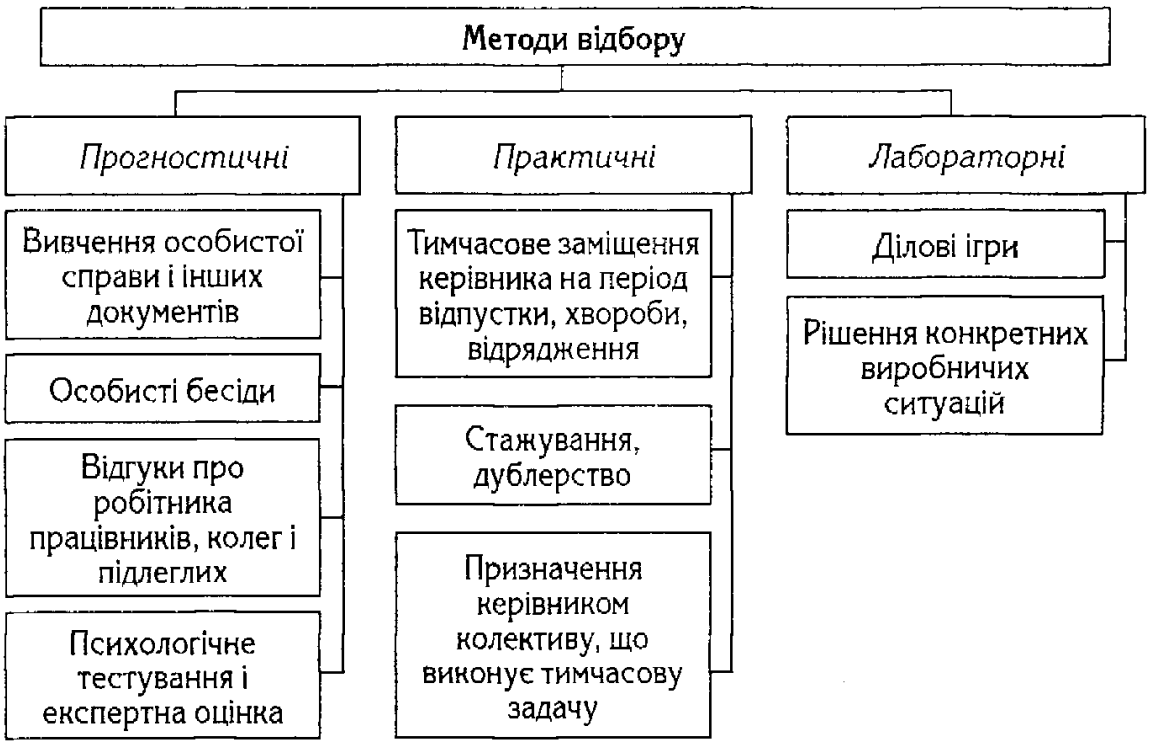


Рисунок 1.3 – Структура типового оперативного плану роботи з персоналом підприємства

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

Організаційні заходь щодо захисту інформації охоплюють наступні етапи:

- проектування;
- розробка;
- виготовлення;
- випробування;
- підготовки до експлуатації;

- експлуатації системи;

- виведення з експлуатації.

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

- проведення на необхідних ділянках робіт з режимом секретності;

- розробка посадових інструкцій щодо забезпечення режиму секретності відповідно до чинного законодавства;

- виділення в разі споживи окремих приміщень з охоронною сигналізацією та пропускною системою;

- розмежування завдань між виконавцями щодо випуску документації;

- присвоєння грифів секретності матеріалам та документації і збереження їх під охороною у виділених приміщеннях з урахуванням та контролем доступу виконавців;

- постійний контроль за дотриманням виконавцем режиму та відповідних інструкцій;

- встановлення і розподіл відповідальних осіб за витік інформації;

- інші заходи, що встановлюються в конкретних системах.

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

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

- встановити охоронну сигналізацію в межах контрольованої зони;

- створити контрольно-пропускну систему;

- перевірити схеми розміщення та місця установки об’єктів;

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

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

- провести навчання кадрів;

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

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

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

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

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

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

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

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

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

Інженерно-технічні заходи.

Інженерно-технічний захист – це сукупність спеціальних органів, технічних засобів та заходів для їхнього використання в інтересах захисту конфіденційної інформації (рис. 1.4).

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

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

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

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

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

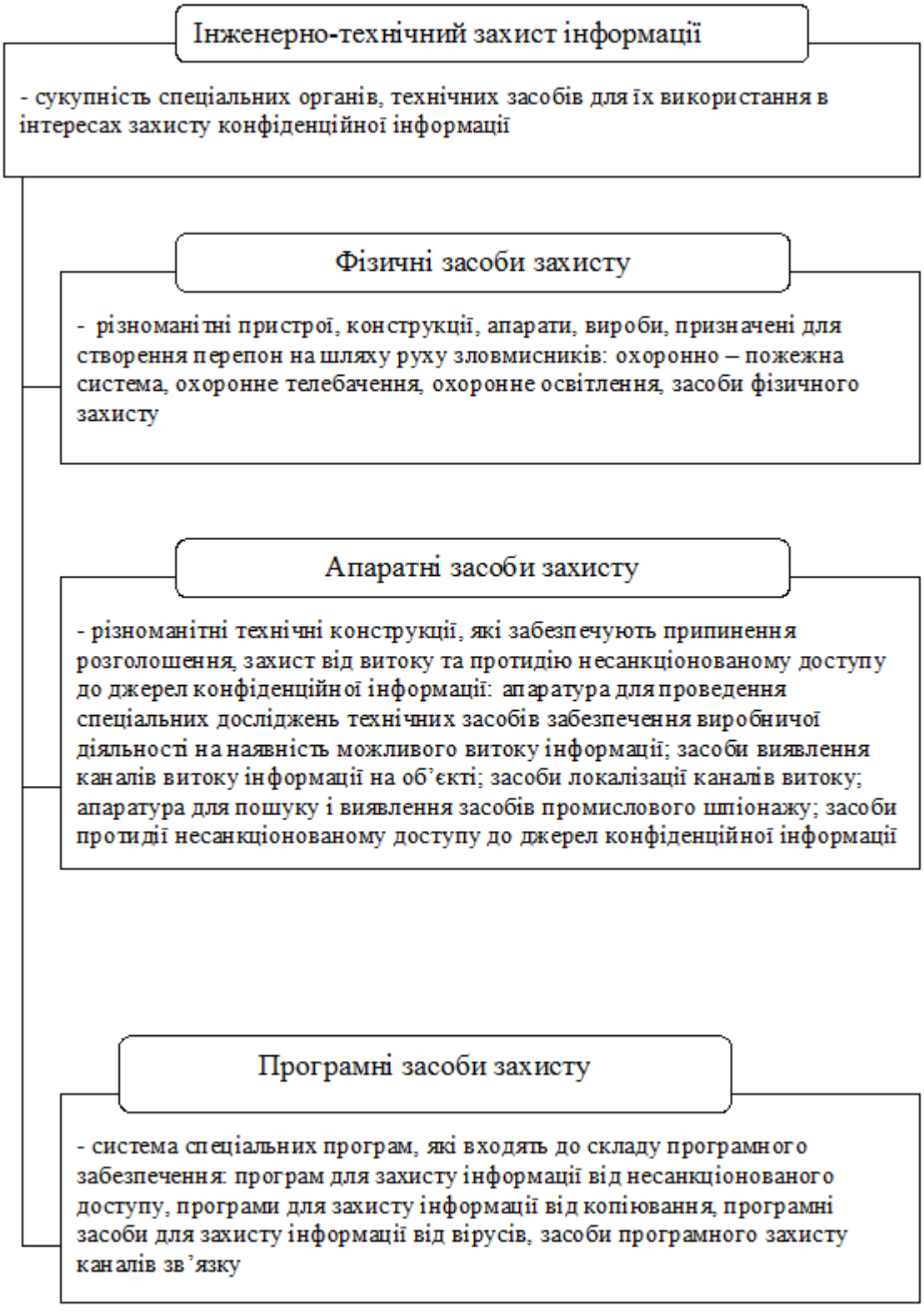


Рисунок 1.4 – Інженерно-технічний захист інформації

До апаратних засобів відносяться прилади, пристрої, та інші технічні рішення, які використовуються в інтересах захисту інформації. Основне завдання апаратних засобів – забезпечення стійкого захисту від

