МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Навчальний посібник

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою
«Системи, технології та математичні методи кібербезпеки»
спеціальності F5 Кібербезпека та захист інформації

Укладачі: С. О. Носок, М. В. Коломицев, І. В. Стьопочкіна

Електронне мережеве навчальне видання

Київ
КПІ ім. Ігоря Сікорського
2025

УДК 004.056

Укладачі: *Носок Світлана Олександрівна,* канд. техн. наук, доц.
Коломицев Михайло Володимирович, канд. техн. наук, доц.
Стьопочкіна Ірина Валеріївна, канд. техн. наук, доц.

Рецензент: *Сологуб Роман Ігорович*, директор міжнародної компанії з кібербезпеки ISSP, магістр зі спеціальності «Захист інформації в комп'ютерних системах та мережах»

Відповідальний редактор: *Литвинова Тетяна Василівна*, канд. техн. наук, доц.

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(протокол №1 від 28.08.2025 р.)
за поданням Вченої ради Фізико-технічного інституту
(протокол № 11 від 27.08.2025 р.)

Управління інформаційною безпекою [Електронний ресурс] : навч. посіб. для здобувачів ступеня бакалавра за освіт. програмою «Системи, технології та математичні методи кібербезпеки» спец. F5 Кібербезпека та захист інформації / КПІ ім. Ігоря Сікорського; уклад.: С. О.Носок, М. В. Коломицев, І. В. Стьопочкіна. – Електрон. текст. дані (1 файл: 870 Кбайт). – Київ: КПІ ім. Ігоря Сікорського, 2025. – 88 с.

Навчальний посібник з дисципліни «Управління інформаційною безпекою» глибше знайомить здобувачів освіти із забезпеченням інформаційної безпеки на підприємстві. Значна увага приділяється висвітленню питань, пов'язаних з технічним захистом інформації, приділено увагу «комерційній таємниці», методикам виявлення комерційної таємниці, питанням створення і функціонування служби інформаційної безпеки підприємства, розглянуто організаційно-адміністративні, соціально-психологічні аспекти забезпечення режиму комерційної таємниці, а також заходи захисту та протидії атакам соціальної інженерії.

УДК 004.056

Реєстр. № НП 25/26-020. Обсяг 3,67 авт. арк.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Берестейський, 37, м. Київ, 03056
https://kpi.ua
Свідоцтво про внесення до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.

ЗМІСТ

ВСТУП

Інформаційна безпека:

1) це захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес-ризику і отримання максимальних рентабельності інвестицій і бізнес-можливостей;
2) це збереження конфіденційності, цілісності та доступності інформації;
3) крім того, можуть враховуватися інші властивості, такі, як автентичність, спостережність, неспростовність та надійність.

Система управління інформаційною безпекою СУІБ (*information security management system,* ISMS) – частина загальної системи управління, яка призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Для процесів СУІБ застосована модель PDCA (плануй-виконуй-перевіряй-дій; *Plan-Do-Check-Act, PDCA*):

- Plan (планування) – фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів;
- Do (дія) – етап реалізації та впровадження відповідних заходів;
- Check (перевірка) – фаза оцінки ефективності та продуктивності СУІБ. Зазвичай виконується внутрішніми аудиторами;
- Act (поліпшення) – виконання превентивних і коригуючих дій

Побудова СУІБ дозволяє чітко визначити, як взаємопов’язані процеси та підсистеми інформаційної безпеки, хто за них відповідає, які фінансові та трудові ресурси необхідні для їх ефективного функціонування і т.д.

Забезпечення власної інформаційної безпеки на підприємствах, як правило, є невід'ємною частиною загальної системи управління, необхідної для досягнення статутних цілей та завдань та має велике значення не тільки для стратегічного розвитку підприємства і створення основного продукту, але і для окремих (іноді

допоміжних) напрямків діяльності та бізнес-процесів, таких як комерційні переговори і умови контрактів, цінова політика, тощо.

Поняття «безпека підприємництва» («безпека бізнесу») є новим у лексиконі української науки. Його виникнення обумовлено розвитком в Україні ринкових відносин, з появою яких набуває актуальності проблема безпеки підприємницької діяльності. Слід зазначити, що до цього термін «безпека» застосовувався переважно в військовій справі. В сучасній більш загальній трактовці «безпека» пов'язується з умовами існування певного об'єкта, які характеризуються відсутністю будь-яких реальних чи потенційних, внутрішніх чи зовнішніх загроз щодо життєдіяльності та нормального функціонування [1, 2, 3].

В зв'язку з цим безпеку підприємництва можна визначити як стан захищеності його правових, економічних та виробничих відносин, а також його матеріальних, інтелектуальних та інформаційних ресурсів від зовнішніх та внутрішніх загроз, що забезпечує стабільний розвиток та функціонування підприємства.

Очевидно, безпека підприємництва є однією із складових національної безпеки країни, питання безпеки підприємництва постає в умовах ринкової економіки і пов'язане перш за все із правом приватної власності. Остання обумовлює феномен свободи підприємництва: підприємець сам вирішує, що, в якій кількості, за якими технологіями буде виробляти, визначає ціну своєї продукції (послуг). З іншого боку, ринкова економіка визначає суверенітет споживача: з усіх видів виробленої продукції (послуг) споживач обере те, що йому найбільш до вподоби. Тобто ринкова економіка базується на принципі пріоритетів особистих інтересів своїх суб'єктів, кожен з них робить те, що йому видається найбільш вигідним, доцільним, навіть якщо це суперечить певним суспільним потребам. Обмеження ролі держави, як регулятора економічних відносин, має як негативні, так і позитивні сторони. Свобода підприємництва сприяє розвиненню ініціативи, підприємливості, закладає підвалини гнучкої креативної економіки, стимулює науково-технічний прогрес, забезпечує право на ризик і конкуренцію, що є противагою монополізації ринку, обмежує потенційно

можливі економічні ексцеси та негаразди ринку. В свою чергу ринкова конкуренція обумовлює можливість виникнення всіляких загроз, небезпечних конфліктів, ризику втрат і т.п. Звісно, що держава і в умовах ринку має певні важелі керування, насамперед правові, адміністративні, в разі необхідності і економічні. На жаль, їх застосування носить вельми загальний, глобальний характер, тоді як загрози і ризики навпаки, характеризуються адресністю та конкретною спрямованістю.

Кожне відомство, установа, підприємство, фірма вирішує питання своєї безпеки власними силами, в рамках наявного професійного кадрового ресурсу. Для вітчизняного бізнесу проблематика безпеки підприємництва характеризується властивостями:

- ринкова економіка, сформована на конкурентних принципах, є достатньо динамічною системою, примхи якої погано прогнозуються, що обумовлює можливість виникнення високих ризиків для суб'єктів ринкових відносин;
- законодавство, що регулює правові відносини в сфері підприємництва, зокрема в галузі безпеки підприємництва, є недосконалим та неповним.

В зв'язку з цим формування якоїсь єдиної типової системи безпеки підприємницької діяльності є питанням вкрай проблематичним, скоріш за все можливість типового розв'язку на поточний момент відсутня, і кожна фірма, організація, установа мають вирішувати проблеми своєї безпеки виключно у індивідуальному порядку відповідно до головних принципів та положень закону [4].

В цій ситуації базовою ланкою системи безпеки підприємництва слід вважати об'єкт підприємницької діяльності, тому далі головну увагу буде приділено саме питанням його захисту. Зазначимо, що захисту в цьому випадку підлягають:

- персонал об'єкту підприємницької діяльності;
- фінансові ресурси;
- матеріально-технічні засоби;

- інформаційні ресурси, що забезпечують підприємницьку діяльність чи є її наслідком;
- засоби та системи інформатизації (зокрема, системи обробки даних, телекомунікаційні системи);
- системи та засоби, що використовуються для охорони та захисту об'єкту підприємницької діяльності.

Реалізація заходів захисту за кожним з наведених вище об'єктів захисту є більш-меньш відомими задачами [1-3, 5]. Тому найважливішим є організація комплексного вирішення всіх цих задач, поєднання сукупності всіх захисних заходів у єдиному логічноув'язаному та цілеспрямованому процесі. Зазвичай ідейним базисом такого об'єднання є концепція безпеки підприємства (фірми, організації).

В посібнику значну увагу приділено визначенню і аналізу поняття "комерційна таємниця", методикам виявлення комерційної таємниці в загальному масиві інформації підприємства (його інформаційних ресурсах), питанням створення і функціонування служби інформаційної безпеки підприємства, певні організаційно-адміністративні і соціально-психологічні аспекти забезпечення режиму комерційної таємниці.

Додатково розглянуто підходи до управління інформаційною безпекою в умовах атак соціальної інженерії, які визначаються людським фактором. Надано характеристики основних атак, засоби та заходи протидії та відповідні підходи до виявлення соціальних інженерів в складі працівників підприємства. Особлива увага тут має бути приділена постановці тренінгів безпеки, які підвищують обізнаність та пильність в області соціальної інженерії, та дозволяють зробити людське середовище більш організованим та керованим в сенсі політик інформаційної безпеки.

1 ЗАГАЛЬНІ АСПЕКТИ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

1.1 Концепція безпеки підприємницької діяльності

В загальному розумінні *концепція* (від латинського *conception* – сприйняття) – це система взаємопов'язаних поглядів, уявлень щодо сутності певних явищ, процесів, проблем, зокрема на рівні їх теоретичного, наукового осмислення та сприйняття.

Концепція безпеки підприємницької діяльності – це система засадничих уявлень з проблем безпеки підприємництва на різних етапах та рівнях підприємницької діяльності, а також головні принципи, напрями і етапи реалізації заходів безпеки.

Концепція виражає систему поглядів на проблему безпеки фірми, підприємства, організації тощо (далі - фірми) на різних етапах і рівнях її діяльності, а також основні принципи, напрямки і етапи реалізації заходів безпеки. Закордонний і вітчизняний досвід забезпечення безпеки свідчить, що для боротьби з усією сукупністю злочинних і протиправних дій необхідна струнка й цілеспрямована організація процесу протидії. Причому в організації цього процесу повинні брати участь професійні фахівці, адміністрація фірми, співробітники й користувачі, що і визначає підвищену значимість організаційної сторони питання.

Накопичений досвід також показує, що:

- забезпечення безпеки не може бути одноразовим актом. Це безперервний процес, що полягає в обґрунтуванні й реалізації найбільш раціональних форм, методів, способів і шляхів створення, удосконалювання й розвитку системи безпеки, безперервному керуванні нею, контролі, виявленні її вузьких місць і потенційних загроз фірмі;
- безпека може бути забезпечена лише при комплексному використанні всього арсеналу засобів захисту й протидії у всіх структурних елементах виробничої системи й на всіх етапах технологічного циклу. Найбільший

ефект досягається тоді, коли всі використовувані засоби, методи й заходи поєднуються в єдиний цілісний механізм – систему безпеки фірми (СБФ);

- ніяка СБФ не може забезпечити необхідний рівень безпеки без належної підготовки персоналу фірми й користувачів і дотримання ними всіх установлених правил, спрямованих на забезпечення безпеки.

З урахуванням накопиченого досвіду систему безпеки фірми можна визначити як організовану сукупність спеціальних органів, засобів, методів і заходів, що забезпечують безпеку підприємницької діяльності від внутрішніх і зовнішніх загроз (рисунок 1.1).

Організація й функціонування системи безпеки повинні здійснюватися на основі наступних принципів.

1. Комплексність:

- забезпечення безпеки персоналу, матеріальних і фінансових ресурсів від можливих загроз всіма доступними законними засобами, методами й заходами;
- забезпечення безпеки інформаційних ресурсів протягом усього їхнього життєвого циклу, на всіх технологічних етапах їхньої обробки (перетворення) і використання, у всіх режимах функціонування;
- здатність системи до розвитку й удосконалювання відповідно до змін умов функціонування фірми.

2. Своєчасність – упереджуючий характер заходів забезпечення безпеки. Своєчасність припускає постановку завдань по комплексній безпеці на ранніх стадіях розробки системи безпеки на основі аналізу й прогнозування обстановки, загроз безпеці, а також розробку ефективних заходів попередження зазіхань на законні інтереси.

3. Безперервність – вважається, що зловмисники тільки й шукають можливість, якби обійти захисні заходи, прибігаючи для цього до легальних і нелегальних методів.

4. Активність. Захищати інтереси фірми необхідно з достатнім ступенем

наполегливості, широко використовуючи маневр силами й засобами забезпечення безпеки й нестандартних заходів захисту.

5. Законність. Припускає розробку системи безпеки на основі законодавства в області підприємницької діяльності, інформатизації й захисту інформації, приватної охоронної діяльності, а також інших нормативних актів по безпеці, затверджених органами державного керування в межах їхньої компетенції, із застосуванням всіх дозволених методів виявлення й припинення правопорушень.

6. Обґрунтованість. Запропоновані заходи й засоби захисту повинні реалізуватися на сучасному рівні розвитку науки й техніки, бути обґрунтованими з погляду заданого рівня безпеки й відповідати встановленим вимогам і нормам.

7. Економічна доцільність і порівнянність можливого збитку й витрат на забезпечення безпеки (критерій "ефективність - вартість").

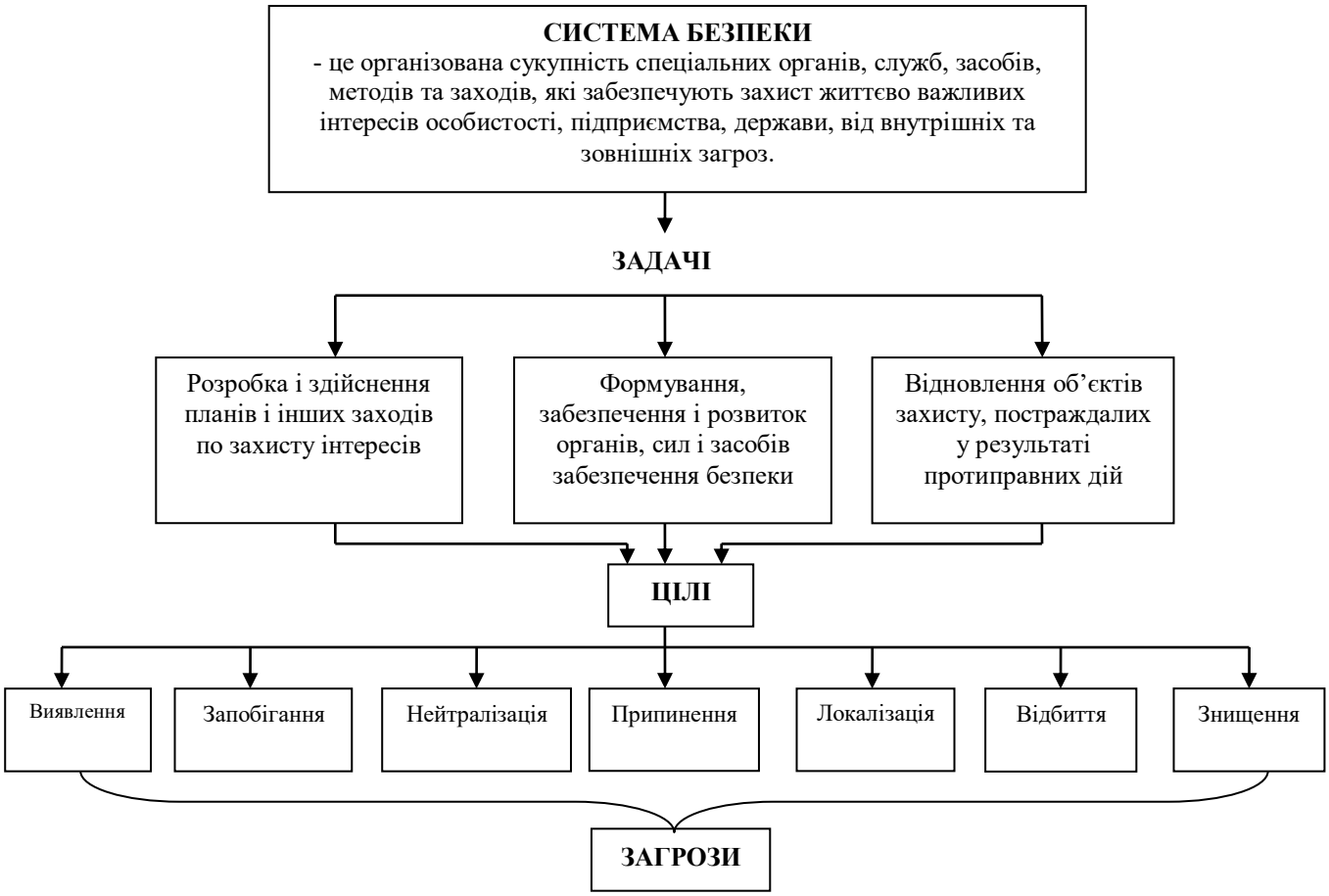


Рисунок 1.1 – Безпека підприємницької діяльності від внутрішніх і зовнішніх загроз

8. Спеціалізація. Передбачається залучення до розробки й впровадження заходів і засобів захисту спеціалізованих організацій, найбільш підготовлених до конкретного виду діяльності по забезпеченню безпеки, які мають досвід практичної роботи й державну ліцензію на право надання послуг у цій області. Експлуатація технічних засобів і реалізація заходів безпеки повинні здійснюватися професійно підготовленими фахівцями служби безпеки, її функціональних й обслуговуючих підрозділів.

9. Взаємодія й координація. Припускає здійснення заходів забезпечення безпеки на основі чіткої взаємодії всіх зацікавлених підрозділів і служб, сторонніх спеціалізованих організацій у цій області, координацію їхніх зусиль для досягнення поставлених ланцюгів, а також інтеграцію діяльності з органами державного керування й правоохоронних органів.

10. Вдосконалення. Передбачає вдосконалення заходів і засобів захисту на основі власного досвіду, появи нових технічних засобів з урахуванням змін у методах і засобах розвідки й промислового шпигунства, нормативно-технічних вимог, накопиченого вітчизняного й закордонного досвіду.

11. Централізація керування. Припускає самостійне функціонування системи безпеки по єдиних організаційних, функціональних і методологічних принципах із централізованим керуванням діяльністю системи безпеки.

Особливу увагу необхідно приділяти *принципу комплексності*. Для забезпечення безпеки у всьому різноманітті структурних елементів фірми, при безлічі загроз і способів несанкціонованого доступу повинні застосовуватися всі види й форми захисту й протидії в повному обсязі. Неприпустимо застосовувати окремі форми або технічні засоби.

Під комплексною безпекою варто розуміти повне охоплення об'єктів захисту всією сукупністю форм протидії й захисту (охорона, режим, кадри, документи тощо) на основі правових, організаційних й інженерно-технічних заходів. З урахуванням цього визначення комплексної безпеки можна представити у вигляді тривимірної моделі (рисунок 1.2).

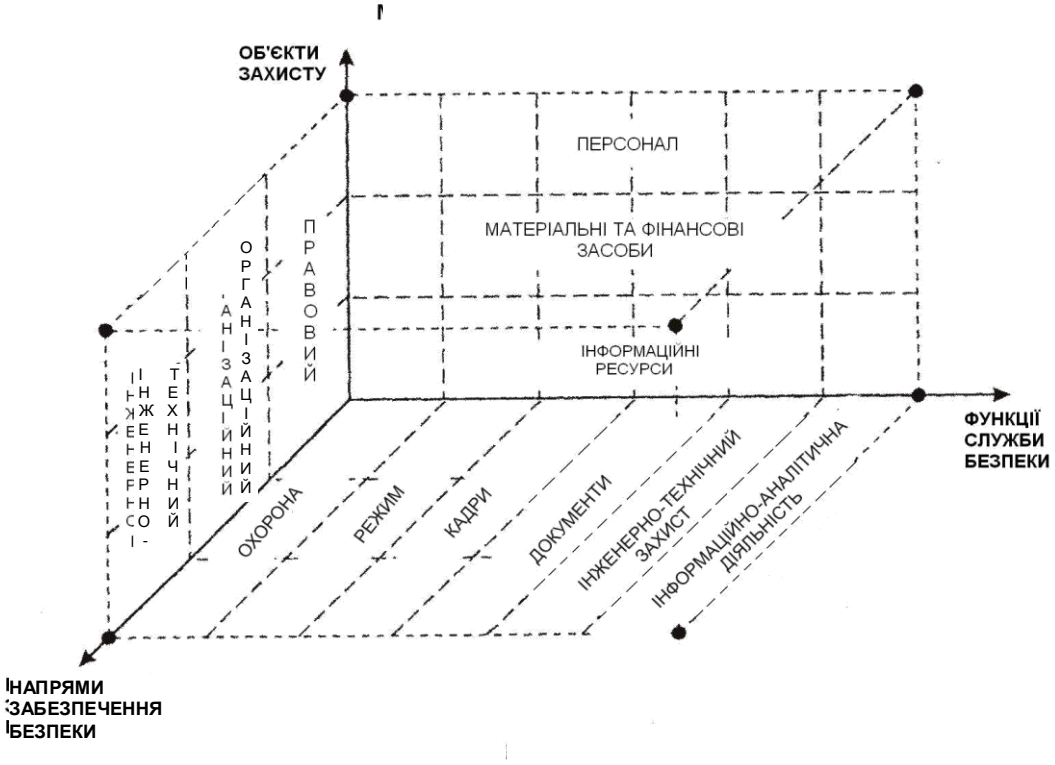


Рисунок 1.2 – Модель комплексної безпеки

1.2 Мета й завдання системи безпеки

Основною метою системи безпеки фірми є запобігання збитків в її діяльності за рахунок розголошення, витоку й несанкціонованого доступу до джерел конфіденційної інформації; розкрадання фінансових і матеріально-технічних засобів; знищення майна й цінностей; порушення роботи технічних засобів забезпечення виробничої діяльності, включаючи й засоби інформатизації, а також запобігання збитків персоналу фірми.

Метою системи безпеки є:

- захист прав фірми, її структурних підрозділів і співробітників;
- збереження й ефективне використання фінансових, матеріальних й інформаційних ресурсів;
- підвищення іміджу й росту прибутків за рахунок забезпечення якості послуг і безпеки клієнтів.

Завданнями системи безпеки є:

- своєчасне виявлення й усунення загроз персоналу й ресурсам; причин й умов, що сприяють нанесенню фінансового, матеріального й морального збитку інтересам фірми, порушенню її нормального функціонування й розвитку;
- віднесення інформації до категорії обмеженого доступу (службовій і комерційній таємницям, іншої конфіденційної інформації, що підлягає захисту від неправомірного використання) і інших ресурсів - до різних рівнів ураженості (небезпеки) і підлягаючих збереженню;
- створення механізму й умов оперативного реагування на загрози безпеки й прояву негативних тенденцій у функціонуванні фірми;
- ефективне припинення зазіхань на ресурси й загроз персоналу на основі комплексного підходу до безпеки;
- створення умов для максимально можливого відшкодування й локалізації завдаваємого збитку неправомірними діями фізичних й юридичних осіб, для ослаблення негативного впливу наслідків порушення безпеки на досягнення стратегічних цілей.

1.3 Об'єкти захисту

До об'єктів, що підлягають захисту від потенційних загроз і протиправних зазіхань, відносяться:

- персонал (керівники, виробничий персонал, що володіє інформацією, що становить комерційну таємницю, працівники зовнішніх служб й інший "вразливий" персонал);
- фінансові засоби (валюта, коштовності, фінансові документи й ін.);
- матеріальні засоби (будинки, спорудження, сховища, устаткування, транспорт і т.д.);

- інформаційні ресурси з обмеженим доступом, що становлять службову й комерційну таємницю, а також інша конфіденційна інформація на паперовій, магнітній, оптичній основі, інформаційні масиви й бази даних, програмне забезпечення, інформативні фізичні поля різного характеру;
- засоби й системи інформатизації (автоматизовані системи й обчислювальні мережі різного рівня й призначення, лінії телеграфного, телефонного, факсимільного, пейджингового радіо- і космічного зв'язку, технічні засоби передачі інформації, допоміжні засоби й системи);
- технічні засоби й системи охорони й захисту матеріальних й інформаційних ресурсів.

1.4 Основні види загроз

Погіршення криміногенного стану в країні, посилення міжрегіональних зв'язків організованих злочинних груп, ріст їхньої фінансової мощі й технічної оснащеності дає підставу думати, що тенденція до ускладнення оперативної обстановки навколо комерційних підприємств у найближчому майбутньому збережеться. Звідси випливає необхідність визначення й прогнозування можливих загроз як основи для обґрунтування, вибору й реалізації адекватних захисних заходів. Загальна характеристика загроз безпеки фірми наведена на рисунку 1.3.

Рисунок 1.3 – Загальна характеристика загроз безпеки фірми

У загальному плані до загроз безпеки особистості (персоналу) відносяться:

- убивства, супроводжувані насильством, знущаннями й катуваннями;
- викрадення й загрози викрадення співробітників, членів їхніх родин і близьких родичів;
- психологічний терор, загрози, залякування, шантаж, вимагання;
- грабежі з метою заволодіння коштами, цінностями, документами, майном.

На рисунку 1.4 наведено концептуальну модель безпеки особистості, що включає і загрози, і об'єкти загроз, і джерела загроз безпеки особистості, а також інші характеристики загроз і засоби забезпечення особистої безпеки.

Злочинні зазіхання відносно матеріальних цінностей (продукції), приміщень (у тому числі й житлових), будинків й інших ресурсів проявляються у вигляді:

- ознайомлення з конструкцією, дизайном, виконанням;
- підробки продукції;

- крадіжок;
- промислового шпигунства;
- шахрайства;
- знищення різними шляхами (вибухи, підпали, обстріли й та ін).

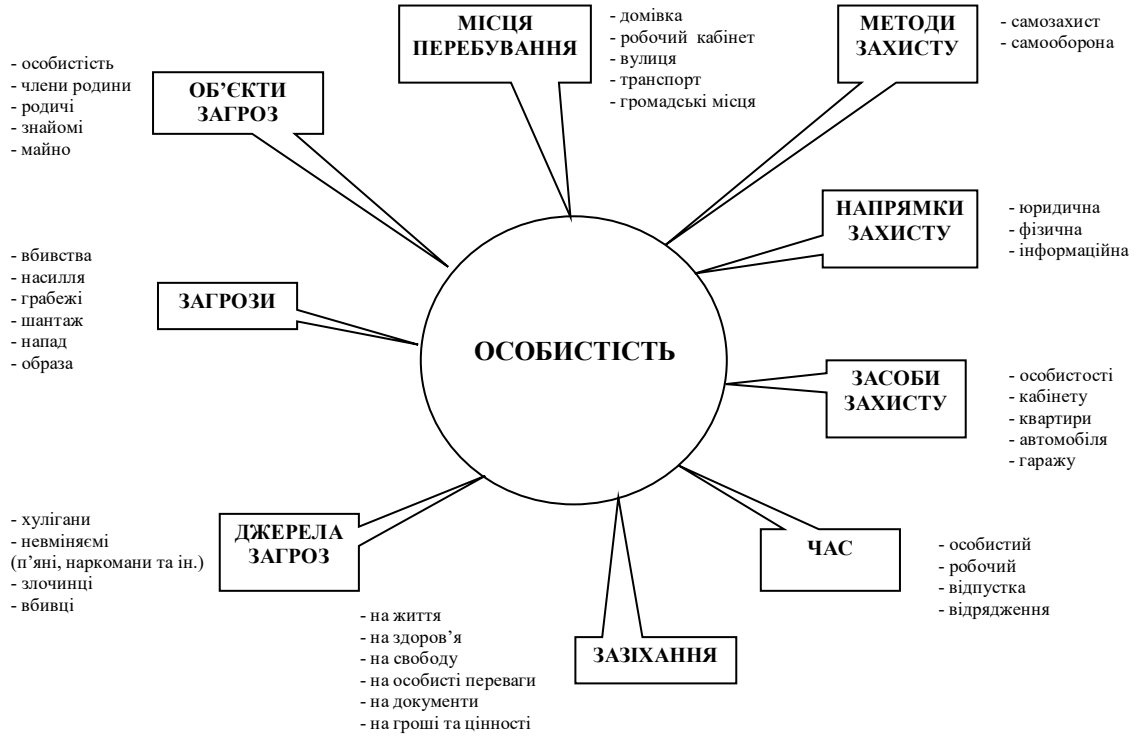


Рисунок 1.4 - Концептуальна модель безпеки особистості

На рисунку 1.5 наведено концептуальну модель безпеки продукції.

Мета протиправних акцій відносно продукції:

- відвертий терор;
- нанесення серйозного морального й матеріального збитку;
- зрив на тривалий час нормального функціонування;
- вимагання значних сум грошей або яких-небудь пільг перед особою терористичної загрози.

Стосовно інформації й інформаційних ресурсів проявляються наступні загрози:

- цілісності;

- конфіденційності;
- повноти;
- доступності.

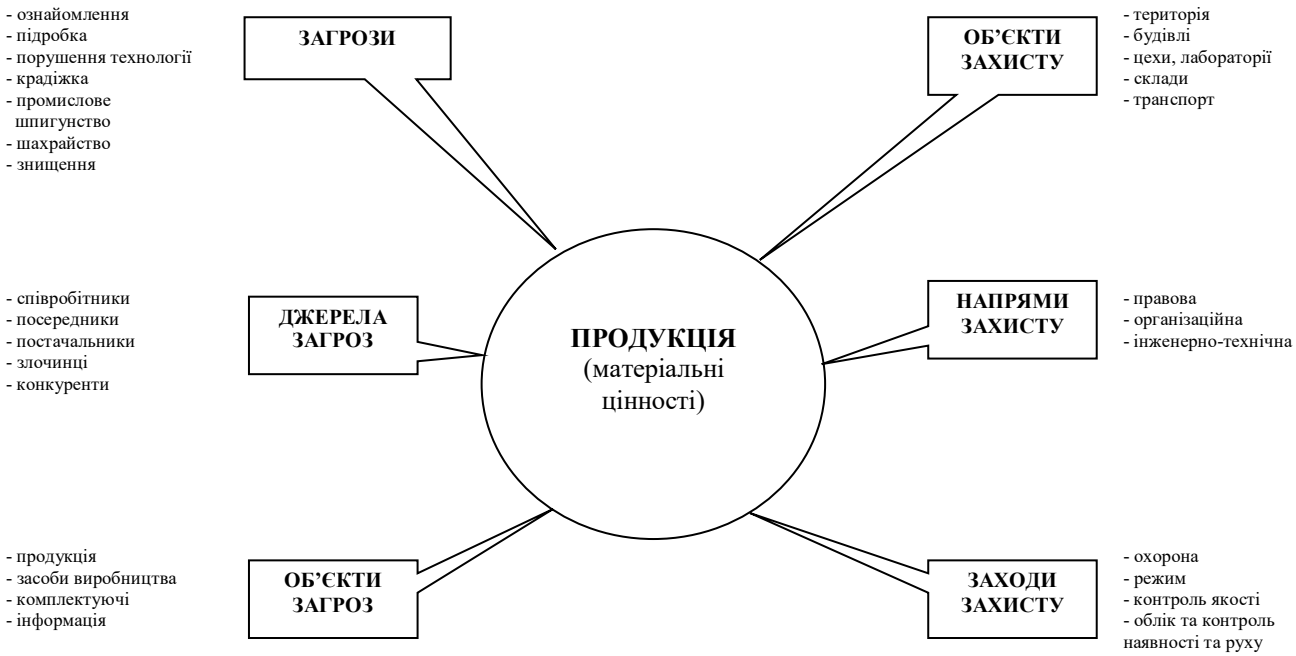


Рисунок 1.5 - Концептуальна модель безпеки продукції

На рисунку 1.6 наведено концептуальну модель безпеки інформації, яка надає уявлення про загрози і їхні джерела, про злочинні цілі, а також про шляхи забезпечення безпеки інформації.

Здійснення загроз інформаційним ресурсам може бути зроблено:

- через наявні агентурні джерела в органах державного управління і комерційних структурах, що мають можливість одержання конфіденційної інформації (суди, податкові органи, комерційні банки та ін.);
- шляхом підкупу осіб, що безпосередньо працюють у фірмі або структурах, безпосередньо пов'язаних з її діяльністю;
- шляхом перехоплення інформації, що циркулює в засобах і системах зв'язку й обчислювальній техніці за допомогою технічних засобів розвідки й знімання інформації;

- шляхом підслуховування конфіденційних переговорів й інших способів несанкціонованого доступу до джерел конфіденційної інформації.

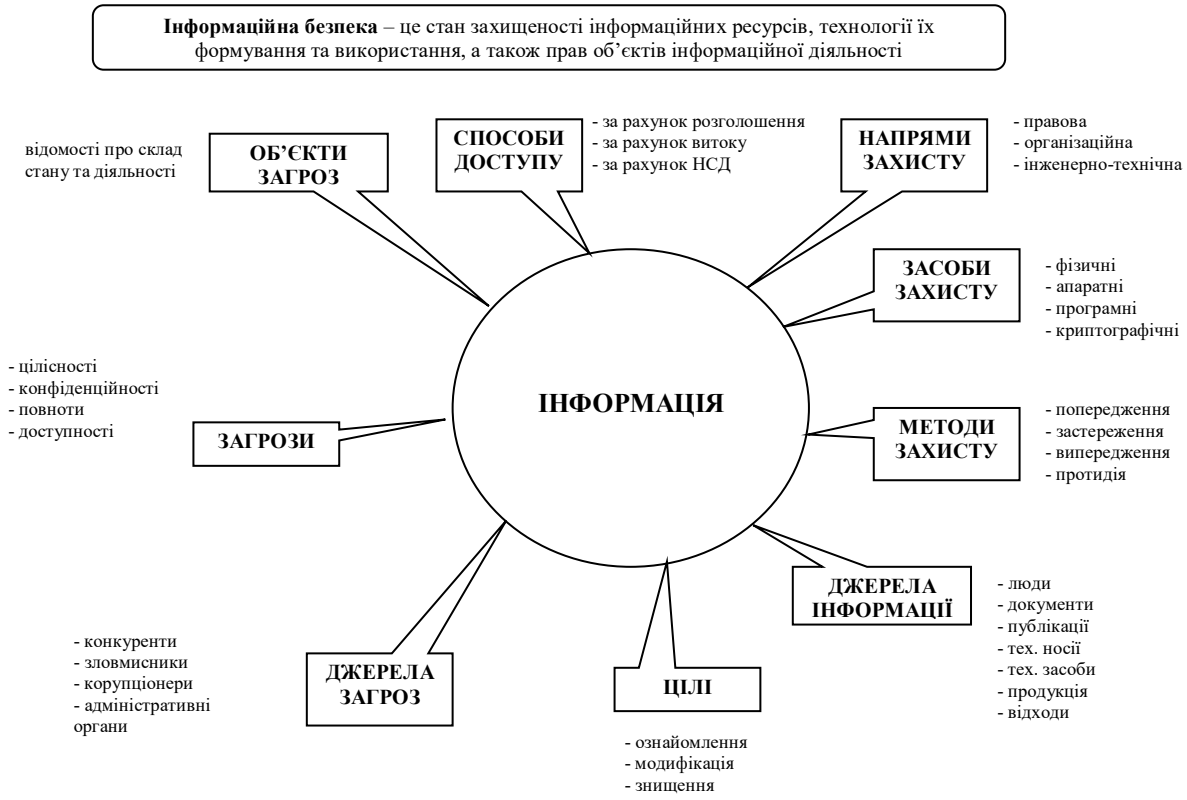


Рисунок 1.6 - Концептуальна модель безпеки інформації

2 СИСТЕМА БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

2.1 Склад і структура системи безпеки

Організаційна структура системи безпеки може бути найрізноманітнішою й залежить від виду конкретного підприємства (банк, фірма), його масштабів, форм власності й т.п. Створювати її необхідно усвідомлено й раціонально, максимально використовуючи досвід фахівців у сфері безпеки бізнесу.

Структура, чисельність і склад СБФ визначаються реальними потребами фірми й ступенем конфіденційності її інформації. Залежно від масштабів і потужності організації її безпека й захист інформації можуть бути забезпечені по-різному: від абонементного обслуговування силами приватних охоронних і детективних структур до розгортання повномасштабної власної служби й системи безпеки з розвиненою структурою й штатною чисельністю.

Опорними пунктами такої структури є:

1) відповідальний керівник системи;
2) рада по безпеці фірми;
3) служба безпеки фірми в складі відділів: охорони, режиму, кадрів, документів із КТ, інженерно-технічних засобів безпеки й контр-розвідувальної й інформаційно-аналітичної діяльності;
4) лінійні підрозділи фірми, що активно беруть участь у забезпеченні економічної безпеки (кадрового, фінансового, планового, юридичного, маркетингу й ін.).

Рішення про створення системи безпеки приймається керівництвом фірми відповідно до її уставу.