розголошення, витоку й несанкціонованого доступу через технічні засоби забезпечення діяльності організації (підприємства).

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

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

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

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

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

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

Для захисту комп'ютерної техніки застосовуємо: блок безперебійного живлення. Для того, щоб уникнути витоку інформації через допоміжні технічні засоби (сигнальних ліній мережі Ethernet, кабелів телефонного зв'язку, ліній мережі електроживлення, системи пожежної сигналізації), необхідно використовувати екрановані кабелі. У якості кабелів, по яких передається найбільш важлива інформація, доцільно використовувати екрановану виту пару.

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

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

Для фіксації факту розбиття віконного скла, використовуємо детектор розбиття скла. Для захисту периметру приміщення використаємо комбінований сповіщувач. У якості пожежних сповіщувачів використовуємо димовий сповіщувач. Для контролю доступу на об'єкт використовуємо замки на відбитки пальців. У якості системи передачі сповіщень використаємо систему, яка являє собою класичну систему централізованого спостереження. І може працювати як з кабельною системою, так і на радіочастотах. Тип зв'язку – односторонній.

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

У якості постійної авторизації користувачів у мережі використовуємо систему «Secure Card», яка дозволяє використовувати смарт-карти.

Підбір персоналу.

Вирішальна роль у системі збереження інформації з обмеженим доступом належить людському факторові. Незалежно від того, на скільки добрі розроблена та впроваджена комплексна система захисту інформації, вона в решті-решт ґрунтується на людській діяльності, у якій можливі помилки або свідомі дії, направлені на знищення інформації, або передачу її зацікавленим організаціям. Неможна, також, не відзначити, що сьогодні, як і завжди між різноманітними організаціями йде постійна боротьба за сфери своїх інтересів. І методи цієї боротьби різноманітні, починаючи від дипломатичної діяльності й закінчуючи збройними конфліктами. Велику актуальність сьогодні мають методи «психологічної війни». Відомо що завданнями психологічної війни є вплив на особу, як носія інформації та як основну ланку в системах управління різноманітного призначення. Потрібно розглянути систему чинників, що визначають кадрову політику підприємства (рис. 1.5).

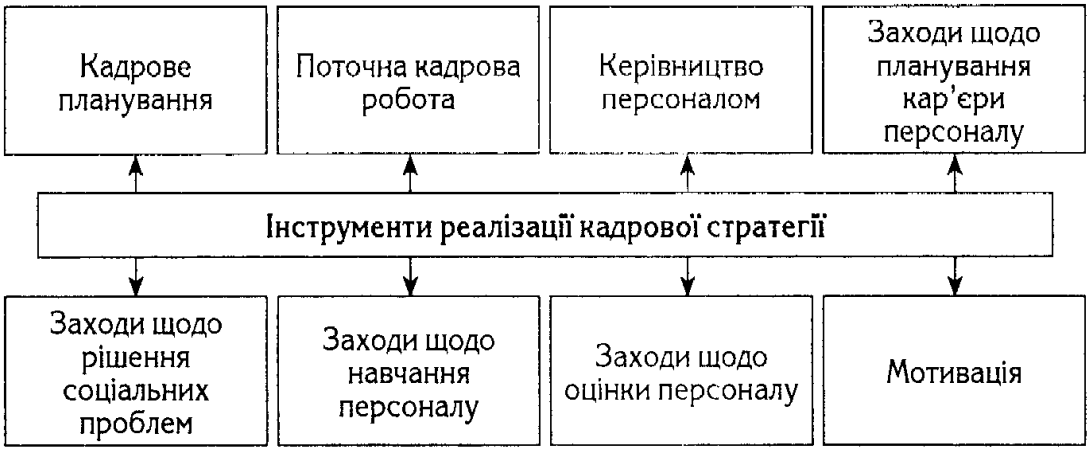


Рисунок 1.5 – Система чинників, що визначають кадрову політику підприємства

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

інформації, які можуть виникати в процесі діяльності персоналу установ і організацій.

Процедура відбору на вакантні посади працівників також є складною і її потрібно не оминати (рис. 1.6).

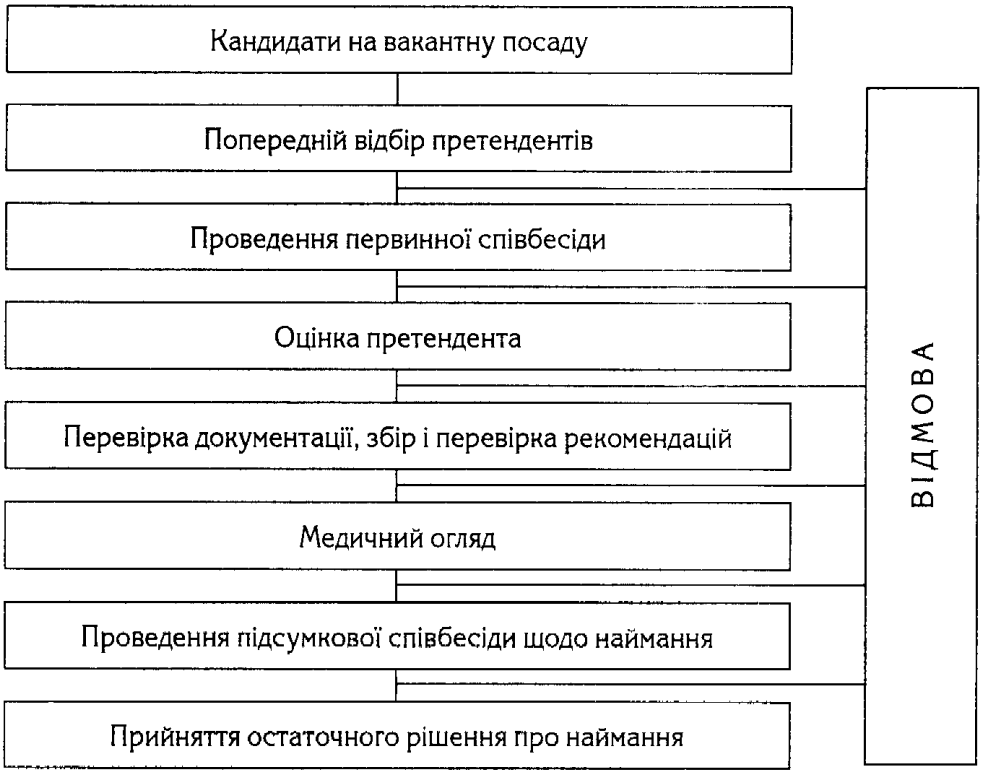


Рисунок 1.6 – Процедура відбору персоналу на вакантні посади

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

Методи впливу:

- підкуп;
- шантаж;
- погрози;
- одержання потрібної інформації при веденні звичайної розмови;
- обмін інформацією;
- переконання;

- використання психологічних методів;

- впровадження співробітником організації «своєї людини».

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

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

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

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

Ефективне планування персоналу ґрунтується на володінні такою інформацією:

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

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

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

- яким чином забезпечити умови для розвитку персоналу;

- яких витрат потребують дані кадрові заходи.

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

Якість трудових ресурсів підприємства тім вища, чим більша частка працівників, що забезпечують високу продуктивність праці, тобто персоналу високої кваліфікації. Тому в сучасних умовах значно зростає значимість та рівень вимог до підбору персоналу. В процесі відбору можливе навчання або перекваліфікація персоналу згідно схеми (рис. 1.7).

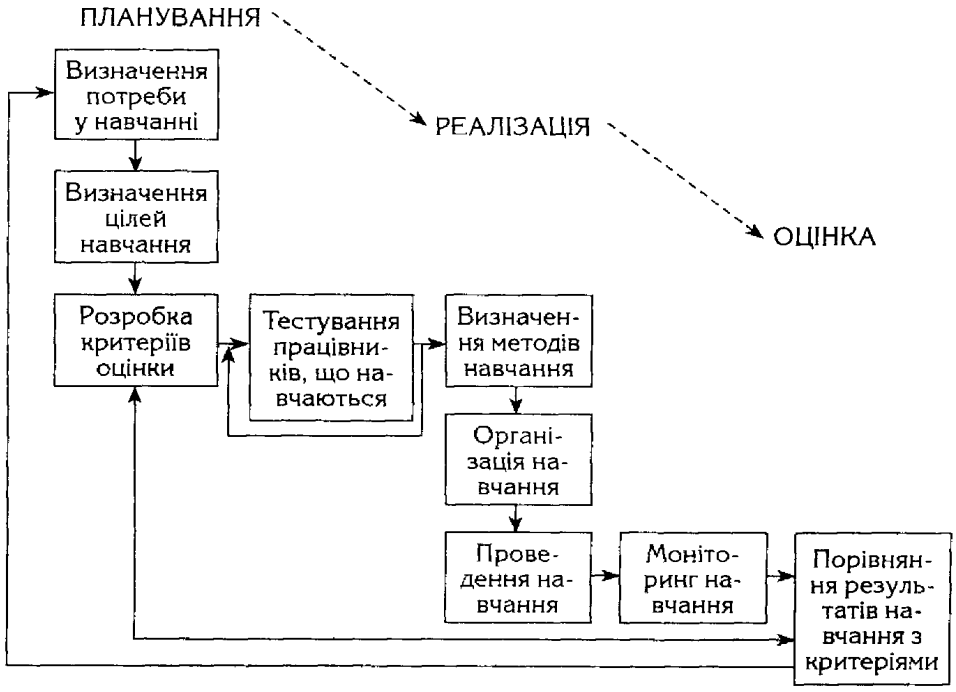


Рисунок 1.7 – Модель організації процесу навчання працівників

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

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

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

В процесі відбору можливо застосовувати тести та методики щодо виявлення професійних та інших якостей (табл. 1.2).

Таблиця 1.2

Види тестів, що застосовуються в процесі відбору персоналу

Найменування	Короткий опис
Методика «Оперативна пам'ять»	Для вивчення короткочасної пам'яті в тихнув випадках, коли вона несе основне функціональне навантаження
Методика «Пам'ять на числа»	Для оцінки зорової пам'яті, її обсягу і точності
Методика «Пам'ять на образи»	Для вивчення образної пам'яті
Методика «Червоно-чорна таблиця»	Для оцінки переключення уваги
Методика «Розміщення чисел»	Для оцінки довільної уваги
Методика «Компаси»	Для визначення просторових представлень
Методика «Складні аналогії»	Для оцінки логічного мислення
Методика Мюнстерберга	Для визначення вибірковості уваги

Продовження таблиці 1.2

Найменування	Короткий опис
Методика Равена	Для вивчення логічності мислення
Опитувальник К. Леонгарда	Для виявлення напрямків характеру
Тест-опитувальник Кеттела 16 PF. Форма А – 187 питань Форма З – 105 питань	Оцінка виразності 16 особистісних рис, запропонованих Кеттелом, як модель структури особистості (доброзичливість, інтелект, домінантність, безтурботність та ін.)
Особистий опитувальник (варіант тесту MMPI, 556 питань)	Оцінка відповідності психологічних особливостей особистості більш ніж за 60 видами діяльності
Ціннісні орієнтації М. Рокича	Визначає змістовну сторону спрямованості особистості і складає основу її відносин до навколишнього світу, до інших людей, до собі, ядро мотивації, основу життєвої концепції
Орієнтаційна анкета Б. Басса	Для визначення особистісної спрямованості
Методика В.П. Захарова (на основі опитувальника А.Л. Журавльова)	Визначення стилю керівництва трудовим колективом
Тест-опитувальник Т. Ліри (діагностика міжособистісних відносин)	Оцінка взаємодії особистості з оточенням, формування ідеальних образів «Я» і найближчого оточення. Виявлення внутрішніх конфліктів, пов'язаних з самореалізацією особистості
Тест-опитувальник К. Томаса (діагностика реагування на ситуації конфлікту)	Оцінка типу поведінки особистості в конфліктній ситуації по п'ятьох узагальнених типах: суперництво, запобігання конфлікту, компроміс, співробітництво, пристосування
Диференційно-діагностичний опитувальник Е.А. Клімова	Оцінка відповідності професійних схильностей особистості по п'ятьох основних сферах діяльності: людина – техніка; людина – знакова система; людина – художній образ; людина – природа
Колірний тест Люшера	Діагностика психофізичного стану особистості і розробка характеристик, що можуть бути використані для побудови психологічного портрету

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Оцінювання потенціалу працівника здійснюється при заміщенні їм вакантного робочого місця. Воно дає змогу визначити ступінь підготовки працівника до виконання саме того виду діяльності, яким він буде займатись, а також виявити рівень його потенційних можливостей для оцінювання

перспектив зростання. Ця процедура включає оцінювання професійних знань, умінь, виробничого досвіду, ділових та особистісних якостей, ціннісних орієнтацій, працездатності та загального рівня культури працівника, що претендує на зайняття вакантної чи посади робочого місця.

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

Атестація кадрів виступає як комплексне оцінювання, що враховує потенціал та індивідуальний внесок шкірного працівника в кінцевий результат.

Вихідними даними для оцінювання персоналу виступають:

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

Оцінювання персоналу на підприємствах відбувається шляхом залучення до оцінювання співробітника колег, підлеглих і навіть зовнішніх клієнтів. Багато підприємств починають проводити опитування клієнтів із метою оцінювання своїх представників.

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

2 ФУНКЦІОНАЛЬНІ МЕТОДИ БАГАТОКРИТЕРІАЛЬНОГО ОЦІНЮВАННЯ УІБЕРЗАХИСТУ

2.1 Багатокритеріальна оптимізація

Часто виникає завдання забезпечити оптимальність об'єкта проектування одночасно за кількома критеріями оптимальності $\phi_k(\mathbf{X}), k \in [1, s]$. Зазвичай ці критерії суперечливі і оптимізація по кожному з них призводить до різних значень вектора змінних параметрів *X*. Тому виділяється окремий клас задач багатокритеріальної оптимізації.