Відповідальний керівник системи безпеки фірми – це або сам директор, або один з його заступників. Він повинен добре знати, що підлягає захисту й охороні й мати певні пізнання в області безпеки.

Рада по безпеці фірми – це колегіальний орган при керівнику системи безпеки. Рада виконує консультативні функції, а його пропозиції носять рекомендаційний характер. Всі члени ради призначаються директором із числа провідних спеціалістів, що мають досвід роботи або зацікавлених у забезпеченні безпеки.

Основними завданнями ради є:

- оцінка й вироблення основних напрямків діяльності фірми по забезпеченню економічної безпеки;
- розробка перспективних програм удосконалювання системи безпеки;
- розробка пропозицій про зміст і характер взаємодії із правоохоронними органами, органами місцевого управління, із сусідніми СБФ, а також з партнерами, замовниками, споживачами продукції з метою дотримання конфіденційності, установлення й підтримки інших заходів безпеки;
- розгляд спільних планів підрозділів фірми по забезпеченню безпеки;
- розгляд проектів рішень про склад, стан і діяльність системи безпеки по звітних періодах.

Служба безпеки фірми – самостійний структурний підрозділ. Вона вирішує завдання по безпосередньому забезпеченню захисту життєво важливих інтересів фірми в умовах комерційного й виробничого ризику, конкурентної боротьби.

До складу служби безпеки фірми входять:

- відділ охорони;
- відділ режиму;
- відділ кадрів;
- відділ спеціального документообігу (відділ документів із грифом "комерційна таємниця");
- відділ контррозвідки й інформаційно-аналітичної діяльності.

Приблизну структуру системи безпеки фірми наведено на рисунку 2.1.

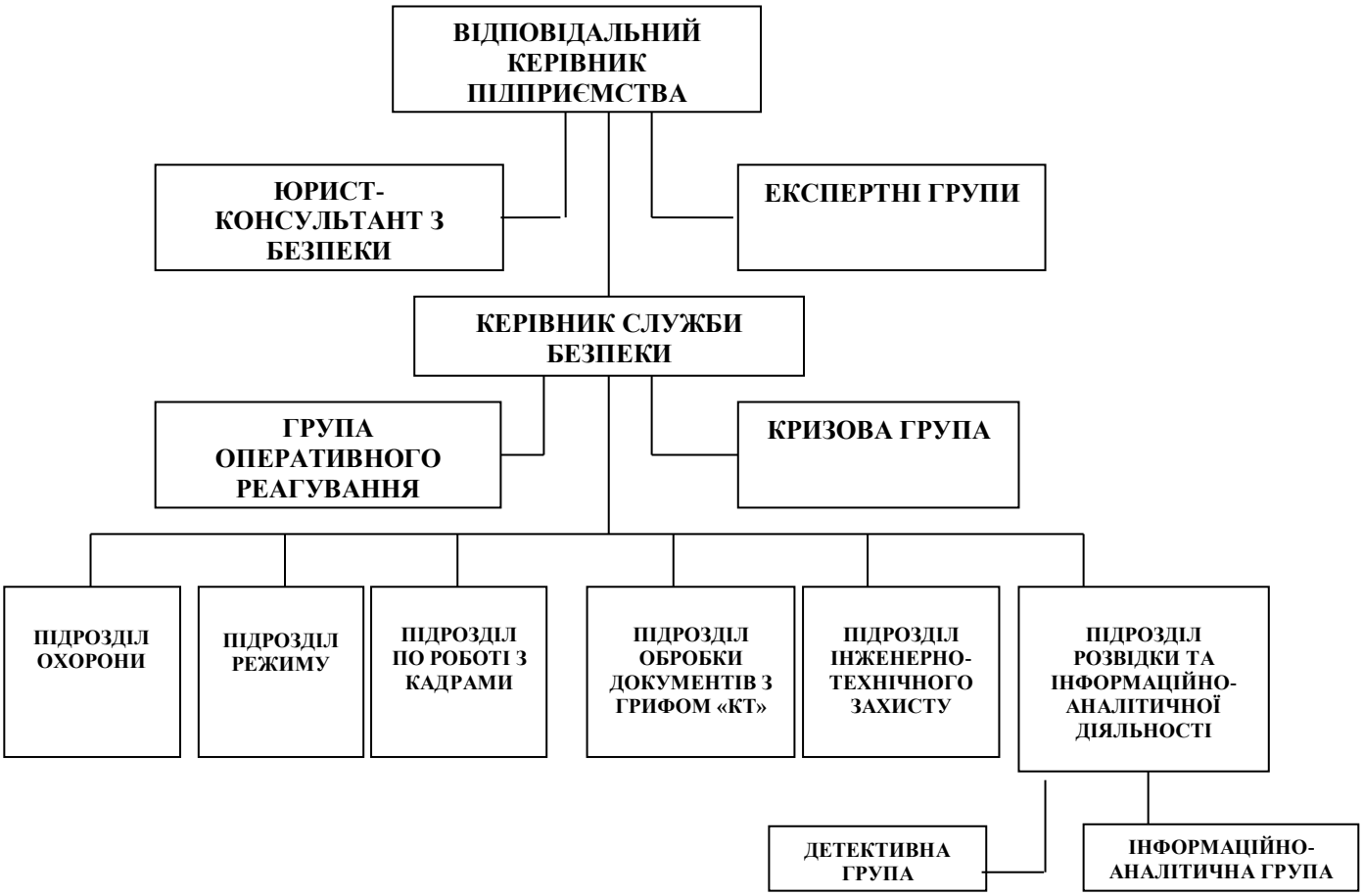


Рисунок 2.1 - Приблизна структура системи безпеки фірми

2.2 Управління безпекою

Служба безпеки (СБ) повинна бути завжди готова до виникнення критичних (кризових) ситуацій, що проявляються в результаті зіткнення інтересів бізнесу й злочинного світу.

Кризова ситуація – це прояв фактів загроз з боку окремих осіб або груп. Кризова ситуація може проявлятися й розвиватися по-різному: повільно або спонтанно, миттєво.

При оцінці й аналізі кризової ситуації дуже важливо якнайшвидше визначитися з відповіддю на питання, чи здатна СБ упоратися із ситуацією самотужки, або для її вирішення необхідне залучення правоохоронних органів. Однак у кожному разі, з огляду на можливість виникнення кризових ситуацій, будь-яка фірма прагне створити в складі СБ окреме формування, іменоване КРИЗОВА ГРУПА. Вона створюється із числа ключових фігур фірми: директор, керівники лінійних підрозділів, філій, служб, юрист, головний бухгалтер й ін. Кризова група може бути створена на постійній основі з неодмінним включенням у число її членів:

- керівника фірми;
- юриста;
- фінансиста;
- керівника служби безпеки.

Керівництво кризовою групою може бути покладене на главу фірми. Перераховані особи, як правило, у силу свого службового становища, володіння спеціальними знаннями, досвідом мають у своєму розпорядженні реальні можливості досить ефективно впливати на обставини, в умовах яких виникає й протікає кризова ситуація, не випускаючи при цьому важелів впливу на повсякденну комерційну й виробничу діяльність.

У кожному конкретному випадку до складу кризової групи можуть включатися й інші фахівці.

Кризова група вирішує наступні завдання:

- оцінка обстановки;
- вживання невідкладних заходів по безпеці;
- керування діяльністю фірми в екстрених умовах;
- забезпечення оперативної взаємодії з органами правопорядку.

Головна мета створення кризової групи - протидія зовнішнім загрозам безпеки фірми. Робочі засідання групи повинні проходити в умовах граничної конфіденційності.

Як правило, діяльність кризової групи регламентується типовим планом дій керівництва й персоналу фірми. Залежно від складної ситуації плани можуть бути наступного виду:

- план дій при загрозах вибуху;
- план дій при захопленні заручників або викраденні співробітників фірми;
- план дій при вимаганні;
- план дій при нападі на приміщення фірми;
- план дій при нападі на інкасаторів.

Типові кризові плани повинні бути документами конфіденційного характеру, доступ до яких повинен мати вузьке коло осіб. І залишатися подібні плани повинні не більш ніж у двох-трьох екземплярах. Один зберігається у керівника, інший - у начальника служби безпеки, третій може перебувати в особи, що заміщає керівника фірми в його відсутність.

Здійснюючи планування, треба виходити з того, що план - це не набір заходів, а послідовна лінія поведінки, стратегія діяльності фірми в конкретній кризовій ситуації, спрямована на забезпечення ефективної безпеки.

2.3 Служба безпеки фірми

2.3.1 Основні завдання служби безпеки

Основними завданнями служби безпеки фірми є:

- забезпечення безпеки виробничо-торгівельної діяльності і захисту інформації і відомостей, що є комерційною таємницею;
- організація роботи з правового, організаційного й інженерно-технічного (фізичного, апаратного, програмного й математичного) захисту комерційної таємниці;
- організація спеціального діловодства, що виключає несанкціоноване одержання відомостей, що є комерційною таємницею;
- запобігання необґрунтованого допуску й доступу до відомостей і робіт, що становлять комерційну таємницю;

- виявлення і локалізація можливих каналів витоку конфіденційної інформації в процесі повсякденної виробничої діяльності і в екстремальних (аварійних, пожежних й ін.) ситуаціях;
- забезпечення режиму безпеки при проведенні всіх видів діяльності, включаючи різні зустрічі, переговори, наради, пов'язані з діловим співробітництвом як на національному, так і міжнародному рівні;
- забезпечення охорони будинків, приміщень, устаткування, продукції і технічних засобів забезпечення виробничої діяльності;
- забезпечення особистої безпеки керівництва і провідних співробітників та фахівців;
- оцінка маркетингових ситуацій і неправомірних дій зловмисників і конкурентів.

У своїй діяльності служба безпеки керується:
- інструкцією з організації режиму і охорони;
- інструкцією із захисту комерційної таємниці;
- переліком відомостей, що становлять комерційну таємницю;
- інструкцією по роботі з конфіденційною інформацією для керівників, фахівців і технічного персоналу;
- інструкцією з організації зберігання справ, що містять конфіденційну інформацію, в архіві;
- інструкцією з інженерно-технічного захисту інформації;
- інструкцією про порядок роботи з іноземними представниками і представництвами.

2.3.2 Загальні функції служби безпеки

Служба безпеки фірми виконує наступні загальні функції:
- організує й забезпечує пропускний і внутрішньо-об'єктивний режим у будинках і приміщеннях, порядок несення служби охорони, контролює

дотримання вимог режиму співробітниками, суміжниками, партнерами і відвідувачами;

- керує роботами з правового і організаційного регулювання відносин по захисту комерційної таємниці;
- бере участь у розробці основних документів з метою закріплення в них вимог забезпечення безпеки і захисту комерційної таємниці, зокрема уставу, правил внутрішнього трудового розпорядку, положень про підрозділи, а також трудових договорів, угод, підрядів, посадових інструкцій і обов'язків керівництва, фахівців, робітників та службовців;
- розробляє й здійснює разом з іншими підрозділами заходи щодо забезпечення роботи з документами, що містять відомості, що є комерційною таємницею, при всіх видах робіт, організує й контролює виконання вимог інструкції із захисту комерційної таємниці;
- вивчає всі сторони виробничої, комерційної, фінансової і іншої діяльності для виявлення і закриття можливих каналів витоку конфіденційної інформації, веде облік і аналіз порушень режиму безпеки, накопичує і аналізує дані про злочинні устремління конкурентів і інших організацій відносно діяльності фірми і її клієнтів, партнерів, суміжників;
- організує і проводить службові розслідування за фактами розголошення відомостей, втрат документів і інших порушень безпеки підприємства;
- розробляє, веде, поновлює і поповнює перелік відомостей, що становлять комерційну таємницю і інші нормативні акти, що регламентують порядок забезпечення безпеки і захисту інформації;
- забезпечує строге виконання вимог нормативних документів по захисту комерційної таємниці;
- здійснює керівництво службами і підрозділами безпеки підвідомчих підприємств, організацій, установ в частині обговорених в договорах умов по захисту комерційної таємниці;

- організує і регулярно проводить навчання співробітників фірми і служби безпеки з усіх напрямків захисту комерційної таємниці;
- веде облік сейфів, металевих шаф, спеціальних сховищ і інших приміщень, в яких дозволене постійне або тимчасове зберігання конфіденційних документів;
- веде облік виділених для конфіденційної роботи приміщень, технічних засобів у них, що володіють потенційними каналами витоку інформації;
- підтримує контакти із правоохоронними органами і службами безпеки сусідніх підприємств в інтересах вивчення криміногенного стану в районі;
- запобігає втратам, розкраденню майна, власності та цінностей підприємства (фірми);
- забезпечує фізичний захист та безпеку персоналу підприємства;
- забезпечує створення та функціонування системи технічного захисту інформації на підприємстві;
- реалізує інженерно-технічний захист території, будівель та приміщень.

Нижче подано деталізацію певних загальних функцій служби безпеки підприємства.

2.3.3 Функції по забезпеченню захисту майнової власності підприємства (з урахуванням особливостей і уразливості підприємства)

1) Визначення системи охорони підприємства, дислокація постів, протипожежної автоматики, зв'язку.
2) Виділення приміщень (ділянок), де зберігаються товарно-матеріальні цінності (гроші) і через керівників відповідних підрозділів здійснення заходів по підвищенню надійності їхнього фізичного захисту.
3) Визначення ділянок, уразливих у вибухо-пожеженебезпечному відношенні, вихід з ладу яких може завдати серйозної шкоди підприємству, і вироблення заходів по нейтралізації загроз.

4) Визначення технологічного обладнання, вихід з ладу якого може привести до більших економічних втрат, і розробка заходів по нейтралізації погроз.
5) Визначення уразливих місць у технології виробничого циклу, несанкціонована зміна в якій може привести до втрати якості продукції, що випускається, і завдати матеріальної шкоди, і вживання відповідних заходів.
6) Розробка, запровадження в дію й підтримка на охороняємій території пропускного й внутріоб'єктового режиму (порядок, час пропуску робітників, відвідувачів на територію, у тому числі й у святкові дні; порядок вивозу (ввозу) або виносу (внесення) матеріальних цінностей, готової продукції, матеріалів і т.п.; місця й кількість контрольних проходів і проїздів; приміщення, підрозділи, у які обмежується доступ; система пропусків і документації).
7) Розробка документів, що регламентують адміністративно-правову основу діяльності по охороні майнових цінностей підприємства (положення про охорону; інструкція про порядок забезпечення й схоронності матеріальних і документальних цінностей підприємства; інструкція про пропускний і внутріоб'єктовий режим).
8) Доведення вимог (відповідних коректив) з питань охорони, пропускного й внутріоб'єктового режиму до співробітників підприємства.
9) Контроль виконання й аналіз стану надійності зберігання матеріальних цінностей, охорони, пропускного й внутріоб'єктового режиму.
10) Проведення службових розслідувань по фактах порушення порядку роботи з майновими цінностями.
11) Організація взаємодії зі Службою безпеки України й органами внутрішніх справ про забезпеченню економічної безпеки підприємства (з урахуванням компетенції цих органів).

2.3.4 Функції по забезпеченню безпеки персоналу підприємства

1) Розробка заходів забезпечення фізичного захисту персоналу; організація охорони (особистої охорони, охорони засобів пересування), пропускного й внутріоб'єктового режиму; установлення відповідного порядку прийому відвідувачів, роботи секретарів-референтів і т. п.
2) Забезпечення коштами технічного захисту персоналу: від несанкціонованого проникнення в приміщення (кабінети), в автомашини, на автостоянку, у квартиру; для фіксації спроб злочинних дій (установка магнітофонів для запису переговорів, кінокамер) для схованого зв'язку керівника з охороною підприємства.
3) Визначення переліку інформації, що не підлягає розголошенню стороннім особам (такої, що не входить до КТ).
4) Збір СБ інформації про ознаки, характерні для конкретних видів загроз персоналу (співробітникам).
5) Забезпечення контролю за проведенням ремонтних, профілактичних робіт, здійснюваних сторонніми організаціями на підприємстві (при необхідності після завершення робіт проводиться спеціальне обстеження цих приміщень, машин, пристроїв, приладів).
6) Підготовка персоналу до дій в екстремальних ситуаціях (вироблення навичок оцінки інформації, відповідних форм поводження й прийняття рішень).
7) Навчання персоналу й членів їхніх родин виявленню ознак, що вказують на підготовку протиправних дій відносно особистості й членів їхньої родини.
8) Правове навчання персоналу:
   - правові можливості захисту від злочинця;
   - правила забезпечення особистої безпеки від неправомірного кримінального переслідування;
   - безпека особи, опитуваної про обставини здійснення злочину;

- забезпечення безпеки особистості в процесі заходів правоохоронних органів, пов'язаних із проникненням у житло.

9) Установлення й підтримка практичних форм взаємодії СБ із правоохоронними органами по забезпеченню безпеки персоналу (при одержанні даних про підготовку протиправних дій відносно персоналу, що зачіпають питання забезпечення економічної безпеки підприємства).

Викладені функції організаційних структур і складність розв'язуваних завдань по забезпеченню безпеки комерційної таємниці об'єктивно викликають потребу використання засобів обчислювальної техніки. В якості конкретного рішення може бути рекомендоване використання організаційно-функціональних автоматизованих місць посадових осіб служби безпеки (АРМів СБ).

На першому етапі впровадження засобів автоматизації можлива розробка АРМів для начальника служби безпеки; для групи обробки документів із грифом "Комерційна таємниця" спеціального відділу; для інженерно-технічної групи, а в деяких випадках для групи аналізу зовнішньої діяльності і групи режиму і роботи з персоналом.

На наступних етапах масштаби впровадження засобів автоматизації можуть бути розширені в напрямку забезпечення оперативного керування поточною діяльністю СБ залежно від зміни умов.

2.3.5 Склад служби безпеки

Служба безпеки є самостійною організаційною одиницею, що підкоряється безпосередньо керівникові фірми.

Очолює службу безпеки начальник служби в посаді заступника керівника фірми по безпеці.

Організаційно служба безпеки складається з наступних структурних одиниць:

- відділу режиму і охорони в складі сектора режиму і сектора охорони;

- спеціального відділу в складі сектора обробки секретних документів і сектора обробки документів з грифом "Комерційна таємниця";
- інженерно-технічної групи;
- групи контррозвідки і інформаційно-аналітичної діяльності.

Співробітники підрозділів служби безпеки з метою забезпечення захисту відомостей, що становлять комерційну таємницю, *мають право*:

- вимагати від всіх співробітників фірми, партнерів, клієнтів строгого і неухильного виконання вимог нормативних документів або договірних зобов'язань по захисту комерційної таємниці;
- вносити пропозиції по вдосконаленню правових, організаційних і інженерно-технічних заходів щодо захисту комерційної таємниці.

Співробітники служби безпеки *зобов'язані*:

- здійснювати контроль за дотриманням інструкції із захисту комерційної таємниці;
- доповідати керівництву про факти порушення вимог нормативних документів по захисту комерційної таємниці і інших дій, що можуть привести до витоку конфіденційної інформації при втраті документів або виробів;
- не допускати неправомірного ознайомлення з документами і матеріалами, що мають гриф "Комерційна таємниця", сторонніх осіб.

Співробітники служби безпеки несуть *відповідальність* за особисте порушення безпеки комерційної таємниці і за невикористання своїх прав при виконанні функціональних обов'язків по захисту конфіденційних відомостей співробітниками підприємства.

З метою більш широкого охоплення і якісного виконання вимог захисту комерційної таємниці рішенням керівництва фірми і служби безпеки можуть

створюватися окремі комісії, що виконують певні контрольно-ревізійні функції на тимчасовій або постійній основі, у тому числі:

- квартальні або річні комісії з перевірки наявності, стану і обліку документів (матеріалів, відомостей, цінностей);
- комісія з оцінки можливостей публікації періодичних документів, оголошень, проспектів, інтерв'ю і інших виступів у пресі, на радіо і телебаченні, семінарах, симпозіумах, конференціях і т.п.;
- періодичні перевірочні комісії для перевірки знань і вміння виконувати вимоги нормативних документів по захисту комерційної таємниці, а також для оцінки ефективності і надійності захисних заходів щодо забезпечення безпеки фірми.

3 ІНФОРМАЦІЙНІ АСПЕКТИ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

3.1 Інформаційна безпека в системі безпеки підприємницької діяльності

Очевидно, що будь-який ОПД в загальному випадку перебуває під впливом певної множини загроз, як зовнішніх так і внутрішніх, що можуть бути реалізовані відносно різних елементів та складових ОПД. Тобто безпека підприємницької діяльності має принципово інтегральний характер й враховує увесь спектр можливих загроз, що відрізняються як за своїм походженням, так і за механізмами їх реалізації. Через це стає можливим виділення та диференціація в межах загальної безпеки ОПД “часткових” безпек: економічної, технологічної, екологічної, інформаційної тощо. Однак, як це неодноразово зазначалося дослідниками, інформаційна безпека (ІБ) серед цих “часткових” безпек займає окреме й, наразі, чільне місце. Це обумовлюється тим, що крім самостійного існування як “часткового” виду безпеки, ІБ входить, як обов’язкова складова, до всіх інших “часткових” безпек і становить невід’ємний елемент їх успішної реалізації.

В загальному випадку до інформаційних процесів, що забезпечують функціонування довільних сфер людської діяльності у будь-якій системі соціальних, виробничих чи інших відносин, висуваються наступні вимоги:

- інформація, що циркулює у цих сферах та системах, має бути повною, достовірною, своєчасною та доступною (за виключеннями, що визначаються правилами функціонування самих систем);
- можливі інформаційні впливи не повинні порушувати встановлений порядок функціонування систем;
- технологічні збої та помилки у ході реалізації інформаційних процесів із збору, формування, обробки, збереження та передавання інформації не повинні призводити до порушення функціонування систем;

- інформація не може бути несанкціоновано знищена, модифікована або розповсюджена, якщо існує певний порядок, що регламентує поводження з цією інформацією.

У найбільш загальному розумінні *інформаційна безпека* – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Інформаційна безпека у більш вузькому розумінні, наприклад, редукованому до певного виду діяльності (зокрема, *підприємницької*), - це захищеність цього виду діяльності від загроз в інформаційній сфері. Очевидно, що множина завдань, виконання яких повинне забезпечити ІБ в цьому випадку, залежить від характеру та особливостей відповідного виду діяльності, а також цілої низки конкретних обставин та факторів, які можуть більш-менш суттєво впливати на стан ІБ у кожному окремому випадку. Однак, незважаючи на таку багатоаспектність та багатовимірність окресленої вище ситуації, практично всі фахівці з безпеки підприємницької діяльності вважають, що найбільш важливим елементом системи ІБ фірми (підприємства, корпорації) є *захист комерційної таємниці*. Такий одностайний висновок обумовлюється насамперед тим, що для ринкової економіки в умовах жорсткої конкуренції, яка часто виходить за правові межі, досягти економічної безпеки підприємницької діяльності, забезпечити її функціональну стабільність, уникнути матеріальної шкоди та інших негараздів можливо лише за умов обов’язкового створення системи захисту комерційної таємниці.

3.2 Комерційна таємниця

Згідно із статтею 36 “Господарського кодексу України”, *комерційною таємницею* визначаються відомості, пов’язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб’єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб’єкта господарювання. До іншої діяльності суб’єктів господарювання звичайно відносять науково-дослідну роботу (НДР), експериментально-конструкторські розробки (ЕКР, разом НДЕКР), інформаційно-аналітичну роботу тощо.

Комерційною таємницею підприємства не може бути інформація, приховання якої може завдати шкоди суспільству. Відповідно до Закону України «Про підприємства в Україні» зміст і обсяг відомостей, що становлять комерційну таємницю, визначається керівником підприємства. Підприємство має право не надавати інформацію, що містить комерційну таємницю.

Для забезпечення взаємодії державних органів влади й управління з підприємствами (фірмами) між самими підприємствами, між підприємствами й фізичними особами Урядом України встановлюється відповідний інформаційний простір, обумовлений переліком відомостей, які не можуть становити комерційну таємницю. Такий перелік викладений у постанові Кабінету Міністрів України «Про перелік відомостей, які не становлять комерційної таємниці» . Цей документ створює правову основу для забезпечення захисту інтересів держави, підприємців, споживачів від зловживань і корупції.

Таким чином, *відомості, віднесені до комерційної таємниці, повинні мати наступні ознаки:*

- не бути державними секретами;
- стосуватися виробничої діяльності підприємства;
- не завдавати шкоди інтересам суспільства;
- мати дійсну або потенційну комерційну цінність і створювати переваги в конкурентній боротьбі;

- мати обмеження в доступі, установлювані керівником підприємства на законній підставі;
- підприємство (фірма) вживає заходів до їхньої охорони.

До комерційної таємниці можуть бути віднесені:

- технологія виробництва;
- технологічні прийоми й устаткування; модифікація раніше відомих технологій і процесів; перспективні методи керування; цінова й збутова політика;
- порівняльні характеристики власних асортиментів і товарів конкурентів з погляду якості, зовнішнього вигляду, упаковки й т.д.; виробничі, комерційні й фінансово-кредитні відносини з партнерами;
- плани підприємства по розширенню (згортанню) виробництв; факти ведення переговорів по питанню купівлі-продажу; дані, які можуть бути використані для завдання збитків репутації підприємства (фірми);
- інформація про кадри (плинність кадрів, провідні спеціалісти й місця їхньої роботи за сумісництвом); наявність коштів і умов для захисту комерційної таємниці.

До промислових секретів фірми відносять основні виробничі показники, проекти, технологічні інструкції, результати перевірок і випробувань, опис зразків продукції на сировину, сутність експериментів, оцінку якості процесів і виробів, дослідницькі звіти, карти контролю якості, інструкції з підготовки кадрів, вартісні показники, дослідження ринку, список покупців, умови поставок і стратегію на ринку, прогнози й т.д.

Перелік відомостей, які необхідно захищати в умовах ринку, може бути досить великий. Становлять інтерес дані про те, що хотіли б знати фірми про своїх конкурентів.

Перелік відомостей, які необхідно захищати в умовах ринку:

<u>Інформація про ринок:</u>

1) ціни, знижки, умови договорів, специфікація продукту;

2) обсяг, тенденція й прогноз для даного продукту;
3) частка на ринку й тенденція її зміни;
4) ринкова політика й плани;
5) відносини зі споживачами й репутація;
6) чисельність і розміщення торговельних агентів;
7) канали, політика й методи збуту;
8) програма реклами.

Інформація про виробництво й продукцію:

1) оцінка якості й ефективності;
2) номенклатура виробів;
3) технологія й устаткування;
4) рівень витрат;
5) виробничі потужності;
6) розміщення й розмір виробничих підрозділів і складів;
7) спосіб упаковки;
8) доставка.

Інформація про організаційні особливості й фінанси:

1) особи, що приймають ключові рішення;
2) філософія осіб, що приймають ключові рішення;
3) фінансові умови й перспективи;
4) програми розширення й придбань;
5) головні проблеми й можливості.

Більш детальна розшифровка відомостей, що представляють першочерговий інтерес для конкурентів, дається також в іншому переліку. Оцінка його дозволяє зробити висновок, що саме ці відомості з більшим ступенем ймовірності можуть бути комерційною таємницею підприємства.

Інформація у фінансово-економічній сфері:

1) результати виробничої діяльності банків і підприємств за квартал, півріччя, рік;
2) висновки й рекомендації експертів з питань тактики й стратегії економічної діяльності, переговорів з партнерами, дані, що показують обсяги закупівлі-продажу товарів, послуг, рівень максимально уторгованих цін, обсяги наявних валютних коштів, використовуваних для підвищення ефективності угод;
3) номенклатура й кількість товарів по взаємних зобов'язаннях, обсяги перевезень, транзиту вантажів і транспортні витрати;
4) собівартість товарів, послуг, кредитні й платіжні умови;
5) фактичний стан розрахунків з тими або іншими партнерами;
6) експортно-імпортна продукція, фінансові планові й фактичні показники цієї продукції;
7) методика розрахунку конкурентних цін по товарах, роботам і послугам;
8) час виходу на ринок при закупівлях або продажу товарів, послуг, і вибір партнерів за висновком угод з дефіцитною продукцією;
9) плановані кредити, умови і їхні розміри;
10) плановане створення спільних, змішаних, малих, акціонерних підприємств;
11) незадовільне фінансове становище підприємства;
12) ефективність і доцільність закупівлі ліцензій, зацікавленість замовників у тій або іншій валюті і її кількості;
13) склад торгових клієнтів, посередників підприємства, товарообіг з ними.

Інформація в науково-технічній і технологічній сферах:

1) основні виробничі фонди, їхні потужності й ефективність;
2) напрямки розширення (згортання) виробництва, застосовувані (що готуються до впровадження) технології, устаткування;
3) модифікація й модернізація застосовуваної раніше техніки, технології;

4) окремі вузли готових виробів, нові розробки високої конкурентоспроможності;
5) застосовувані (що готуються до застосування) методи керування виробництвом, програмне й комп'ютерне забезпечення виробництва, можливі шляхи одержання інформації, що зберігається в ЕОМ і ПЕОМ керівництва, головні фахівці підприємства;
6) НДЕКР що ведуться, проектні роботи і їхні результати;
7) цілі нарад, засідань органів керування підприємства.

Інформація в соціальній сфері:

1) інтелектуальний потенціал колективу, його провідні спеціалісти, їх моральні й ділові якості, наявність компрометуючих їх зв'язків, біографічні дані;
2) використовувана в колективі система стимулів, що зміцнюють дисципліну, що підвищують продуктивність праці, схоронність комерційної таємниці;
3) різні аспекти, що стосуються економічної безпеки підприємства;
4) будь-які можливості завдання моральних збитків підприємству, зниження його престижу в суспільстві й конкурентоспроможності;
5) плановані рекламні акції;
6) наявні протиріччя між колективом підприємства й державними структурами, інтересами громадськості;
7) особисті відносини провідних спеціалістів як між собою, так і з керівниками екологічних, економічних, адміністративних організацій;
8) можливі протиріччя, конфлікти усередині колективу, їхні конкретні учасники;
9) наявність у членів колективу, керівництва, керівників підрозділів намірів почати свою справу, фінансові й моральні проблеми.

Дослідження механізму протиборства в торгово-економічній сфері дозволяють виділити відомості, які можна віднести до комерційної таємниці при укладанні контрактів.

Інформація у зв'язку з підписанням контракту:

1) обсяги експортних поставок і послуг;
2) ціна на товари і послуги що, поставляються;
3) валютно-фінансові умови;
4) суми надходжень від реалізації контрактів;
5) факт ведення переговорів, партнери на переговорах.

Нерозповсюдження, приховання від імовірних конкурентів вищезгаданої інформації утрудняє їхні дії, забезпечує підприємству економічні переваги.

Забезпечення схоронності комерційної таємниці створює передумови для монопольних дій у конкретній сфері бізнесу, є своєрідною форою в економічному змаганні.

3.3 Методика виявлення відомостей, що становлять комерційну таємницю

Порядок виділення із усього обсягу власної інформації підприємства (фірми) її найцінніших частин для наступного захисту тісним образом пов'язаний із процесом виробництва товарів (послуг) і слідує із практики конкурентної боротьби. Фактори, що визначають конкурентоспроможність підприємства, можуть давати позитивні результати за умови їхнього приховання від економічних суперників. Тому віднесення таких відомостей до комерційної таємниці є формою захисту економічної безпеки підприємства (фірми).

Суть завдання формування методики виділення коштовних відомостей полягає у відшуканні логіки дій і ознак, що характеризують комерційну таємницю.

Перший етап. Представимо всю циркулюючу на підприємстві інформацію у вигляді кола. Здійснимо послідовно наступні дії:

1) спочатку вилучимо сектор відомостей, що являються державними секретами (якщо вони є на підприємстві), тому що порядок і організація їхнього захисту регламентується вимогами, установленими урядом;

2) виключимо з розгляду загальновідомі або широко застосовувані іншими підприємствами відомості, а також інформацію, що утримується в постанові кабінету міністрів України «Про перелік відомостей, які не становлять комерційної таємниці»;

3) сектор, що залишився, розділимо на два види відомостей:

- НДЕКР, технологія, керування;
- ділова (комерційно-фінансова) інформація.

Частково перший вид інформації, з огляду на вигоду й доцільність, можна захищати за допомогою патентного й авторського права.

Після послідовного виконання згаданих дій предметом аналізу й оцінки залишається частина незахищених за допомогою патентів і авторського права відомостей, а також комерційно-фінансові дані.

Зробимо невеликий відступ. Ключем до розуміння того, які відомості доцільно в той або інший період захищати як комерційну таємницю, є конкуренція (цінова й нецінова). Саме тому до комерційної таємниці варто відносити ті відомості, які дають (можуть дати) значні переваги в конкурентній боротьбі. Розголошення ж цієї інформації завдає економічної шкоди внаслідок зниження конкурентоспроможності товарів і послуг підприємства.

Розглянемо один із прикладів *цінової конкуренції.* Ваше підприємство закінчує розробку магнітофона, що має переваги перед аналогічними товарами інших виробників, які, у свою чергу, ведуть роботи зі створення більш досконалих виробів. У силу яких-небудь причин конкурентам стає відома інформація про появу на ринку новітнього магнітофона і його планованій ціні. Отримані відомості дозволяють економічним суперникам завчасно (на стадії НДЕКР, досвідченого виробництва) внести корективи в розробку свого виробу й домогтися зниження витрат

виробництва, а отже, створити умови для продажу свого товару по більш низькій ціні в порівнянні із ціною Вашого магнітофона. При схожих параметрах покупець швидше за все віддасть перевагу виробу конкурента.

Знання особливостей цінової конкуренції дозволяє зрозуміти, чому собівартість розроблювального товару є комерційною таємницею. Таким чином, на останньому етапі блок інформації, що залишився, оцінюється з позицій одержання конкурентних переваг на ринку товарів і послуг. І чим більші вигоди можуть бути отримані від використання цих відомостей у конкурентній боротьбі, тим вони цінніше й вимагають відповідного захисту.

Певні вимоги пред'являються до інформації, пропонованої на ринку як самостійний товар. У цьому випадку таємність (ступінь захищеності) на стадіях розробки, купівлі-продажу є складовою частиною інформаційного товару. Адже ніхто не стане купувати широко відомі (розголошені) відомості, навіть такі, що становлять комерційну таємницю, тому що дана інформація не дозволить покупцеві одержати які-небудь переваги в економічному суперництві.

Наступним етапом методики виділення відомостей, що становлять комерційну таємницю, *є аналіз і оцінка сфер і циклів виробництва товарів.*

Фірма «Артур Д. Литлл» склала перелік з восьми сфер, у яких можливі нововведення: товар, сервіс, маркетинг, виробництво, розподіл, фінансування, керування, соціальна сфера. На основі аналізу для кожної із цих сфер був визначений обсяг нововведень, необхідний для успішної діяльності (дані представлені в процентному вигляді):

	Пн. Америка	Європа	Японія	середнє
товар	49	50	80	62
сервіс	42	36	51	43
маркетинг	45	35	55	45
виробництво	27	33	53	37
розподіл	14	8	29	17
соціальна сфера	12	16	26	18

З наведених даних слідує, що найбільший обсяг відомостей (нововведень, що впливають на конкурентоспроможність), що становлять комерційну таємницю припадає на сфери: *товар, маркетинг, виробництво, сервіс*.

Основні цикли виробництва товару входять у так звану *петлю якості товару*.

Петля якості включає:

1) маркетинг, пошук, вивчення ринку;
2) проектування або розробку технічних вимог;
3) матеріально-технічне постачання;
4) підготовку й розробку виробничих процесів;
5) виробництво;
6) контроль, проведення випробувань і обстежень;
7) упаковки й зберігання;
8) реалізацію й розподіл продукції;
9) монтаж і експлуатацію;
10) технічну допомогу й обслуговування;
11) утилізацію після використання.

Маркетингові дослідження дозволяють виявити запити споживача, сформулювати вихідні вимоги до нової продукції, а також визначити потребу в принципово новій продукції.

Фірми економічно розвинених країн приділяють значну увагу оцінці положення на ринку продукції, що випускається, дослідженню факторів, що забезпечують конкурентоспроможність. Більшість закордонних фірм починає створення нової продукції з аналізу даних служби маркетингу про переваги й недоліки вже освоєної продукції, а також продукції конкурентів.

Результати досліджень ринку й намічувані на їхній основі заходи є інформаційною базою для ведення ефективної виробничо-комерційної діяльності й у силу цього можуть бути віднесені до комерційної таємниці підприємства.

Важливим елементом маркетингової діяльності підприємства є так званий реінжиніринг (зворотний інжиніринг) - конструювання навпаки.

Зворотним інжинірингом називається розбирання й вивчення продукту для визначення його компонентів, конструкції й комерційних секретів.