Якщо кожним критерієм поставити у відповідність гравця, то це завдання близьке до задачі теорії ігор *N* осіб в її кооперативному варіанті. Відмінність в тому, що множину *X*, взагалі кажучи, представимо у вигляді добутку *X*1 x ... x *Xn*, де *Xk* – множина стратегій *k*-го гравця. Ця обставина не дозволяє повністю звести розглянуту задачу до згаданої гри.

Будемо називати кожен з скалярних критеріїв оптимальності $\phi_k(\mathbf{X}), k \in [1, s]$ окремим критерієм оптимальності. Сукупність окремих критеріїв оптимальності

$$\mathbf{\Phi}(\mathbf{X}) = (\phi_1(\mathbf{X}), \phi_2(\mathbf{X}), \dots, \phi_s(\mathbf{X}))$$

будемо називати векторним критерієм оптимальності. Припустимо, що ставиться завдання мінімізації кожного з окремих критеріїв оптимальності ф1(*X*), ф2(*X*), ... , ф*s*(*X*) в одній і тій же області допустимих значень $D_{\mathbf{x}} \in R^{\mathrm{n}}$.

Вирішення задачі багатокритеріальної оптимізації в загальному випадку не є оптимальним ні для одного з окремих критеріїв, а виявляється деяким компромісом для вектора $\mathbf{\Phi}(\mathbf{X})$ в цілому.

Завдання багатокритеріальної оптимізації будемо записувати у вигляді:

$$\min_{\mathbf{X} \in \mathrm{D}_X} \mathbf{\Phi}(\mathbf{X}) = \mathbf{\Phi}(\mathbf{X}^*),$$

де D_x – множина допустимих значень вектора змінних параметрів *X*.

Перш, ніж застосувати той чи інший метод вирішення задачі багатокритеріальної оптимізації кіберзахисту, зазвичай проводять нормалізацію окремих критеріїв, приводячи всі окремі критерії

оптимальності $\phi_k(\mathbf{X}), k \in [1, s]$ до одного масштабу. Найчастіше при цьому використовують відносні відхилення окремих критеріїв від їх мінімальних значень:

$$\bar{\phi}_k(\mathbf{X}) = \frac{\phi_k(\mathbf{X}) - \phi_k^*}{\phi_k^{**} - \phi_k^*}, k \in [1, s],$$

де

$$\phi_k^* = \min_{\mathbf{X} \in D_X} \phi_k(\mathbf{X}), \qquad \phi_k^{**} = \max_{\mathbf{X} \in D_X} \phi_k(\mathbf{X}).$$

Збережемо за нормалізованими окремими критеріями оптимальності позначення $\phi_k(\mathbf{X}), k \in [1, s]$.

Введемо поняття простору критеріїв $\{\mathbf{\Phi}\}$. Простір критеріїв має розмірність (по числу окремих критеріїв) і утворюється ортогональними осями координат, уздовж яких відкладаються значення окремих критеріїв оптимальності кіберзахисту

$$\phi_k(\mathbf{X}), k \in [1, s].$$

Векторний критерій оптимальності $\mathbf{\Phi}(\mathbf{X})$ виконує відображення множини допустимих значень $D_X \in \{\mathbf{X}\}$ в деяку область $D_\Phi \in \{\mathbf{\Phi}\}$, де $\{\mathbf{X}\}$ – простір змінних параметрів.

Найбільшого поширення набула оптимізація за Парето.

Введемо на множині D_X співвідношення переваги. Будемо говорити, що вектор $\mathbf{X}^1 \in D_X$ кращий вектора $\mathbf{X}^2 \in D_X$ та писати $\mathbf{X}^1 \succ \mathbf{X}^2$, якщо рівностей і нерівностей $\phi_k(\mathbf{X}^1) \le \phi_k(\mathbf{X}^2), k \in [1, s]$ є хоча б одна сувора нерівність. Аналогічно на множини D_Φ введемо відношення домінування: будемо говорити, що векторний критерій оптимальності $\mathbf{\Phi}(\mathbf{X}^1) \in D_\Phi$ домінує над векторним критерієм оптимальності $\mathbf{\Phi}(\mathbf{X}^2) \in D_\Phi$ та писати $\mathbf{\Phi}(\mathbf{X}^1) \succ \mathbf{\Phi}(\mathbf{X}^2)$, якщо $\mathbf{X}^1 \succ \mathbf{X}^2$.

Введені відношення переваги і ставлення домінування є транзитивними. Виділимо з множини D_Φ підмножину $D_\Phi^* \in D_\Phi$ точок, для яких нема точок домінування.

Множина $D_X^* \in D_X$, відповідне D_Φ^* називається множиною Парето. Іншими словами множиною Парето можна визначити як множину, в якій значення будь-якого з окремих критеріїв оптимальності кіберзахисту можна поліпшити тільки за рахунок погіршення інших окремих критеріїв – будь-яке з рішень, яке належить множині Парето, не може бути покращено одночасно за всіма окремими критеріями.

Роль множини Парето при вирішенні задач багатокритеріальної оптимізації визначається наступною теоремою:

Теорема 1. Якщо для деяких вагових множників $\lambda_k, k \in [1, s]$ і вектора $\mathbf{X}^* \in D_X$ має місце рівність:

$$\sum_{k=1}^{s} \lambda_k \phi_k(\mathbf{X}^*) = \min_{\mathbf{x} \in D_X} \sum_{k=1}^{s} \lambda_k \phi_k(\mathbf{X}),$$

то вектор $\mathbf{X}^*$ оптимальний за Парето тобто $\mathbf{X}^* \in D_X$.

Теорема показує, що вибір певної точки з множини Парето еквівалентний і вказує на ваги для кожного з окремих критеріїв оптимальності. На цьому факті заснована велику кількість чисельних методів розв'язання задач багатокритеріальної оптимізації кіберзахисту.

Для вирішення задачі багатокритеріальної оптимізації широко використовуються методи, засновані на зведенні задачі багатокритеріальної оптимізації до задачі однокритеріальної оптимізації. Розглянемо кілька методів цієї групи.

2.2 Метод вагових множників

У методі вагових множників додатковою інформацією щодо інформації, заданої в постановці загальної задачі є інформація про відносну важливість окремих критеріїв. Метод вимагає, щоб ця інформація була

формалізована в значеннях вагових множники $\lambda_k, k \in [1, s]$. У цьому випадку в якості скалярного критерію використовується критерій:

$$\varphi(\mathbf{X}) = \sum_{k=1}^{s} \lambda_k \phi_k(\mathbf{X}), \lambda_k \geq 0, \sum_{k=1}^{s} \lambda_k = 1. \quad (2.1)$$

Тобто замість (2.1) вирішується багатовимірна задача умовної оптимізації зі скалярним критерієм оптимальності

$$\min_{\mathbf{X} \in D_x} \varphi(\mathbf{X}) = \min_{\mathbf{x} \in D_{xi}} \sum_{i=1}^{s} \lambda_i \phi_i(\mathbf{X}) = \varphi(\mathbf{X}^*).$$

Існують різні способи вибору вагових множники $\lambda_k, k \in [1, s]$. Одним з таких способів є призначення коефіцієнтів в залежності від відносної важливості відповідних окремих критеріїв оптимальності. Для того щоб при виборі вагових множників $\lambda_k, k \in [1, s]$ позбутися від впливу масштабів окремих критеріїв оптимальності, в методі вагових множників доцільно використовувати нормалізовані критерії.