У більшості випадків у зворотному інжинірингу немає нічого незаконного. У світі комерційних таємниць це практикується. У каліфорнійській версії закону про уніфіковані комерційні секрети, наприклад, проголошено, що зворотний інжиніринг не розглядається як «незаконний засіб» одержання інформації. Причина появи цього правила цілком зрозуміла, коли ви розглядаєте основу захисту комерційних секретів: якщо ви представили привселюдно свій продукт, ви не можете оголосити секретом те, що може бути виявлене в результаті дослідження цього продукту. Це просто більше не є таємницею.

Як і більшість інших правил, це теж має свої границі. Ви не можете використовувати процес зворотного інжинірингу для того, щоб «відкрити» і скопіювати запатентований винахід. Це одна з переваг використання захисту патентом у порівнянні з комерційними таємницями. Також, якщо ви не просто придбали продукт на вільному ринку, а придбали його за якою-небудь формою лімітованої ліцензії або по іншому контракту, що обмежує ваші права по зворотному інжинірингу, суди звичайно вважають ці обмеження такими, що мають законну силу. Зрештою, через зворотний інжиніринг ви не можете просто скопіювати продукт, захищений товарним знаком, інакше продаж ідентичного продукту викличе в покупців сумнів у джерелі його виробництва. Така справа буде розглядатися як несумлінна конкуренція.

Результати маркетингових досліджень мають важливе значення і на стадії проектування й розробки. Це обумовлено тим, що рівень витрат на експлуатацію – один з основних показників конкурентоспроможності товару – більш ніж на 80% визначається характеристиками, що закладаються на стадії розробки. На стадії проектування й виготовлення дослідного зразка конструктор

може вплинути лише на 15% загальних витрат, а коли виріб передається в серійне виробництво, ці можливості зменшуються на 5%.

Проектування й розробка включають:

- визначення основних техніко-економічних параметрів;
- складання кошторисів витрат;
- визначення структури витрат по етапах впровадження;
- визначення ціни;
- розрахунок прибутку;
- формулювання умов продажів;
- проектування каналів і методів збуту;
- порядок техобслуговування й обсяг послуг після продажного обслуговування.

Кожний з названих етапів розробки нового товару, враховує результати маркетингових досліджень, включає інформацію, що створює передумови для конкурентних переваг, тобто містить відомості, що становлять комерційну таємницю.

Розробники нової продукції використовують відомості про дефекти, поломки раніше спроектованих виробів, але таких, що ще реалізуються на ринку. Розголошення такої інформації може завдати серйозної шкоди фірмі внаслідок зниження рівня продажів, довіри споживачів.

Матеріально-технічне постачання – найважливіший елемент процесу виробництва товарів. Найціннішою інформацією, що вимагає захисту, є відомості, використання яких може привести до виникнення вузьких місць у постачанні. Результатом розголошення комерційної таємниці в цій області діяльності може стати підвищення цін на сировину, устаткування, що комплектують; зрив поставок, розірвання контракту; зниження рівня співробітництва підприємства з постачальниками й т.п.

Розглядаючи цикл виробництва з позиції охорони комерційної таємниці, ми повинні враховувати, що більшості фірм вдається домогтися динамічного росту й

фінансово-комерційного успіху за рахунок невеликих поступових удосконалень. Як вважають фахівці, це самий реалістичний шлях.

Варто також мати на увазі, що хоча великі прориви з більшою часткою ймовірності можливі при значних інноваціях в області високої технології, які вимагають для здійснення й солідних капіталовкладень, і тривалого часу, успіх на ринку незмінно приносять безперервні вдосконалення в сфері високої технології, на які не потрібно ні великих грошей, ні тривалих строків.

Більшість новинок являє собою вдосконалені варіанти раніше існуючих виробів. І тільки одна-дві зі ста виявляються чимось принципово новим.

Заставою успіху багатьох фірм є невеликі поетапні вдосконалення. Їх застосовують не відразу в момент появи. Фірма акумулює ці вдосконалення, а потім на їхній основі випускає товари - доповнення, поліпшені в порівнянні з існуючими відразу по декількох показниках.

З урахуванням цих особливостей ринку до комерційної таємниці повинні ставитися й відомості про вдосконалення виробів, що випускаються, включаючи технологію й інші аспекти (а не тільки значні інновації).

Для керівників і фахівців із захисту комерційної таємниці проблема диференціації якості товарів щодо товарів конкурентів обов'язково повинна знайти відбиття в заходах щодо захисту інформації. На стадії розробки товару певну цінність саме й будуть подавати відомості (інформація) про його властивості, що забезпечують істотну відмінність від наявних на ринку виробів. Це найцінніші відомості підприємства (фірми), що становлять комерційну таємницю.

При покупках керуються в основному показниками диференціації товарів, досягнутої за рахунок ефективного дизайну, а не факторами ціни.

Зусилля підприємств направляються на підвищення ціннісної значимості власних товарів в очах клієнта й на поглиблення різниці між своїми товарами й товарами конкурентів (цього можна досягти різними шляхами: зробити товар менше по розміру, легше по масі, могутніше, дешевше, підсиливши існуючі властивості).

Доцільно скласти вичерпний перелік властивостей свого товару, а потім задаватися питанням, яка із цих властивостей, будучи удосконаленою, забезпечить йому найбільшу конкурентну відмінність. Саме ці відомості з великим ступенем імовірності можуть бути віднесені до комерційної таємниці.

Щоб не програвати в конкурентній боротьбі, фірми постійно вдосконалюють керування, організують виробництво або надання послуг з більш низькими витратами й вищою якістю. Для цього автоматизують виробництво, спрощують структури керування, реалізують програми по активному залученню працівників у керування, погодять розмір оплати з ефективністю праці.

Потреба в удосконалюванні керування обумовлена також зменшенням тривалості життєвого циклу товару, збільшенням номенклатури, зниженням обсягів, ускладненням технологічних процесів.

Змінюються традиційні погляди людей на бізнес. Фірми рішуче відмовляються від прихильності до масового виробництва тисяч, а те й мільйонів зовсім однакових виробів, що пояснюється тільки тим, що це - дешевий спосіб виготовлення. Виробники усе точніше й точніше пристосовують товари до потреб замовників.

Проведені порівняльні аналізи показують, що інвестиції в підвищення кваліфікації й удосконалювання організаційно-управлінської складової дають у багато разів більший економічний ефект, ніж просто інвестиції в автоматизацію основного виробництва.

Принцип вузької спеціалізації кожного із працівників заміняється підходом, при якому група робітників високої кваліфікації несе повну відповідальність за певну ділянку роботи. Вона відповідає за якість, економію ресурсів, залучення нових фахівців, підготовку персоналу й т.д. Груповий підхід до організації робіт приносить значний економічний ефект, створює умови для підвищення продуктивності праці в кілька разів.

Раціональне планування робочих місць, висока організація виробництва й зборки різко скорочують час на транспортування й складальні операції. Так звані

операційні центри зменшують час зборки більш ніж в 10 разів при використанні тих же інструментів.

Оцінка ролі управлінської інформації в конкурентній боротьбі, в одержанні переваг над економічними суперниками також дозволяє включити ряд відомостей у цій сфері діяльності підприємства в перелік даних, що складають комерційну таємницю.

Відчутний економічний збиток може нанести розголошення комерційної таємниці на етапі випробування розробленого товару ринком.

Головне в процесі ринкових випробувань - оцінити привабливість його для споживачів. У процесі випробувань необхідно забезпечити захист таких відомостей, які б істотно полегшили прийняття конкурентами відповідних контрзаходів. Як правило, підлягають охороні на цій стадії торговельна марка продукту, назва фірми, що проводить випробування, результати випробувань, час виходу продукту в серійне виробництво й т.п.

Істотне значення для організації успішного збуту продукції має упаковка. Вона виконує функцію захисту товару від ушкоджень. Ефективна конструкція упаковки забезпечує умови для найкращого використання транспорту, застосування погрузочно-розгрузочних механізмів, доставки товару в неушкодженому вигляді на значні відстані, що сприяє освоєнню нових ринків. Упаковка повинна привертати увагу покупця й спонукати його придбати даний товар. По суті, упаковка є самостійним товаром. Тому до комерційної таємниці доцільно відносити відомості, що описують характеристики розроблювальних упаковок, технологію їхнього виготовлення, економічні показники її виробництва й використання.

Важливим етапом дослідження збутової діяльності є аналіз витрат обігу. У якості одного з методів оцінки ефективності збуту використовується прийом зіставлення з аналогічними витратами конкурентів. При цьому виявляються

необґрунтовані витрати, втрати в сфері просування товару до покупця, перевіряється рентабельність систем збуту.

Таке зіставлення робить видимими зайві витрати на реалізацію, створює інформаційні передумови для вироблення заходів по підвищенню конкурентоспроможності даного виду товару. Ці відомості безумовно створюють певні переваги в економічному суперництві й багатьма фірмами вважаються комерційною таємницею.

Для втримання або завоювання позицій на ринку підприємства активно використовують рекламу. При цьому можуть демонструватися промислові зразки, певним чином доводиться інформація про новітні технології й т.п. Важливо не допустити помилок, які можуть призвести до розголошення коштовної інформації, тому що конкуренти, довідавшись її з реклами, можуть внести необхідні корективи в процес конкурентної боротьби.

Випробуваним методом реклами, що забезпечує захист комерційної таємниці, є так званий метод чорного ящика. При цьому описується проблема, показуються досягнуті результати, отримані переваги, але як це досягається, повідомляється в урізаному виді, із крайньою обережністю.

В останні роки в промислово розвинених країнах служби безпеки стали вживати заходів по захисту інформації, що фірми, що суперничають, можуть одержати при аналізі відходів продукції, що надходять в утилізацію або на ринок. Головною формою захисту є збереження в таємниці фірмами, що спеціалізуються на продажі відходів виробництв, відомостей про підприємства-постачальників цієї сировини.

Прибуток в основному залежить від виробничих і ринкових факторів. Тому *великий блок захищаємої інформації відображає специфіку взаємодії виготовлювача (постачальника) і споживача (замовника).*

Розгляд інформаційного відображення процесів виробництва й збуту дозволяє виділити структурні елементи переліку відомостей, що становлять комерційну таємницю підприємства.

Перелік містить у собі наступні блоки інформації:

- виробництво;
- керування виробництвом;
- планування;
- фінансовий стан;
- технологія виробництва;
- НДЕКР, ринкова політика й стан ринку;
- партнери й конкуренти;
- переговори й контракти;
- ціни;
- збут;
- власна безпека підприємства.

Для того, щоб ухвалити рішення щодо включення тих або інших даних про діяльність підприємства в перелік відомостей, що становлять комерційну таємницю, доцільно на першому етапі визначити можливі негативні наслідки у випадку їхнього розголошення.

До негативних наслідків належать:

- розрив ділових відносин з партнерами підприємства;
- зрив переговорів, втрата можливості укладення вигідного контракту;
- зниження рівня співробітництва з діловими партнерами;
- невиконання договірних зобов'язань;
- необхідність проведення додаткових ринкових досліджень;
- відмова від рішень, що стали неефективними в результаті розголошення інформації, і необхідність вживання додаткових заходів, пов'язаних з фінансовими витратами;
- використання конкурентами отриманих відомостей для підвищення ефективності економічного суперництва;
- втрата можливості патентування й продажі ліцензій;
- скорочення витрат конкурентів на проведення НДЕКР, удосконалювання технологій;
- зниження цін на продукцію або обсягів продажу;

- завдання збитків авторитету фірми;
- зниження рівня економічної безпеки;
- випереджальний вивід аналогічного товару на ринок конкурентом;
- погіршення умов одержання кредитів;
- поява труднощів у постачанні, придбанні устаткування;
- звільнення провідних спеціалістів підприємства.

Для того, щоб уникнути необґрунтованої класифікації відомостей, фахівці підприємства повинні керуватися додатковими критеріями віднесення інформації до комерційної таємниці. *Найбільш загальними з них є:*

- одержання виграшу в часі для підприємства порівняно з конкуруючими фірмами;
- унікальність розробки;
- наявність новизни (нова функція споживання, нова технологія, застосування в нових областях);
- переваги техніко-економічних характеристик товару перед виробами конкурента;
- оригінальне застосування матеріалів, технологій; наявність переваг у ціновій конкуренції; значні трудозатрати для одержання інформації; монополії підприємства на інформацію з даного напрямку виробничо-комерційної діяльності;
- ймовірність використання інформації конкурентами у випадку її опублікування;
- перспективи самостійного одержання відомостей, що закриваються, конкурентами і в які строки;
- поява можливості виходу на міжнародний ринок; ступінь впливу на формування в споживачів позитивного подання про фірму;
- можливість забезпечення схоронності на підприємстві інформації у випадку її віднесення до комерційної таємниці.

Структура й утримування переліку залежить від характеристики підприємства. У переліку вказуються строки перегляду віднесених до комерційної таємниці відомостей і перекладу їх у розряд загальнодоступних.

Практика організації захисту інформації показує, що в певних випадках навіть при поставках товару на ринок конкретні відомості про його виробництво й збут можуть досить тривалий час охоронятися як інтелектуальна власність підприємства.

При віднесенні відомостей до комерційної таємниці керуються економічною доцільністю, тому що обмеження на користування інформацією може істотно заважати ефективному функціонуванню підприємства. Відомості зберігаються в таємниці в тому випадку, коли вони є складовою частиною основної якості виробу (наприклад, прилади й пристрої охорони, спеціальні замки, сейфи) або технологія виготовлення товару така, що не дозволяє конкурентові в процесі реконструювання одержати сховані дані.

Джейм Н. А. Кулі у своїй книзі «Комерційна таємниця» рекомендує виділити у виробничо-комерційній діяльності підприємства все те, що відрізняє вас від конкурентів, що вам не хотілося розкривати їм.

Зіставивши список вашої технології й ділової інформації зі схеми, що для вас прийнятна, треба в першу чергу захищати коштовну інформацію, витік якої здатен завдати шкоди, значно перевищуючої витрати на її захист.

При аналізі важливо встановити:

- яка інформація має потребу в захисті;
- кого вона може зацікавити, яка її цінність для конкурентів;
- які елементи інформації найцінніші;
- який строк існування відомостей, що становлять комерційну таємницю;
- у що обійдеться захист.

4 АДМІНІСТРАТИВНО-ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ РЕЖИМУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ НА ПІДПРИЄМСТВІ

4.1 Служба інформаційної безпеки підприємства

У разі, коли підприємство працює із значними обсягами інформації, яка віднесена до комерційної таємниці (КТ), й в додачу до цього збереження та обробка цієї інформації потребує розвиненої інформаційної інфраструктури, зокрема, потужних комп'ютерних систем, складної мережі передачі й т.п., доцільним може виявитися виділення із складу служби безпеки окремого підрозділу – служби захисту інформації (СЗІ) або (альтернативна назва) служби інформаційної безпеки (СІБ).

Простіше за все діяльність цього підрозділу можна було б регламентувати існуючим нормативним документом системи технічного захисту інформації "Типове положення про службу захисту інформації в автоматизованій системі" [12]. Цьому ж сприяє і певний історичний аспект [13]: перші прояви інституалізації систем інформаційної безпеки в Україні виникли у сфері охорони державних секретів та на інженерно-техніко-технологічному рівні у формі організаційно виокремлених підрозділів технічного захисту інформації. Останні інтегрували в собі службу урядового зв'язку та систему протидії іноземним технічним розвідкам, що існували ще за радянських часів. Організаційне оформлення системи технічного захисту інформації співпало у часі з етапом інтенсифікації інформатизаційних процесів в Україні, тому служби захисту інформації в установах, підприємствах та фірмах часто створювалися на базі департаментів чи відділів інформаційних технологій (ІТ) й підпорядковувалися директору з ІТ. Саме ці служби стали зародками служб інформаційної безпеки (ІБ) на локальному рівні (в окремих організаціях) системи інформаційної безпеки. В кадровому відношенні робота цих служб забезпечувалася випускниками технічних навчальних закладів та університетів, фахово орієнтованих на

діяльність в сфері фізико-технічних або інформаційних технологій захисту. Окрему, вузьку й професійно достатньо замкнену групу фахівців складали спеціалісти з криптології. Як зазначалося вище, з функціонально-виробничих міркувань здавалося доцільним розгортання служб ІБ у складі департаменту (відділення) ІТ. Однак з часом виявилися суттєві недоліки такої точки зору.

По-перше, реалізація технологій захисту часто уповільнює і ускладнює роботу користувачів та адміністраторів обчислювальних систем, що призводить до виникнення певних суперечливостей між представниками служб ІТ та ІБ, які, зважаючи на підпорядкованість ІБ служб, вирішуються не на їх користь.

По-друге, хоча ІТ-департамент теж зацікавлений у захисті інформації, його бачення цієї задачі є достатньо вузьким, в межах парадигми суто технічного захисту інформації, тоді як інформаційна безпека організації вимагає більш широкої, масштабної постановки задачі. Ця суперечливість є принциповою. Тому доцільно більш детально проаналізувати завдання служби ІБ. Для інформаційної безпеки організації характерним є органічний взаємозв’язок задач захисту інформації з забезпеченням комерційної та економічної ефективності організації, забезпечення неперервності та захищеності бізнес-процесів (основних функціональних напрямків діяльності організації).

Очевидно, що глобальний розвиток інформаційної сфери робить бізнес вельми вразливим для загроз безпосередньо інформаційного характеру: тільки точна, повна за обсягом, релевантна інформація здатна гарантувати прибутковість бізнесу. Реалізувати ці вимоги можна лише в умовах побудови комплексної системи інформаційної безпеки, яка окрім виключно ІТ-ризиків буде враховувати ризики, пов’язані з кадровою та фізичною безпекою, забезпечення захищеного документообігу, тощо. Зважаючи на те, що за комплексного підходу інтенсивно зростає множина можливих загроз (атак), його практичне застосування має поєднуватися із принципом розумної достатності: неможливо створити абсолютно непереборний захист, тому слід орієнтуватися на певний прийнятний рівень інформаційної безпеки, на якому досягається компроміс між витратами на захист та розміром шкоди від реалізації загроз бізнесу. Впровадити принцип

розумної достатності можливо лише за умов активного захисту [14], що базується на прогностичній випереджувальній стратегії захисту, яка дозволяє передбачити найбільш ймовірні напрямки атак й, відповідно, зосередити на них максимум засобів захисту, реалізувавши таким чином гранично ефективну й одночасно економічну, маловитратну систему комплексного захисту. Очевидно, що цей захист не може бути статичним, він має постійно адаптуватися до змін оточуючого середовища. Це обумовлює необхідність здійснення неперервного управління системою інформаційної безпеки організації, включення до її складу нової ланки, яка за термінологією міжнародних стандартів безпеки отримала назву менеджменту інформаційної безпеки [15,16,17].

Розв'язання задач менеджменту ІБ потребує від спеціалістів служби ІБ, зокрема, її керівного складу, нових вмінь та знань, які виходять за межі традиційної освітянської підготовки з технічного захисту інформації. Це має бути принципово новий тип фахівця, професійно спроможного виконувати великий обсяг специфічної аналітичної роботи, добре обізнаного з сучасними інформаційними технологіями прогнозування, прийняття рішень, обробки даних, представлених якісними змінними, знайомого з принципами системного аналізу та ґрунтовною правовою підготовкою. Тому, зважаючи на зміст викладеного вище (після слів „По-друге...") службу ІБ у ряді випадків підпорядковують департаменту з економічної безпеки організації (установи).

Однак існує досить вагоме „по-третє", яке примушує шукати інше рішення. Це пов'язано з тим, що все частіше до компетенції менеджменту ІБ відносять контроль дій користувачів, моніторинг нелояльних користувачів та потенційних інсайдерів, контроль та налаштування мережевого захисту, моніторинг контенту електронної пошти та пошти миттєвих повідомлень, поточний аудит стану інформаційної безпеки організації, розроблення та реалізацію політики доступу та політики безпеки організації в цілому. Ця діяльність має базуватися на жорсткій правовій основі, а певні дії та, зокрема, результати контролю та моніторингу, можуть носити конфіденційний характер. Тому у ряді випадків доцільним є

виділення служби ІБ у окремий підрозділ, підпорядкований безпосередньо керівництву організації (установи).

Розглянемо детально, які функції має виконувати виділений підрозділ (СІБ).

4.2 Функції СІБ із захисту комерційної таємниці

1) Вироблення критеріїв виділення коштовної інформації, що підлягає захисту.
2) Визначення об'єктів інтелектуальної власності, що підлягають охороні.
3) Вибір методів захисту (патентування, авторське право, комерційна таємниця).
4) Розробка для наступного затвердження переліку (доповнень до переліку) відомостей, що становлять комерційну таємницю (далі - КТ).
5) Установлення правил допуску й розробка дозвільної системи доступу (ДСД) до відомостей, що становлять комерційну таємницю.
6) Оформлення списків осіб (переліків посад) , що мають право працювати з конкретними складовими КТ.
7) Визначення списку посад (осіб), уповноважених класифікувати інформацію.
8) Установлення правил і процедур класифікації, маркування документів, інших носіїв інформації, а також виводу їх зі сфери обмеженого доступу (розсекречення).
9) Розробка й запровадження в дію єдиного порядку обігу з носіями інформації (технологія створення, облік, правила роботи, зберігання, пересилання, транспортування, розмноження, знищення).
10) Складання плану розміщення й обліку приміщень, у яких після відповідної атестації дозволене постійне або тимчасове зберігання носіїв КТ, робота з ними. Установлення єдиного порядку проходу в ці приміщення.
11) При особистій участі керівників структурних підрозділів і фахівців, що

мають доступ до КТ, планування, здійснення й контроль за реалізацією заходів при проведенні всіх видів робіт, у яких використовується закрита інформація, класифіковані носії.

12) Надання методичної допомоги керівникам підрозділів підприємства в розробці й здійсненні заходів захисту відомостей у процесі наукової, конструкторської, виробничої й іншої діяльності (які технологічні заходи безпеки необхідно використовувати; які зміни в технологію треба ввести; які вимоги доцільно включити в умови контракту; яку інформацію доцільно захищати навіть при виході товару на ринок і т.п.).
13) Розробка й здійснення спільно з фахівцями заходів по недопущенню розголошення КТ на стадіях:
    - оформлення матеріалів, призначених для опублікування у відкритій пресі, для використання на конференціях, виставках, в рекламній діяльності (аналогічні заходи здійснюються відносно зразків виробів, що містять КТ);
    - оформлення документів (зразків) для передачі замовникові (співвиконавцеві) .
14) Організація при участі керівників і фахівців підприємства захисних заходів при випробуваннях, зберіганні, транспортуванні, знищенні продукції, що містить КТ.
15) Розробка порядку й контроль за проведенням закритих нарад.
16) Визначення режимних заходів прийому представників інших фірм, відряджених осіб, представників контрольних органів влади.
17) Участь спільно з фахівцями підприємства в розробці заходів по забезпеченню безпеки в процесі використання технічних засобів передачі інформації, - ЕОМ (ПЕОМ), а також системи протидії технічним коштам промислового шпигунства.
18) Організація охорони підприємства, спецприміщень, сховищ, введення пропускного й внутріоб'єктового режиму (розмежування доступу в приміщення).
19) Формування пропозицій на установку технічних засобів охорони (ТЗО),

організація робіт з їхнього монтажу, експлуатації й ремонту.

20) Участь у підборі й розміщенні співробітників, що допускаються до КТ, виробленню заходів по зниженню плинності кадрів.
21) Розробка положень, інструкцій, правил, методик і т.п. по забезпеченню режиму роботи для виконавців закритих робіт фахівців СБ (недосконалість розроблених норм - одна з головних обставин витоку).
22) Організація й участь у навчанні осіб, допущених до КТ (складання програми навчання, прийом заліків по знанню відповідних вимог режиму).
23) З урахуванням конкретної обстановки разом з керівниками підрозділів у процесі організаційної й профілактичної роботи формування на плановій основі в співробітників свідомого відношення до забезпечення захисту інформації.
24) Розробка заходів по попередженню несанкціонованого знищення носіїв інформації, у тому числі в автоматизованих системах зберігання, обробки й передачі інформації.
25) Контроль виконання режимних вимог: проведення аналітичних досліджень по оцінці надійності прийнятих заходів захисту КТ і вироблення пропозицій по підвищенню ефективності охорони.
26) Проведення службових розслідувань по фактах порушення режиму поводження із КТ.
27) Організація взаємодії зі Службою безпеки України в сфері міжнародного економічного співробітництва й спільного підприємництва.

Крім того, СІБ має забезпечити певну специфічну складову інформаційної діяльності підприємства.

4.3 Інформаційне забезпечення діяльності підприємства з боку СІБ

1. Участь в підготовці і проведенні спеціальних інформаційних акцій, що

підвищують репутацію фірми в очах партнерів, громадськості, органів влади (у тому числі і відносно СІБ по формуванню у оточення переконання в силі і ефективності її діяльності по захисту).

2. Сумісне з іншими підрозділами підприємства отримання аналітичним шляхом інформації про конкурентів, в частині, що стосується можливої підготовки і здійснення ними заходів несумлінної конкуренції і виробітку заходів по їх нейтралізації.
3. Планування організації збору, оцінки інформації на користь забезпечення стабільної і ефективної діяльності підприємства (перелік питань, по яких необхідний збір інформації, хто, як, коли її збирає).
4. Розробка заходів по накопиченню, зберіганню, користуванню, прискореному доведенню до виконавців цінної інформації, зокрема класифікованих документів і відомостей.
5. Інформаційне забезпечення діяльності СІБ в частині отримання даних про підготовлювані посягання на інтереси підприємства.
6. Отримання і узагальнення відкритих публікацій з питань організації інформаційної безпеки підприємств і розробка на цій основі пропозицій.

Вибравши з приведеного переліку функції, виконання яких забезпечувало б надійний захист підприємства (фірми), керівник визначає кількісний склад і структуру СІБ.

Директором підприємства СІБ можуть надаватися наступні права:

1) вносити керівнику підприємства пропозиції про заборону робіт з документами, що становлять комерційну таємницю, а також зміну порядку зберігання або перевезення товарів, інших цінностей при виявленні порушень, які можуть спричинити нанесення економічного збитку;
2) виходити з клопотанням про усунення конкретних виконавців підприємства (фірми) від ведення закритих робіт, переговорів з іншими фірмами, перевезення, зберігання, охорона майнової власності;

3) контролювати із залученням фахівців підприємства стан і надійність захисту закритих робіт і охорони майна, грошових засобів;
4) погоджувати заходи, що розробляються підрозділами перед прийняттям, в цілях забезпечення інформаційної безпеки;
5) давати в рамках своєї компетенції керівникам підрозділів і виконавцям обов'язкові для виконання рекомендації; проводити з питань режиму навчання і інструктажі співробітників;
6) за наказом директора підприємства (фірми) брати участь або проводити самостійно розслідування фактів розголошувань комерційної таємниці, втрати документів і виробів, розкрадань товарів, інших цінностей, а також грубих порушень встановленого режиму комерційної таємниці підприємства.

Рішення і організаційно-розпорядчі документи з питань відносин СІБ з іншими підрозділами підприємства при необхідності оформляються наказами директора. Підрозділи СІБ повинні мати достатньо великі повноваження і прирівнюватися до прав і обов'язків основних структурних підрозділів підприємства. Про наявність такого підрозділу його повноваження повинні знати всі співробітники підприємства. Це пояснюється перш за все тим, що навіть не працюючий з комерційною таємницею співробітник підприємства може стати носієм цінної інформації, що вимагає негайного захисту.

СІБ підкоряється безпосередньо керівнику підприємства і створюється відповідно до його наказу. Вона є структурною одиницею підприємства й безпосередньо бере участь у виробничо-комерційній діяльності. Її робота проводиться у взаємодії із структурними підрозділами підприємства.

Структура і штати СІБ залежно від об'єму робіт і особливостей виробничо-комерційної діяльності визначаються керівником підприємства і, як правило, повинні комплектуватися інженерно-технічними працівниками – фахівцями основного профілю роботи даного підприємства (фірми), а також фахівцями, що мають практичний досвід у області захисту інформації або оперативної, кадрової, керівної чи виховної роботи з різними групами людей. Рішення про призначення на

посаду начальника (заступника начальника) служби безпеки підприємства (фірми), а також його звільнення приймається тільки керівником підприємства.

Ці та інші вимоги вносять в положення про СІБ, яке розробляється по вказівці директора.

При виконанні покладених на СІБ задач її співробітники використовують в своїй роботі різні форми і методи: видання організаційно-розпорядчої і методичної документації, проведення в підрозділах підприємства комплексних і цільових перевірок, заслуховування звітів керівників відповідного рівня про стан режиму в підрозділі, різні форми і методи профілактичної роботи і т.п.

Керівник СІБ щорічно звітує про свою роботу перед директором підприємства.

Приступаючи до розробки системи заходів по забезпеченню інформаційної безпеки підприємства, його керівник або начальник СІБ повинні одержати відповіді на наступні питання:

1. Що конкретно необхідно захищати (охороняти), від кого, як і коли?
2. Хто організовує і забезпечує захист (охорону)?
3. Як оцінювати ефективність і достатність захисту (охорони)?

Для ілюстрації розглянемо етапи організації системи захисту комерційної таємниці.

1. Визначається предмет захисту. Розробляється перелік відомостей, що становлять комерційну таємницю, в якому виділяється найбільш цінна інформація, що вимагає особливої охорони, враховуються вимоги по захисту інших підприємств (фірм), що беруть участь в спільних роботах.
2. Встановлюються періоди існування конкретних відомостей як комерційна таємниця.
3. Виділяються категорії носіїв цінної інформації: персонал, документи, вироби і матеріали; технічні засоби зберігання, обробки і передачі інформації; фізичні випромінювання. Для забезпечення сприйняття можна скласти схему, в якій

вказуються конкретні з працівниками, обізнаними в комерційній таємниці, назви (категорії) класифікованих документів і виробів і т.п.

4. Перераховуються стадії (етапи робіт), час матеріалізації комерційної таємниці в носіях інформації стосовно просторових зон (місцям роботи з ними всередині і за межами підприємства).
5. Складається схема роботи і передбачуваного переміщення конкретних відомостей, матеріалізованих в носіях, в просторі підприємства (фірми) і поза ним.

Розглядаються можливі для підприємства несанкціоновані переміщення, які можуть бути використані конкурентами для отримання комерційної таємниці.

6. Розробляються (або коректуються) в процесі аналізу дозвільні підсистеми допуску і доступу до конкретних відомостей, що становлять комерційну таємницю.
7. Визначається, хто реалізує заходи і хто несе відповідальність за захист конкретної інформації, процесів робіт з класифікованими даними. Намічаються заходи з координації, призначаються відповідальні виконавці.
8. Плануються дії з активізації і стимулюванню осіб, задіяних в захисті.
9. Перевіряється надійність вжитих до реалізації заходів захисту.

Аналіз стану ефективності інформаційної безпеки включає:

- вивчення і оцінку фактичного стану;
- виявлення недоліків і порушень режиму, які можуть привести до втрати фізичних носіїв таємниці (цінного майна) або розголошування комерційної таємниці;
- встановлення причин і умов виявлення недоліків і порушень;
- вироблення пропозицій, направлених на усунення недоліків і запобігання порушенням.

Об'єктами контролю і аналізу можуть бути:

- дотримання норм, правил зберігання і охорони в приміщеннях,

спецсховищах, на робочих місцях;

- ведення обліку і забезпечення особистої відповідальності за виконання цієї функції;
- дотримання порядку зберігання, відбору і знищення;
- дотримання вимог порядку обігу;
- заходи по запобіганню несанкціонованому винесенню носіїв комерційної таємниці за територію підприємства;
- дотримання режиму і охорони при транспортуванні, розсилці, переносі, доставці;
- організація доступу до інформації, осіб відряджених на підприємство;
- організація проведення нарад, виставок, переговорів і т.п.;
- рівень знань вимог режиму особами, допущеними до закритих робіт і документів;
- ступінь забезпеченості служби безпеки надійними сховищами, замикаючими пристроями, засобами опечатування;
- забезпеченість співробітників відповідними робочими місцями для роботи з носіями секретів;
- стан пропускного і внутрішнього режиму в будівлях, приміщеннях, в цілому на підприємстві;
- механізм розподілу носіїв комерційної таємниці за рівнями виконання і управління;
- обгрунтованість доступу конкретних груп співробітників до різних видів носіїв;
- порядок поводження з носіями на робочих місцях;
- порядок користування засобами отримання, обробки, зберігання, відображення і передачі інформації;
- порядок обміну відомостями усередині підприємства і із зовнішніми партнерами;
- своєчасність і правильність класифікації і розкриття відомостей;
- організація і проведення виставок, конференцій, симпозіумів і т. д.;

- якість розробки організаційно-методичних документів, виконання планів робіт і спеціальних заходів щодо захисту інформації;
- рівень і повнота виконання вимог керівництва підприємства;
- стан профілактичної роботи із співробітниками;
- рівень організаційно-методичного забезпечення взаємодії між підрозділами;
- час пошуку і доведення інформації до виконавців.

Аналіз включає також моделювання вірогідних каналів просочування інформації, можливих прийомів і способів несанкціонованого отримання закритої інформації.

Іноземні фірми до числа найвірогідніших каналів просочування класифікованої інформації відносять:

- спільну з іншими фірмами діяльність, участь в переговорах;
- фіктивні запити про можливість працювати у фірмі на різних посадах;
- екскурсії і відвідини фірми;
- повідомлення торгових представників фірми про характеристики виробу;
- надмірну рекламу;
- поставки суміжників;
- консультації зовнішніх фахівців, які внаслідок цього отримують доступ до устаткування і документів фірми;
- публікації у пресі і виступи;
- наради, конференції, симпозіуми і т. п.;
- розмови в неробочих приміщеннях;
- скривджені фірмами співробітники.

Слід враховувати також можливі *методи і способи збору інформації:*

- опитування при особистій зустрічі;
- нав'язування дискусій по проблемах, що цікавлять;
- розсилка на адреси підприємств і окремих фахівців запитальників і анкет;

- ведення приватного листування наукових центрів і учених із спеціалістами фірми.

В цілях збору відомостей у ряді випадків використовуються переговори, що проводяться для визначення перспектив співпраці, створення спільних підприємств.

Наявність такої форми співпраці як виконання сумісних програм, що передбачають безпосередню участь представників інших організацій в роботі з документами, відвідини робочих місць, розширюють можливість для зняття копій документів, збору різних зразків матеріалів, проб і т.д. Найімовірніше можуть бути використані наступні *способи отримання інформації:*

- візуальне спостереження;
- підслуховування;
- технічне спостереження;
- пряме опитування, вивідування;
- ознайомлення з матеріалами, документами, виробами і т. д.;
- збір відкритих документів і інших джерел інформації;
- розкрадання документів і інших джерел інформації;
- вивчення джерел інформації, що містять по частинах необхідні відомості.

При необхідності плануються додаткові заходи захисту. Оцінюється реальність їх виконання, наявність методичного матеріалу, матеріального забезпечення, готовності персоналу і служби безпеки їх виконати. При плануванні враховуються недоліки в забезпеченні збереження комерційної таємниці, що мали місце на підприємстві.

Заплановані заходи захисту повинні:

- сприяти досягненню певних задач, відповідати загальному задуму;
- не суперечити законам, вимогам керівника фірми (інтересам фірм, що кооперуються);
- бути оптимальними;

- не дублювати інші дії.

При плануванні враховуються цілі, інтереси і можливості задіяних підрозділів.

Організація системи захисту має адаптуватися до обстановки на фірмі. У зв'язку з цим вкрай важливий облік та врахування принципових і вірогідних змін в цій обстановці.

4.4 Соціально-психологічні особливості управління співробітниками, що працюють з комерційною таємницею

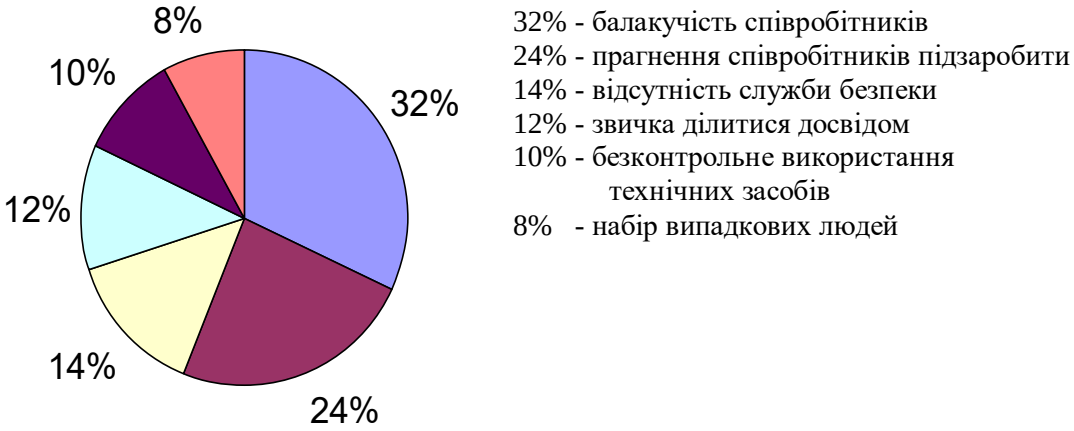
Чітко діюча на підприємстві система режиму доступу до інформації, забезпечує передачу конкретним особам тільки такого об'єму інформації, який їм необхідний для виконання своїх службових обов'язків, знижує рівень вірогідного збитку під час переходу співробітника в конкуруючу фірму. Наявність обмеженого об'єму відомостей також не спонукає до звільнення для подальшого використовування їх на новому місці роботи.