Недоліком методу є те, що в разі неопуклої множини Парето не всі точки множини можуть бути досягнуті за допомогою зміни вагових множників.

2.3 Метод епсилон обмежень

У методі ε-обмежень в якості скалярного критерію оптимальності $\varphi(\mathbf{X})$ використовується найважливіший з окремих критеріїв оптимальності $\phi_p(\mathbf{X})$, а інші окремі критерії враховуються за допомогою обмежень типу нерівностей виду

$$\phi_k(\mathbf{X}) \leq \varepsilon_k, k \in [1, s], k \neq p.$$

Додатковою інформацією в методі ε-обмежень є інформація про номер найважливішого з окремих критеріїв, а також інформація про максимально допустимі значення окремих критеріїв.

Таким чином, в методі ε-обмежень замість загального завдання вирішується завдання умовної оптимізації зі скалярним критерієм оптимальності $\phi_p(\mathbf{X})$:

$$\min_{\mathbf{X}\in\tilde{D}} \varphi(\mathbf{X}) = \min_{\mathbf{X}\in\tilde{D}} \phi_p(\mathbf{X}) = \varphi(\mathbf{X}^*),$$

$$\tilde{D} = D_{\mathbf{X}} \cap D_p,\ D_p = \{\mathbf{X} \mid \phi_k(\mathbf{X}) \le \varepsilon_k,\ k\in[1, s],\ k\neq p\}.$$

Метод ε-обмежень в значній мірі вільний від зазначеного вище недоліку методу вагових множників в рази, коли множина не опукла. Недоліком методу ε-обмежень є труднощі вибору максимально допустимих значень окремих критеріїв

$$\varepsilon_k, k \in [1, s], k \neq p,$$

які гарантували б досяжність деякого рішення. Крім того, жорсткість обмежень $\phi_k(\mathbf{X}) \le \varepsilon_k, k \in [1, s], k \neq p$ далеко не завжди адекватна уявленням про найкращий спосіб вирішення кіберзахисту. Відзначимо також труднощі побудови в явному або неявному вигляді множин D_P.

2.4 Метод справедливого компромісу

Справедливим компромісом будемо називати такий компроміс, при якому відносний рівень зниження якості по одному або декільком окремим критеріям не перевищує відносного рівня підвищення якості по іншим окремим критеріям (менше або дорівнює).

Для формалізації поняття справедливого компромісу введемо відношення переваги на множині Парето. Нехай в множині Парето задачі дано дві точки $\mathbf{X}^1 \in D_X^*$ та $\mathbf{X}^2 \in D_X^*$ і значення всіх окремих критеріїв оптимальності в них

$$\phi_k(\mathbf{X}^1), \phi_k(\mathbf{X}^2), k \in [1, s].$$

Введемо міру відносного зміни (зниження – знак «мінус» або підвищення – знак «плюс») якості рішення по кожному з цих критеріїв:

$$\Delta\tilde{\phi}_k(\mathbf{X}^1, \mathbf{X}^2) = \frac{\Delta\phi_k(\mathbf{X}^1, \mathbf{X}^2)}{|\max\limits_{\mathbf{X} \in (\mathbf{X}^1, \mathbf{X}^2)} \phi_k(\mathbf{X})|}, k \in [1, s],$$

,

де $\Delta\phi_k(\mathbf{X}^1, \mathbf{X}^2) = \phi_k(\mathbf{X}^1) - \phi_k(\mathbf{X}^2)$ – абсолютні зміни значень окремих критеріїв оптимальності $\phi_k(\mathbf{X}), k \in [1, s]$ при переході від параметру $\mathbf{X}^1$ до параметру $\mathbf{X}^2$.

Обчислимо максимальне зниження якості рішення при переході від параметра $\mathbf{X}^1$ до параметру $\mathbf{X}^2$:

$$\Delta\tilde{\phi}_{\min}(\mathbf{X}^1, \mathbf{X}^2) = \min_{k \in [1, s]} \Delta\tilde{\phi}_k(\mathbf{X}^1, \mathbf{X}^2).$$

.

Аналогічно обчислимо максимальне підвищення якості рішення при переході від параметра $\mathbf{X}^1$ до параметру $\mathbf{X}^2$:

$$\Delta\tilde{\phi}_{\max}(\mathbf{X}^1, \mathbf{X}^2) = \max_{k \in [1, s]} \Delta\tilde{\phi}_k(\mathbf{X}^1, \mathbf{X}^2).$$

.

Будемо говорити, що параметр $\mathbf{X}^2$ перевершує параметр $\mathbf{X}^1$ та писати:

$$\mathbf{X}^2 \succ \mathbf{X}^1, \text{если } |\Delta\tilde{\phi}_{\max}(\mathbf{X}^1, \mathbf{X}^2)| > |\Delta\tilde{\phi}_{\min}(\mathbf{X}^1, \mathbf{X}^2)|.$$

.

З іншого боку, будемо говорити, що $\mathbf{X}^1$ параметр перевершує параметр $\mathbf{X}^2$ та будемо писати:

$$\mathbf{X}^1 \succ \mathbf{X}^2, \text{если } |\Delta\tilde{\phi}_{\max}(\mathbf{X}^1, \mathbf{X}^2)| \le |\Delta\tilde{\phi}_{\min}(\mathbf{X}^1, \mathbf{X}^2)|.$$

.

Таким чином, додатковою інформацією щодо кіберзахисту в методі справедливого компромісу є інформація про однакову важливість всіх окремих критеріїв $\phi_p(\mathbf{X})$, які характеризують методи захисту, а також інформацію про справедливий компроміс, формалізований ставленням переваги.

Оскільки метод справедливого компромісу використовує відносні зміни окремих критеріїв оптимальності щодо кіберзахисту, то цей метод інваріантний до масштабу виміру окремих критеріїв, тобто не потрібна їх нормалізація. Це є перевагою.

2.5 Метод наближення до ідеального рішення

Ідеальним рішенням задачі багатокритеріальної оптимізації називається вектор

$$\mathbf{\Phi}^* = (\phi_1^*, \phi_2^*, \dots, \phi_s^*),$$

де $\phi_k^* = \min_{\mathbf{X} \in D_X} \phi_k(\mathbf{X}), k \in [1, s]$ – значення окремого критерію оптимальності $\phi_k(\mathbf{X})$ в множині D_X. Нагадаємо, що вектори $\mathbf{X}_k^*, k \in [1, s]$ відповідають мінімуми відповідним критеріям оптимальності $\phi_k(\mathbf{X})$ взагалі кажучи, різні.