Проте світовий досвід захисту виробничо-комерційних секретів фірм показує, що суто адміністративними способами гарантувати позитивний результат не представляється можливим. Тому підприємці, удосконалюючи організаційно-адміністративні заходи, все активніше переходять до поєднання їх з інтенсивним залученням в процес захисту всіх співробітників фірми.

Фахівці із захисту інформації наводять дані, підтверджуючі, що визначальною фігурою в забезпеченні збереження цінних відомостей підприємства (фірми) є його співробітник. Так, вірогідність витоку відомостей, що становлять комерційну таємницю, при проведенні таких дій, як підкуп, шантаж, переманювання службовців фірми, упровадження на підприємство промислового шпигунства дорівнює 43 %; отримання відомостей шляхом їх вивідування у співробітників – 24 %; проникнення в ПЕОМ – 18 %; крадіжка документації – 10 %; підслуховування телефонних переговорів – 5 % [13].

За даними експертів ЄС, ефективність способів економічного шпигунства (розвідки) і умови витоку комерційної таємниці приведені відповідно на діаграмах I і II :

Діаграма I



Діаграма II

Було б неправильним зосереджувати увагу служб безпеки в роботі з персоналом підприємства (фірми) тільки на особах, що працюють із закритою інформацією. Співробітник, що не має доступу до комерційної таємниці, може надати допомогу конкуруючій фірмі в проведенні електронного промислового шпигунства, забезпечити умови для розкрадання носіїв інформації, зняття копій тощо.

Персонал підприємства (фірми) є, з одного боку, найважливішим ресурсом підприємницької діяльності, виступаючим як творець матеріальних і інтелектуальних

цінностей, а з іншого – конкретні співробітники через різні обставини можуть стати джерелом масштабних втрат і навіть його банкрутства.

Найважливішим напрямом захисту комерційної таємниці підприємства (фірми) є *стабільність кадрового складу.* Якщо склад кваліфікованих фахівців змінюється через високу текучість, цінні розробки фірми будуть ставати безкоштовним надбанням конкурентів. Технологічні процеси дозволяють працівникам, що звільнилися, безпосередньо конкурувати з своїми колишніми наймачами.

Велику тривогу в розвинених країнах викликає *практика переманювання інженерів і науковців*, що широко розповсюджується, *конкуруючими фірмами.* Цей метод добування виробничих секретів є не тільки кращим способом отримання цінної інформації, але і серйозно ослаблює підприємство. Переманювання співробітників може привести до істотного скорочення або втрати можливостей фірми брати участь в конкурентній боротьбі.

Таким чином, конкурентні відносини, суперництво між підприємствами (фірмами) можуть сформувати бажання удатися до промислового шпигунства щоб паралізувати виробництво протилежної сторони і підвищити конкурентоспроможність.

5 АДМІНІСТРАТИВНО - ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

5.1 Завдання захисту при атаках соціальної інженерії

Серед сучасних завдань безпеки протидія атакам соціальної інженерії та управління безпекою, пов'язане з такими атаками, посідає одне з ключових місць. Це пов'язане із тим, що атаки соціальної інженерії, як правило, є типовим початком кібератак на інфраструктуру підприємств, в тому числі і критичної інфраструктури [22]. Адміністративно-організаційні заходи захисту від атак соціальної інженерії спрямовані на створення у компанії системи управління безпекою, в якій ризики, пов'язані з маніпулятивними методами впливу на персонал, мінімізуються за рахунок формалізації процедур, підвищення обізнаності працівників та чіткої організації процесів. Атаки соціальної інженерії можуть мати місце на різних етапах, у різних ланках ланцюга постачання [23], і відповідні ризики повинні бути враховані при управлінні інформаційною безпекою.

Першочерговим завданням є розробка та впровадження *політики інформаційної безпеки*, що містить окремий розділ, присвячений протидії соціальній інженерії. У цьому документі слід визначити, які саме види атак (фішинг, вішинг, смішинг, фізичні методи на кшталт шолдер-серфінгу) розглядаються як загрози для організації, та встановити чіткі правила поведінки у випадку їх виявлення. Окремо мають бути затверджені інструкції для співробітників із покроковим алгоритмом дій при отриманні підозрілих електронних листів, телефонних дзвінків чи особистих запитів. Важливим компонентом є регламент підтвердження особи запитувача, що може передбачати, наприклад, двофакторну перевірку при зверненні щодо зміни фінансових реквізитів або доступу до конфіденційних даних.

Організаційна структура підприємства повинна включати чітко визначених відповідальних осіб або підрозділи, які координують роботу щодо виявлення та

запобігання атакам соціальної інженерії. Як правило, цю роль виконує CISO (Chief Information Security Officer) або служба інформаційної безпеки. Для ефективності роботи необхідно закріпити розподіл обов'язків: хто здійснює первинну перевірку інциденту, хто проводить розслідування, а хто організовує заходи з навчання та профілактики. Також важливо передбачити механізм звітності, що визначає порядок та канали повідомлення про підозрілі ситуації.

Не менш значущим є системне *навчання персоналу* та підвищення їх обізнаності. Для цього організовуються регулярні тренінги, на яких співробітникам демонструють реальні приклади атак і пояснюють механізми маніпуляцій. Позитивний ефект мають імітаційні фішинг-кампанії, під час яких працівників навчають виявляти та правильно реагувати на підозрілі повідомлення. Візуальні нагадування у вигляді постерів або екранів-заставок із порадами безпеки допомагають підтримувати уважність у повсякденній роботі. Особливу увагу слід приділяти інструктажу нових працівників ще до початку виконання ними службових обов'язків.

Важливим адміністративним елементом є регламентація *службових комунікацій*. Запроваджується принцип «довіряй, але перевіряй», коли будь-які критично важливі запити перевіряються по альтернативних каналах зв'язку. Має бути визначений єдиний офіційний канал для обміну конфіденційною інформацією, а використання особистих акаунтів або несанкціонованих месенджерів для робочих питань забороняється.

Організаційні заходи тісно пов'язані з *контролем доступу*. Використовується принцип найменших привілеїв, коли працівник має доступ лише до тих ресурсів, які необхідні йому для виконання службових обов'язків. Права доступу регулярно переглядаються, особливо після зміни посад або звільнення співробітників. Для входу до критичних систем застосовується мультифакторна автентифікація, що ускладнює несанкціоноване використання облікових записів навіть у разі компрометації пароля.

Необхідно мати *план реагування на інциденти*, у якому передбачено порядок дій при виявленні атаки соціальної інженерії. Він повинен включати

ведення журналу інцидентів, аналіз кожного випадку та, за потреби, взаємодію з правоохоронними органами. Це дозволяє не лише ліквідувати наслідки, а й накопичувати знання для подальшої профілактики.

Регулярний *контроль та аудит* процесів – ще один ключовий адміністративний інструмент. Внутрішні перевірки дозволяють оцінити, наскільки персонал дотримується встановлених політик, а також виявити слабкі місця в існуючих заходах. Паралельно проводиться оцінка ризиків з урахуванням соціальної інженерії, щоб адаптувати заходи безпеки до нових загроз.

Зрештою, важливо формувати *культуру безпеки* в колективі. Це означає створення атмосфери, в якій співробітники не бояться повідомляти про підозрілі інциденти, розуміють власну роль у захисті компанії та дотримуються принципу відповідального поводження з інформацією. Запровадження політики «zero blame» за повідомлення про власні помилки дозволяє уникнути замовчування інцидентів та сприяє своєчасному реагуванню. Корисним є також розвиток психологічної стійкості працівників до маніпуляцій шляхом спеціальних тренінгів, які навчають розпізнавати та нейтралізовувати емоційний тиск.

Таким чином, адміністративно-організаційний захист від соціальної інженерії є багаторівневим процесом, який поєднує регламентацію, навчання, технічну підтримку та формування безпечної корпоративної культури. Лише інтеграція цих складових у щоденну роботу організації дозволяє суттєво знизити ймовірність успішної атаки.

5.2 Рекомендації та вимоги щодо захисту при атаках соціальної інженерії згідно ISO/IEC 27001

Захист від атак соціальної інженерії в рамках вимог ISO/IEC 27001 ґрунтується на комплексному підході, який поєднує управління ризиками, формування політик, організаційні заходи, навчання персоналу та постійний контроль ефективності. Організація повинна офіційно визнати соціальну

інженерію як один із значущих класів загроз, оцінити рівень ризику та впровадити заходи, спрямовані на зменшення ймовірності їх реалізації.

Важливим елементом є створення політики інформаційної безпеки, яка чітко визначає правила поводження з інформацією, порядок підтвердження особи при обміні даними, а також вимоги до безпечної взаємодії як усередині компанії, так і з зовнішніми партнерами. Керівництво повинно підтримувати культуру безпеки, виділяти ресурси на протидію маніпулятивним технікам та заохочувати персонал до обережної поведінки.

Ключову роль відіграє робота з людським фактором. Працівники мають бути компетентними в питаннях інформаційної безпеки та регулярно проходити навчання, спрямовані на розпізнавання фішингу, вішингу, смішингу та інших методів психологічного впливу. Доцільно проводити тренінги з реальними прикладами атак, а також періодично здійснювати симуляційні перевірки у формі тестових фішингових кампаній, щоб закріпити навички реагування.

Управління доступом до інформаційних ресурсів повинно будуватися на принципі мінімально необхідних привілеїв, а автентифікація – доповнюватися багатофакторними механізмами. Необхідно впроваджувати засоби захисту від шкідливого програмного забезпечення, у тому числі від вкладень та посилань, які часто використовуються у фішингових атаках. Важливо також регламентувати канали передавання інформації, надаючи перевагу лише захищеним способам обміну та забороняючи використання несанкціонованих інструментів.

Організація повинна мати чітко визначені процедури реагування на інциденти, включно з механізмами повідомлення про підозрілі дії та планом локалізації наслідків атак. Кожен інцидент слід фіксувати, аналізувати та використовувати отримані висновки для вдосконалення заходів безпеки.

Важливою складовою є робота з постачальниками та підрядниками – під час взаємодії з ними необхідно передбачати процедури перевірки достовірності запитів та осіб, що звертаються, аби уникнути атак через зовнішні канали.

Окрему увагу слід приділяти управлінню людськими ресурсами на всіх етапах – від перевірки кандидатів перед прийомом на роботу, через ознайомлення

з вимогами безпеки під час трудової діяльності, до своєчасного відкликання доступів після звільнення.

Реалізація цих заходів у комплексі дозволяє не лише зменшити вразливість до соціальної інженерії, але й сформувати стійку систему, де персонал розглядається як активний елемент захисту, а не як найслабша ланка. ISO/IEC 27001 у цьому контексті забезпечує рамкову основу, в межах якої організація може побудувати багаторівневий захист, орієнтований на мінімізацію впливу людського фактору та підтримку високого рівня інформаційної безпеки.

5.3 Рекомендації та вимоги щодо захисту при атаках соціальної інженерії згідно NIST SP 800-53

Захист від атак соціальної інженерії у вимогах NIST розглядається як багаторівневий процес, у якому ключовими є управління людським фактором, формалізація процедур реагування та безперервне підвищення обізнаності персоналу. NIST підходить до цього більш деталізовано, ніж ISO/IEC 27001, розбиваючи вимоги на чіткі контрольні сімейства, кожне з яких містить конкретні механізми протидії маніпуляціям та шахрайським діям.

Однією з базових вимог є впровадження комплексної програми навчання та обізнаності у сфері кібербезпеки. NIST рекомендує проводити регулярні тренінги, що охоплюють не лише загальні питання безпеки, а й окремо сфокусовані модулі з розпізнавання фішингу, вішингу, смішингу, шахрайських телефонних дзвінків і спроб несанкціонованого доступу через особисті контакти. Велика увага приділяється тестуванню співробітників шляхом імітаційних атак і подальшому аналізу результатів для виявлення слабких місць.

NIST підкреслює важливість політик, які регламентують обмін інформацією, підтвердження особи співрозмовника та порядок виконання критичних запитів. Вимоги передбачають створення стандартних процедур для перевірки достовірності вхідних комунікацій, зокрема через альтернативні

канали, а також впровадження принципу «need-to-know» для доступу до конфіденційної інформації.

Особлива увага приділяється управлінню автентифікацією та захистом облікових даних. NIST рекомендує застосування багатофакторної автентифікації, динамічного моніторингу використання облікових записів та негайного відкликання доступу після зміни ролі або звільнення співробітника. Це тісно пов’язано з тим, що значна частина атак соціальної інженерії спрямована саме на компрометацію облікових даних.

Ще однією особливістю є інтеграція захисту від соціальної інженерії в процеси реагування на інциденти. NIST детально описує необхідність фіксації кожного випадку, що може бути пов’язаний із маніпуляціями, швидкого аналізу ситуації та коригування політик і тренінгів на основі отриманих уроків.

На відміну від ISO/IEC 27001, підхід NIST є більш операційно орієнтованим і містить конкретні технічні та організаційні контрольні заходи з прив’язкою до процедур і метрик. Якщо ISO більше задає рамки та залишає організації свободу у виборі інструментів, то NIST фактично пропонує «чекліст» із визначеними вимогами та рівнями зрілості впровадження.

Ще однією відмінністю є те, що NIST більш явно інтегрує питання соціальної інженерії в управління ланцюгом постачань та взаємодією з зовнішніми сторонами. У рекомендаціях прописані вимоги до перевірки контрагентів, безпечної комунікації з ними та контролю дій підрядників, які можуть стати об’єктами атак або каналом проникнення.

Таким чином, NIST пропонує більш деталізовану і процедурно насичену модель протидії соціальній інженерії. Вона зосереджується на регулярному тренуванні персоналу, жорсткій регламентації комунікацій, посиленому управлінні доступами та безперервному аналізі інцидентів. На відміну від ISO/IEC 27001, де основний акцент робиться на створенні системи управління інформаційною безпекою в цілому, підхід NIST є більш практико-орієнтованим і може бути використаний як докладний інструмент впровадження конкретних заходів у цій сфері.

5.4 Види атак соціальної інженерії та рекомендовані заходи захисту. Ролі працівників в системі захисту

Атаки соціальної інженерії охоплюють широкий спектр методів, спрямованих на те, щоб обманом або маніпуляцією змусити людину розкрити конфіденційну інформацію, виконати небезпечну дію чи надати доступ до ресурсів, які у звичайних умовах залишилися б захищеними. Одним із найпоширеніших різновидів є фішинг, коли зловмисники надсилають електронні листи, що маскуються під повідомлення від відомих організацій або колег, щоб змусити отримувача перейти за шкідливим посиланням або відкрити заражене вкладення. Захист у цьому випадку передбачає використання фільтрів електронної пошти, технологій аналізу вмісту повідомлень, двофакторної автентифікації для доступу до облікових записів, а також регулярне навчання персоналу з виявлення ознак підроблених листів.

Іншою формою є вішинг – телефонні дзвінки, під час яких атакуючі, видаючи себе за працівників банку, технічної підтримки чи керівництво компанії, намагаються отримати паролі, коди підтвердження або іншу критично важливу інформацію. Ефективними контрзаходами є чіткі внутрішні процедури підтвердження особи, заборона передавання конфіденційних даних телефоном без незалежної перевірки запиту та використання скриптів безпечної комунікації для співробітників, які обробляють дзвінки.

Смішинг це аналог фішингу у форматі SMS чи повідомлень у месенджерах, де користувачеві пропонують перейти за посиланням або встановити мобільний додаток, який насправді є шкідливим. Захист тут включає налаштування мобільних пристроїв на блокування підозрілих посилань, використання корпоративних мобільних політик, а також роз’яснення працівникам, що ніколи не слід завантажувати додатки з неперевірених джерел чи переходити за сумнівними URL.

Пре-текстинг полягає у створенні зловмисником детальної легенди, яка виглядає правдоподібно та змушує жертву надати інформацію або виконати дію. Наприклад, атакуючий може представитися представником служби безпеки чи партнерської компанії, посилаючись на вигадані, але правдоподібні обставини. Захист від цього виду атак базується на суворих процедурах перевірки повноважень, незалежній верифікації будь-яких запитів та мінімізації розкриття внутрішньої інформації в публічному просторі, щоб зменшити можливість створення правдоподібного легендування.

Метод “baiting” або “приманки” використовує фізичні або цифрові носії інформації, наприклад флеш-накопичувачі з привабливою етикеткою, залишені у місцях, де їх знайдуть співробітники. При підключенні такого носія до комп’ютера відбувається зараження системи. Захист тут полягає у впровадженні політики заборони використання невідомих носіїв, технічному блокуванні автозапуску та налаштуванні системного моніторингу для виявлення аномальної активності при підключенні пристроїв.

Tailgating або “прохід за кимось” передбачає фізичне проникнення на охоронювану територію, коли зловмисник слідує за працівником, який має право доступу, розраховуючи на ввічливість чи неуважність. Запобігти цьому можна за допомогою впровадження турнікетів та систем контролю доступу, навчання персоналу не впускати сторонніх без перевірки, а також організації охорони, яка контролює вхідні зони.

Ще одним поширеним методом є shoulder surfing – спостереження за введенням паролів чи конфіденційних даних через плече або з відстані. Для протидії слід використовувати захисні екрани для моніторів, розташовувати робочі місця так, щоб ускладнити сторонній огляд, та привчати персонал прикривати клавіатуру під час введення даних.

Загалом захист від соціальної інженерії ґрунтується на поєднанні технологічних та організаційних заходів, відповідні підходи розглядались у роботах [25-27]. Технічні рішення, такі як фільтри контенту, системи виявлення вторгнень, багатофакторна автентифікація та обмеження доступу, повинні

доповнюватися адміністративними заходами: політиками безпечної комунікації, процедурами перевірки запитів, регулярними тренінгами та симуляційними атаками. Найважливішим залишається формування культури безпеки, коли кожен співробітник усвідомлює свою роль у захисті інформаційних активів і здатен розпізнати спробу маніпуляції на ранній стадії.