Введемо в розгляд скалярний критерій оптимальності кіберзахисту:

$$\varphi(\mathbf{X}) = \|\bar{\Phi}(\mathbf{X}) - \bar{\Phi}^*\|,$$

де $\|*\|$ – деяка векторна норма, наприклад, евклідова. Нормований векторний критерій оптимальності:

$$\bar{\Phi}(\mathbf{X}) = \left(\frac{\phi_1(\mathbf{X})}{\phi_1^*}, \frac{\phi_2(\mathbf{X})}{\phi_2^*}, \dots, \frac{\phi_s(\mathbf{X})}{\phi_s^*} \right)^T.$$

Нормоване ідеальне вирішення (одиничний $(s * 1)$ – вектор):

$$\bar{\mathbf{\Phi}}^* = \left(\frac{\phi_1^*}{\phi_1^*}, \frac{\phi_2^*}{\phi_2^*}, \dots, \frac{\phi_s^*}{\phi_s^*} \right)^T = (1, 1, \dots, 1).$$

У методі наближення до ідеального рішення замість загального завдання вирішується завдання умовної оптимізації зі скалярним критерієм оптимальності:

$$\min_{\mathbf{X} \in D_X} \varphi(\mathbf{X}) = \min_{\mathbf{X} \in D_X} \|\bar{\mathbf{\Phi}}(\mathbf{X}) - \bar{\mathbf{\Phi}}^*\| = \varphi(\mathbf{X}^*).$$

Зауважимо, що якщо $\|*\|$ – евклідова норма, то скалярний критерій оптимальності є квадратичною функцією компонент вектора $\mathbf{X}$. Тому якщо, додатково, множина D_X є опуклим, то поставлена задача являє собою задачу квадратичного програмування. Цей факт значно спрощує рішення поставленого завдання. Додатковою інформацією в методі наближення до ідеального рішенням є інформація, яка укладена в способі згортання векторного критерію оптимальності кіберзахисту:

$$\mathbf{\Phi}(\mathbf{X}) = (\phi_1(\mathbf{X}), \phi_2(\mathbf{X}), \dots, \phi_S(\mathbf{X})),$$

де в скалярний критерій $\varphi(\mathbf{X})$.

Оскільки метод наближення до ідеального рішення використовує нормовані окремі критерії оптимальності, цей метод інваріантний до масштабу виміру окремих критеріїв.

2.6 Евристична процедура вирішення задачі багатокритеріальної оптимізації

Для вибору єдиного рішення з області компромісів необхідно обґрунтувати аксіоматику і на її основі сформувати правило (схему компромісу) прийняття рішення щодо кіберзахисту. Для вирішення цього завдання потрібна додаткова інформація, яку можна отримати шляхом аналізу і формалізації особливостей мети системи.

Найважливішим результатом аналізу особливостей мети системи є встановлення взаємної важливості окремих критеріїв, що надає основу для вибору схеми компромісу. Залежно від особливостей системи і результатів такої формалізації можна виділити кілька ситуацій прийняття єдиного рішення в умовах багатокритеріальності:

Ситуація 1. Відомі кількісні значення вагових коефіцієнтів окремих критеріїв.

Ситуація 2. Кількісні значення вагових коефіцієнтів невідомі, але оптимізація має інформацію, що дозволяє ранжувати окремі критерії за важливістю.

Далі ранги перераховуються в вагові коефіцієнти за певними формулами.

Ситуація 3. Оптимізація не має ні кількісної, ні якісної інформації про коефіцієнти. У цьому випадку не слід віддавати перевагу якомусь критерію і логічно використовувати схему рівності або квазірівності критеріїв.

Нехай є множина $\{I\}$ варіантів вирішення завдання багатокритеріальної оптимізації кіберзахисту (множина Парето).

Якість кожного *i*-го варіанту оцінюється окремим критерієм $K_i=[K_{i1}, ..., K_{im}]^T$.

Потрібно визначити варіант $I^* \in \{I\}$, при якому забезпечуються задовільні значення всіх m показників K_i при $i=\overline{1,m}$ і найкращий компроміс між ними з урахуванням властивостей множини $\{I\}$ і апріорної інформації про співвідношення важливості показників. Розглядаються наступні випадки наявності апріорної інформації про важливість показників кіберзахисту:

- задані ваги показників;
- задана зіставна важливість показників;
- відсутня інформація про важливість показників.

Алгоритм, за допомогою якого відшукується рішення задачі вибору, враховує роль кожного окремого критерію з точки зору його впливу на властивості системи в цілому за допомогою вагових коефіцієнтів або коефіцієнтів важливості P_j, причому $\sum P_j^m = 1$. Функція корисності для кожного варіанта $i \in \{I\}$ задається у вигляді узагальненого адитивного критерію:

$$Q_i = \sum_{j=1}^{m} P_j q_{ij} ,$$

де $i=\overline{1,n}$ – номер варіанту системи; $j=\overline{1,m}$ – номер окремого критерію; $q_{ij} = \xi_{ij}\left[K_{ij}(x)\right]$ – функція корисності *j*-го окремого критерію в *i*-му варіанті системи і визначається з формули:

$$\xi_i(K_i) = \left(\frac{K_i - K_{i\text{НХ}}}{K_{i\text{НЛ}} - K_{i\text{НХ}}} \right)^{\alpha_i} \text{ при } \alpha_i = 1.$$

Визначення вагових коефіцієнтів стикається з серйозними труднощами і зазвичай зводиться до експертної оцінки. Для спрощення роботи експертів іноді пропонується вимагати від них тільки ранжирування критеріїв за важливістю. Далі ранги перераховуються в вагові коефіцієнти за певними формулами. У разі ж, коли багатокритеріальна оптимізація не має ні кількісної, ні якісної інформацією про коефіцієнти, логічно використовувати «рівність» критеріїв.

Пошук оптимального рішення проводиться за такою процедурою. Досліджується множина всіх варіантів {*I*} і проводиться оптимізація по кожному з показників K_{ij}. Отримані максимуми утворюють вектор *Z*1. Цей вектор містить «найкращі» значення окремих критеріїв з кіберзахисту по всьому множини варіантів {*I*} і використовується далі оптимізація для прийняття рішення. (аксіоматика прийняття оптимального рішення)

$$Z1 = \begin{vmatrix} \max\limits_{i\in\{I\}} K_{i1} \\ \dots \\ \max\limits_{i\in\{I\}} K_{im} \end{vmatrix}.$$

Проводиться оптимізація за сумарним критерієм Q_i. Найбільшим значенням $Q_l = \max\{Q_i\}$ відповідає варіант системи з параметром $l \in \{I\}$, де значення окремих критеріїв K_{lj} варіанту $l\left(j = \overline{1,m}\right)$ записується у вигляді вектора *Y*1, який представляє собою багатокритеріальне рішення рішення:

$$Y1 = \begin{vmatrix} K_{l1} \\ \dots \\ K_{lm} \end{vmatrix}.$$

Після оптимізації ставиться питання: «Чи всі показники кіберзахисту мають задовільні значення?» При відповіді на це питання використовується вектор *Z*1. У разі негативної відповіді оптимізація виділяє приватний критерій з номером *r*, який має найменш задовільне значення, а також вказує його величину K_r таку, що значення показника *r* можна вважати задовільним. Тобто відбуваються ітерації.

Структурна схема алгоритму процедури пошуку оптимального рішення задачі оптимізації кіберзахисту приведена в додатках.

3 ЕКОНОМІЧНІ АСПЕКТИ КІБЕРЗАХИСТУ

3.1 Аналіз доцільності вкладень на забезпечення захисту інформації

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

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

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

3.2 Моделювання бізнес-процесів на підприємстві

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

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

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

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

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

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

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

Бізнес-процес – це логічний, послідовний, взаємозалежний набір заходів, що залучає ресурси виробника, створює цінність і видає результат споживачеві. Серед основних причин, що спонукують організацію оптимізувати бізнес-процес, можна виділити необхідність зниження витрат або тривалості виробничого циклу, вимоги, пропоновані споживачами й державою, впровадження програм керування якістю, злиття компаній, внутрішньо- організаційні протиріччя й ін.

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

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

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

Для об'єкта й зв'язків характерний ряд параметрів, або, як прийнято говорити, атрибутів, що відбивають певні характеристики реального об'єкта. Склад атрибутів залежить від типу відображуваного за допомогою моделі реального об'єкта організації. Атрибутами можуть служити такі характеристики, як номер об'єкта, назва, опис, тривалість виконання (для функцій), вартість і ін. На практиці при створенні моделей організації опис атрибутів об'єктів моделі здійснюється за допомогою спеціальних

інструментальних засобів моделювання бізнес-процесів. Це дозволяє зробити з найпростішого «опису» бізнесу-процесу більш складну «модель», на основі якої роблять певні обчислення, здійснюють аналіз і оцінку процесу.

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

а) основні бізнес-процеси;

б) забезпечуючі бізнес-процеси;

в) бізнес-процеси розвитку;

г) бізнес-процеси керування.

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

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

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

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

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

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

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

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

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

- компонування нових, наприклад, будматеріалів та сумішей;

- виробництво продукції;

- перевірка та контроль за якістю продукції, що виготовляється;

- маркетинг;

- збут.

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

- матеріально-технічного забезпечення;

- управління інфраструктурою;

- управління персоналом;

- управління логістикою;

- юридичне забезпечення.

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

- стратегічне планування;

- бюджетування;

- менеджмент якості.

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

якістю продукції, що виготовляється. Вартість інформації, за допомогою якої смороду реалізуються, експерти оцінюють в 100 тис. грн.

3.3 Виявлення та оцінка ризиків втрати інформації

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

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

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

$$P_{\text{заг.}} = 1 - \prod_{i=1}^{n} (1 - p_i), \tag{3.1}$$

де p_i – ймовірність порушення інформаційної безпеки через i-й канал витоку; n – кількість каналів витоку.

Як видно з формули (3.1), щоб точно оцінити величину можливих збитків, необхідно правильно визначити область ризику втрати інформації через певний канал.

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

- негативний – програш, збиток;
- нульовий;
- позитивний – виграш, вигода, прибуток.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- збитки від ризику незалежні один від одного;

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

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

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

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

Аналіз ризику проводять у такій послідовності:

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

2) аналіз виявлених чинників;

3) оцінювання певного виду ризику за двома підходами:

4) визначення економічної доцільності (ефективності вкладених засобів);

5) розробка заходів щодо зниження ступеня ризику.

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

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

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

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

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

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

Другий аспект якісного аналізу ризику пов'язаний з виявленням впливу рішень, що приймаються за розумів невизначеності, на інтереси суб'єктів економічного життя. Без урахування інтересів (зацікавленості), без керування ними неможливі реальні якісні перетворення в соціально-економічному житті. Необхідно виявити: кому ризик корисний? чиїм інтересам відповідає?

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

Отже, ризикованій ситуації притаманні такі основні умови:

- наявність невизначеності;

- наявність альтернатив та необхідність вибору однієї з їх (відмова від вибору також є різновидністю вибору);

- зацікавленість у результатах;

- можливість оцінити наявні альтернативи прийняття рішення.

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

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

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

хто добре володіє обраною галуззю діяльності, на високому професійному рівні вирішує задачі, що постають, хто мислить не ординарно й у змозі творчо застосувати знання в реальній економічній і фінансовій ситуаціях.

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

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

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

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

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

Таблиця 3.1

Шкала ризику

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

Оцінка ризику виконується поетапно:

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

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

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

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

$$\max(a_i - b_i) \le 50,$$

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

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

Результати експертного опитування наведено в табл. 3.2.

Таблиця 3.2

Ймовірність втрати інформації через обрані канали витоку

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

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

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

тобто $P_{\text{заг.}} = 57$ %.

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

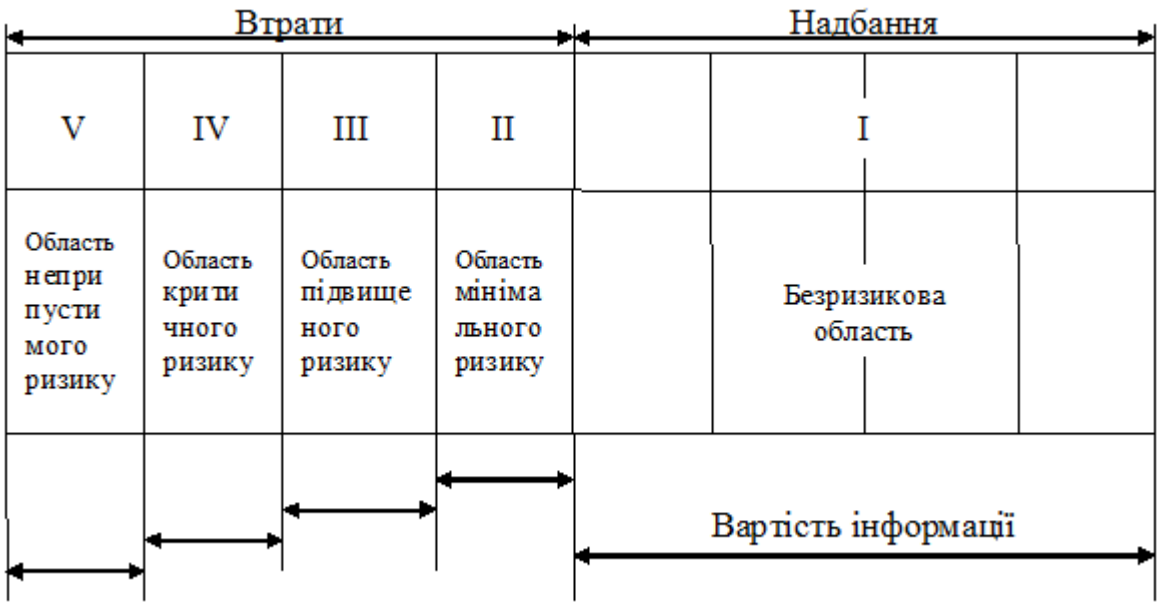


Рисунок 3.3 – Схема областей ризику

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

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

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

Для кількісної оцінки рівня втрат використовують коефіцієнт ризику *K*. Коефіцієнт ризику можна розраховувати як відношення розміру втрат до величини власних коштів підприємства:

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

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

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

Таблиця 3.3

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

$K = \frac{B_m}{BI}$	Рівень ризику
$K \leq 0{,}25$	Прийнятий
$0{,}25 < K \leq 0{,}5$	Припустимий
$0{,}5 < K \leq 0{,}75$	Критичний
$K > 0{,}75$	Катастрофічний

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

Таблиця 3.4

Типи поведінки керівництва підприємства залежно від коефіцієнту ризику

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

Розглянемо характеристику кожної з областей згідно рис. 3.3.

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

Область мінімального ризику (II) – характеризується розмірами втрат, які не перевищують чистого прибутку. Коефіцієнт ризику K=0-0,25.

Підприємство ризикує тім, що, у гіршому випадку, воно не одержить чистого прибутку. У кращому випадку – чистий прибуток буде менше його розрахункового значення.

Область підвищеного ризику (III) – характеризується втратами, що не перевищують валового доходу. Коефіцієнт ризику K=0,25-0,5. Підприємство ризикує тім, що, у гіршому випадку, воно не зможе виплатити заробітну плату своїм працівникам за виконану роботові, алепри цьому покриє матеріальні витрати, пов'язані з виробництвом продукції.

Область критичного ризику (IV) –характеризується втратами, величина яких не перевищує виторгу від реалізації продукції. Коефіцієнт ризику K=0,5-0,75.

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

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

Наступним етапом є проведення аналогічних процедур визначення коефіцієнта ризику й величини можливих втрат після застосування контрзаходів. Коефіцієнт визначає група експертів – фахівців у галузі захисту інформації для шкірного каналу витоку окремо. Після чого знаходять загальний показник за формулою (3.1).

ВИСНОВКИ

В роботі проведено дослідження багатокрітеріального підходу до вибору параметрів аналізу і протидії атакам, а також показані економічні аспекти інформаційної безпеки вибраної організації, в залежності від застосованого обладнання для захисту інформації.

Проведено огляд найбільш використовуваних методів вирішення задач багатокритеріальної функціональної оптимізації кіберзахисту. Велика кількість чисельних методів розв'язання задач багатокритеріальної оптимізації заснована на виборі певної точки з множини Парето та окремих критеріїв оптимальності. Для вибору одного кращого варіанту необхідно сформувати умовні переваги із залученням додаткової інформації від експертів і її подальшої обробки на основі теорії корисності. В роботі запропоновано використовувати евристичну процедуру уточнення рішення з залученням елементів програмування.

Також запропоновано розробити стратегію відбору персоналу на роботу з документацією, що має обмежений доступ, оцінені ризики бездіяльності керівництва щодо захисту інформації на об’єкті інформаційної діяльності.

Оцінені економічні ризики втрати конфіденційної інформації, запропоновані методи виявлення вразливостей, що можуть нести суттєві економічні наслідки для роботи та нормального функціонування підприємства в умовах кібератак.

ПЕРЕЛІК ЛІТЕРАТУРИ

1. Халяпин Д.К. Защита информации в телефонных линиях (каналах) связи // Охрана, № 4. - 2001. - С.24-55.

2. Гирин С.Н., Лысов А.В. Защита информации в телефонных сетях // Разведка, № 4. - 2001. - 52 с.

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

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

5. Виханский О.С. Стратегическое управление: [Учеб.]. – М.: Гардарика, 1998. – 296 с.

6. Основы управления персоналом: [Учеб. для вузов] / Б.М. Генкин, Г.А. Кононова, В.И. Кочетков и др.– М.: Высш. шк., 1996. – 383 с.

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

8. Управление персоналом организации: [Учеб.] / Под ред. А.Я. Кибанова. – М.: ИНФРА-М, 1997. – 512 с.

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

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

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

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

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

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

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

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

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

18. Ногин В.Д. Проблема сужения множества Парето. - СПб: Искусственный интеллект и принятие решений, 2008. – 310 с.

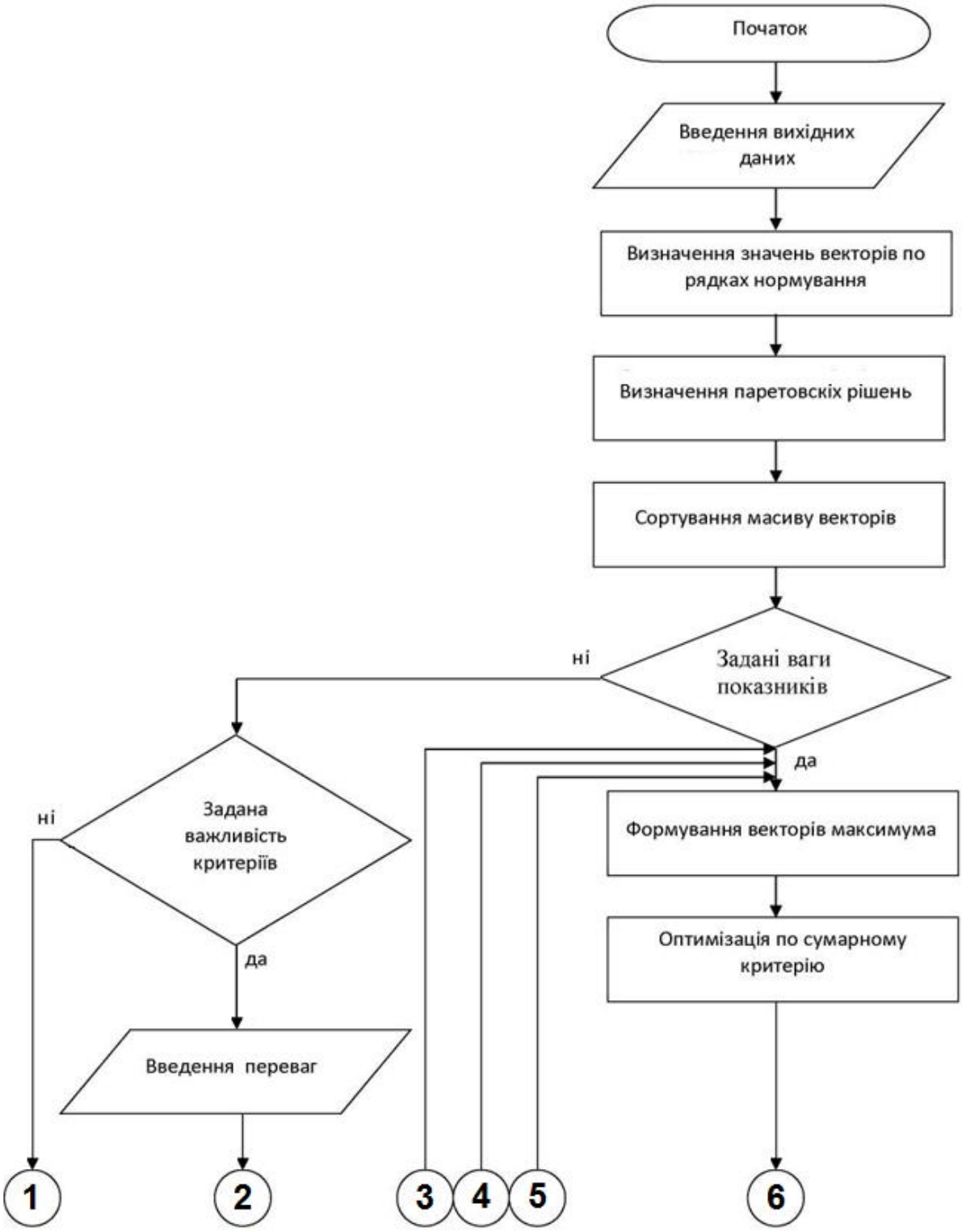
19. Безрук В.М. Методы многокритериальной оптимизации в задачах проектирования телекоммуникационных систем. - Львів: Компютерні технології друкарства, 2006. – 190 с.

20. Анализ перспектив применения математического аппарата многокритериального анализа к задаче автоматической маршрутизации в телекоммуникационных сетях [Електронний ресурс]. - 2010. - Режим доступу до ресурсу: http://www.pandia.ru/text/77/132/330.php.

ДОДАТКИ

Схема

алгоритму програми багатокритеріальної оптимізації



Продовження схеми

алгоритму програми багатокритеріальної оптимізації