Ефективний захист від атак соціальної інженерії потребує залучення різних категорій персоналу, адже ця загроза стосується не лише IT-фахівців чи відділу безпеки, а фактично кожного працівника організації. У першу чергу ключову роль відіграє керівництво компанії. Воно відповідає за формування стратегії інформаційної безпеки, виділення ресурсів, затвердження політик і створення культури, де безпека розглядається як спільна відповідальність. Підтримка з боку топ-менеджменту забезпечує легітимність усіх заходів і стимулює їх виконання на всіх рівнях.

Важливою ланкою є служба інформаційної безпеки або CISO, яка здійснює координацію всієї діяльності, пов’язаної з протидією соціальній інженерії. Ця роль включає розробку та впровадження політик, організацію навчання, проведення тренувальних атак, аналіз інцидентів і вдосконалення процедур. Служба також відповідає за взаємодію з іншими підрозділами та зовнішніми партнерами з питань безпеки.

Підрозділ IT підтримує технічну сторону захисту: налаштовує фільтри електронної пошти, впроваджує багатофакторну автентифікацію, обмежує використання зовнішніх носіїв, контролює доступ до мережі, а також забезпечує оновлення програмного забезпечення для закриття вразливостей, якими можуть скористатися зловмисники після успішної атаки на персонал.

Відділ кадрів має інтегрувати вимоги з інформаційної безпеки в процеси управління персоналом: перевіряти кандидатів перед прийомом на роботу, включати інструктажі з безпеки в програму адаптації новачків, контролювати підписання угод про нерозголошення та забезпечувати своєчасне відкликання доступів після звільнення або зміни посади.

Рядові працівники, незалежно від функцій, є першою лінією оборони. Вони повинні вміти розпізнавати ознаки фішингу, вішингу, смішингу, фізичних маніпуляцій та повідомляти про підозрілі випадки без страху покарання. Для цього необхідно проводити регулярні тренінги та надавати чіткі алгоритми дій у різних ситуаціях.

Щодо документів, політики управління інформаційною безпекою щодо соціальної інженерії слід відобразити у кількох основних джерелах. Базовим документом є загальна політика інформаційної безпеки, яка визначає принципи, підходи та цілі захисту, у тому числі від маніпулятивних атак. Доцільно розробити окрему політику або процедуру реагування на атаки соціальної інженерії, де детально описані сценарії, порядок верифікації запитів, правила обміну інформацією та механізми повідомлення про інциденти.

Також варто інтегрувати відповідні положення в політику управління доступом, регламент безпечної роботи з електронною поштою та месенджерами, інструкції з фізичної безпеки та процедури управління інцидентами. У сфері кадрів ці вимоги слід закріпити у положеннях про адаптацію персоналу, програмах навчання та договорах про конфіденційність.

Комплексний підхід передбачає, що кожна роль в організації має чітко визначені обов’язки у захисті від соціальної інженерії, а всі необхідні правила закріплені в офіційних документах і регулярно оновлюються відповідно до актуальних загроз. Саме поєднання формалізованих політик, навчання та міжпідроздільної взаємодії створює середовище, де людський фактор стає сильним елементом захисту, а не вразливістю.

HR – перевірки кандидатів на посаду при наймі є важливою запорукою здорового та безпечного контингенту працівників.

Щоби мінімізувати ризик найму соціального інженера або зловмисного інсайдера, підхід до перевірки кандидата повинен бути комплексним, поєднувати юридично допустимі перевірки, психологічну оцінку та ретельний аналіз минулої діяльності.

Найперше, важливо здійснити перевірку особи та підтвердження автентичності наданих документів, включно з паспортними даними, ідентифікаційними кодами та іншими офіційними посвідченнями. Це дозволяє виключити випадки підробленої або викраденої особистості.

Далі необхідно перевірити історію працевлаштування. Це не просто звірка з резюме, а й підтвердження інформації безпосередньо у попередніх роботодавців, із фокусом на причини звільнення, репутацію, дисциплінарні порушення та будь-які випадки, що можуть свідчити про ненадійність або зловмисні дії. Особливо важливо виявити невідповідності або прогалини в трудовій історії, які кандидат не може логічно пояснити.

Важливим етапом є перевірка рекомендацій – але не лише тих, що надав сам кандидат. Доцільно використовувати метод “indirect references”, коли зв’язуються з колегами чи партнерами по проєктах, яких кандидат не вказував, але які можуть надати більш об’єктивну оцінку його професійної поведінки.

Оцінка фінансової стабільності кандидата теж може бути показовою. Наявність значних боргів, судових позовів чи незрозумілих джерел доходів іноді свідчить про потенційний ризик підкупу або шахрайських дій. Зрозуміло, така перевірка має виконуватися з дотриманням законодавчих обмежень у сфері захисту персональних даних.

Корисним інструментом є моніторинг відкритих джерел – аналіз активності в соціальних мережах, участі у форумах, публікацій та коментарів, які можуть демонструвати ставлення до етичних норм, рівень агресивності, схильність до маніпуляцій або поширення конфіденційної інформації.

Додатково можна застосувати перевірку через правоохоронні органи, якщо це дозволено законодавством, для виявлення судимостей, фактів адміністративних правопорушень або участі в розслідуваннях.

Психологічне тестування та інтерв’ю з елементами поведінкової аналітики допомагають оцінити схильність до маніпуляцій, брехні або порушення норм. Запитання, що моделюють реальні робочі ситуації, дозволяють перевірити реакцію кандидата на етичні дилеми та спроби тиску.

Окремо варто включити перевірку технічної репутації та участі в кіберспільнотах, якщо посада передбачає роботу з конфіденційними даними чи доступ до критичних систем. Тут можуть допомогти пошук за нікнеймами, email-адресами, участь у CTF чи хакерських форумах – знову ж таки, в межах правового поля.

Нарешті, варто встановити політику перевірки надійності не лише перед прийомом, а й під час роботи, особливо при зміні посади чи розширенні доступів. Це допоможе виявляти ризики, які з'явилися вже після працевлаштування.

Соціальні інженери, на відміну від випадкових порушників політик безпеки, діють цілеспрямовано і системно, використовуючи маніпулятивні методи для досягнення своїх цілей. Їхня поведінка часто має певні індикатори, які, у поєднанні між собою, можуть вказувати на підвищений ризик. Важливо розуміти, що кожен окремий сигнал не завжди означає зловмисні наміри, однак їхня сукупність, особливо в контексті доступу до чутливих ресурсів, повинна привернути увагу.

Одним із ключових індикаторів є підвищений інтерес до внутрішньої інформації, яка не стосується прямих обов'язків працівника. Соціальний інженер може ставити надмірну кількість уточнювальних запитань про структуру організації, імена співробітників, робочі процеси, конфігурацію систем або безпекові процедури. Такі запитання нерідко формулюються непрямо, у контексті дружньої бесіди чи нібито робочої необхідності.

Часто спостерігається тенденція до побудови швидких неформальних контактів і отримання довіри. Соціальний інженер може активно демонструвати готовність допомогти, прагнути до особистих розмов, підкреслювати спільні інтереси чи обставини, щоб знизити пильність співрозмовника. Іноді він цілеспрямовано обирає окремих співробітників, які здаються більш відкритими або менш обізнаними у питаннях безпеки.

Іншим сигналом може бути обхід офіційних каналів комунікації та процедур. Зловмисник намагатиметься вирішити питання через особисті повідомлення, приватні месенджери або телефони, уникати електронної пошти

компанії чи формальних запитів. У такій поведінці може простежуватися поспіх або створення штучного відчуття терміновості, що є класичною тактикою тиску.

Підозру повинні викликати й спроби отримати фізичний доступ до заборонених зон або використання чужих облікових даних. Соціальні інженери можуть з'являтися в робочих приміщеннях без супроводу, "проходити за кимось" через контрольні точки або просити тимчасові доступи під виглядом термінового завдання.

Ще одним індикатором є невідповідність офіційної ролі та реальної поведінки. Наприклад, людина, яка не працює у технічному відділі, цікавиться налаштуваннями мережі чи конфігурацією серверів; співробітник з адміністративної посади виявляє детальне знання внутрішніх IT-процесів, хоча не має на це формальної потреби.

Соціальний інженер часто уникає залишати сліди. Він може відмовлятися від офіційних перепусток, уникати електронних заявок, рідко користуватися корпоративними системами комунікації, надаючи перевагу усним чи неформальним обговоренням.

Додатковими індикаторами можуть бути надмірна впевненість у спілкуванні, агресивне або маніпулятивне реагування на запити про уточнення, а також часте посилання на авторитетні імена чи посади ("мене просив директор", "це для безпеки клієнтів"). Такі фрази покликані зменшити ймовірність перевірки інформації.

Виявлення соціального інженера – це не разова дія, а постійний процес спостереження та аналізу поведінки в динаміці. Важливо навчати персонал розпізнавати ці сигнали та повідомляти про них через офіційні канали без побоювання дисциплінарних наслідків. Саме системне реагування на підозрілі дії дозволяє запобігти реалізації атак, що базуються на маніпуляціях та психологічному впливі.

5.5 Матриця ризикових індикаторів соціального інженера

Наведемо матрицю, яка призначена для використання в політиці інформаційної безпеки та програмах підвищення обізнаності персоналу. Ця матриця є орієнтиром для виявлення потенційних ознак соціальної інженерії, визначення ймовірних загроз, потенційного впливу, а також відповідальних осіб, які можуть допомогти у викритті соціальних інженерів та їхньої рекомендованої поведінки.

Таблиця 5.1 – Матриця індикаторів соціального інженера

№	Індикатор поведінки	Ймовірність загрози	Потенційний вплив	Відповідальні особи	Рекомендована реакція / Політика
1	Надмірний інтерес до внутрішньої інформації, яка не стосується посадових обов'язків	Висока	Може призвести до збору даних для подальших атак	Керівник підрозділу, Служба ІБ	Задати уточнюючі питання, повідомити керівника або службу ІБ, зафіксувати інцидент. Політика управління доступом, Політика інформаційної безпеки
2	Швидке встановлення неформальних контактів і демонстративна дружелюбність	Середня	Використання довіри для зниження пильності	Керівник підрозділу, HR	Моніторинг взаємодій, нагадування про правила безпечної комунікації. Політика навчання та обізнаності
3	Обхід офіційних каналів комунікації та процедур	Висока	Зменшення можливості фіксації запитів і перевірки достовірності	Служба ІБ, Керівник підрозділу	Наполягати на використанні офіційних каналів, повідомити службу ІБ. Політика комунікацій
4	Створення штучного відчуття терміновості ("це потрібно зараз")	Висока	Підштовхування до поспішних рішень без перевірки	Всі співробітники, Служба ІБ	Зберігати стандартні процедури перевірки, навіть під час термінових запитів. Політика реагування на інциденти

№	Індикатор поведінки	Ймовірність загрози	Потенційний вплив	Відповідальні особи	Рекомендована реакція / Політика
5	Спроби отримати фізичний доступ без повноважень або “прохід за кимось”	Висока	Може призвести до фізичного доступу до критичних ресурсів	Охорона, Служба ІБ	Негайно зупинити, перевірити повноваження, повідомити охорону та службу ІБ. Політика фізичної безпеки
6	Невідповідність офіційної ролі та знань/інтересів	Середня	Може свідчити про приховану роль або підготовку атаки	Керівник підрозділу, Служба ІБ	Встановити джерело інтересу, обмежити доступ, повідомити керівництво. Політика управління доступом
7	Уникання офіційних перепусток, електронних заявок, фіксації дій	Висока	Ускладнює розслідування інцидентів	Охорона, Служба ІБ	Наполягати на виконанні процедур, зафіксувати інцидент. Політика фізичної безпеки
8	Часті посилання на авторитет без підтвердження	Середня	Використання психологічного тиску	Всі співробітники, Керівник підрозділу	Перевіряти інформацію незалежно від джерела, повідомити службу ІБ. Політика комунікацій
9	Агресивна або маніпулятивна реакція на перевірку	Середня	Намагання уникнути контролю	Керівник підрозділу, HR	Спокійно продовжити перевірку, зафіксувати поведінку. Політика реагування на інциденти
10	Незрозумілі прогалини в історії роботи чи навчання	Середня	Може свідчити про приховані факти	HR	Перевірити бекграунд через доступні канали. Політика перевірки персоналу

5.6 Аналіз реагування персоналу на атаки соціальної інженерії

Щоб виявити невідповідні реакції персоналу на спроби соціальної інженерії, використовують поєднання імітаційних тестів, психологічних методик і практичних ситуаційних завдань. Ці інструменти дозволяють не лише оцінити

рівень знань і обізнаності, але й перевірити поведінкові реакції у реальних або максимально наближених до реальних умовах [28].

Найефективнішими є імітаційні атаки. Це контрольовані сценарії, у яких відтворюють фішингові, вішингові чи смішингові повідомлення. Наприклад, співробітникам надсилають тестовий фішинговий лист із елементами, характерними для реальних атак (помилки в доменах, терміновість, “посилання” на фальшиві ресурси). Реакція співробітників аналізується: хто відкрив лист, перейшов за посиланням, ввів дані або повідомив службу безпеки. Аналогічно можна проводити тестові дзвінки, коли інструктори грають роль зловмисників, намагаючись отримати конфіденційні дані чи змусити виконати дію.

Дуже показовими є тести на фізичну безпеку та уважність. Приклад – залишення у видимих місцях підозрілих носіїв (USB, DVD) або документів із міткою “Конфіденційно”, щоб перевірити, чи працівник повідомить охорону чи спробує скористатися знахідкою. Ще один варіант – спроба проникнення в офіс із використанням “tailgating” (прохід за співробітником), аби оцінити, чи перевіряють вони наявність повноважень у сторонніх осіб.

Психометричні й поведінкові тести можуть бути частиною навчання та відбору персоналу. Це завдання, які оцінюють уважність до деталей, здатність критично мислити, визначати приховані мотиви співрозмовника або виявляти маніпулятивні техніки. Наприклад, кандидату або співробітнику пропонують набір робочих сценаріїв (“Вам телефонує колега з іншого відділу і просить терміново надати йому доступ до системи – ваші дії?”) і аналізують, чи дотримується він процедур перевірки.

Також ефективними є онлайн-тести з розпізнавання загроз: учасникам показують приклади листів, скриншотів чатів чи сторінок сайтів, і вони мають визначити, які з них безпечні, а які потенційно небезпечні. Оцінюють не лише правильність, а й швидкість прийняття рішень.

Додатково можна застосовувати стрес-тести на багатозадачність і терміновість. Під час навчальної сесії співробітника можуть перервати

“терміновим” запитом (імітація зловмисника), щоб подивитися, чи зможе він зберегти процедури перевірки в умовах тиску часу.

Результати таких тестів дають змогу не лише виявити тих, хто схильний до ризикованої поведінки, а й зрозуміти, які аспекти навчання потрібно підсилити. Головне – проводити їх регулярно та комбінувати кілька методів, адже соціальна інженерія багатогранна, і реакція співробітників залежить від контексту.

В таблиці 5.2. наведемо перелік основних типів тестів, які дозволяють оцінити готовність співробітників до виявлення та правильного реагування на атаки соціальної інженерії. В таблиці наведено описи сценаріїв, рекомендовану періодичність перевірок, критеріїв успішності перевірок та відповідальних осіб, задіяних у перевірках. Наведені у таблиці цифри (наприклад, кількість правильних реакцій, кількість перевірок на рік – є експертною думкою авторів, і можуть бути скореговані на основі вподобань експертів конкретної організації).

Таблиця 5.2 – Характеристики тестування персоналу на реагування щодо спроб соціальної інженерії

Тип тесту	**Сценарій**	**Періодичність**	**Критерії успішності**	**Відповідальні**
Фішинг-тести (електронна пошта)	Класичний фішинг; цільовий фішинг з персоналізованими даними; фішинг із вкладеннями	3–4 рази на рік	≥85% правильних реакцій, зростання кількості повідомлень службі ІБ	Служба ІБ, ІТ-відділ
Вішинг-тести (телефонні дзвінки)	Дзвінок від «служби безпеки» з проханням надати пароль або код; імітація керівника з терміновим запитом	1–2 рази на рік	Відсутність розголошення даних, дотримання процедури перевірки	Служба ІБ, Керівники підрозділів
Смішинг-тести (SMS / месенджери)	Повідомлення з фішинговим посиланням; пропозиція встановити «оновлений корпоративний додаток»	1–2 рази на рік	Нуль переходів за шкідливими посиланнями або завантажень додатків	Служба ІБ, ІТ-відділ
Фізичні тести	Залишений USB-носій у місці загального доступу; tailgating (прохід за	1–2 рази на рік	Повідомлення охорони про носій; відсутність порушень правил доступу	Служба ІБ, Охорона

Тип тесту	Сценарій	Періодич-ність	Критерії успішності	Відповідальні
	співробітником без перепустки)			
Претекстинг-тести	Звернення від «партнерської компанії» із запитом даних; імітація співробітника іншого відділу	1–2 рази на рік	Відсутність розголошення без перевірки; виконання процедур верифікації	Служба ІБ, Керівники підрозділів
Онлайн-тести на розпізнавання загроз	Визначення фішингових листів, підроблених сайтів, шкідливих вкладень	2–3 рази на рік	≥85% правильних відповідей; швидке прийняття рішень	Служба ІБ, Відділ навчання
Стрес-тести з елементами терміновості	Імітація термінового завдання від керівника під час завантаженості	1 раз на рік	Збереження процедур перевірки в умовах тиску часу	Служба ІБ, Керівники підрозділів

З усього вищенаведеного можна зробити висновок, що управління інформаційною безпекою із врахуванням атак на людську складову є складним міждисциплінарним завданням, яке повинно спиратись на науково-практичні підходи та методики.

ЛІТЕРАТУРА

1. Нижник Н.Р. Національна безпека України / Нижник Н.Р., Ситник Г.П., Білоус В.Т.– Ірпінь: Академія ДПС України, 2000. – 304с.
2. Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України. – Харків: Фоліо, 2002. – 285с.
3. Кормич Б.А. Інформаційна безпека: організаційно правові основи. – К.: Кондор, 2008. – 384с.
4. Закон України «Про основи національної безпеки України» від 19.06.2003 // Голос України. – 22.07.2003 - №134.
5. Ареф'єв О.В., Кузенко Т.Б. Планування економічної безпеки підприємств. – К.: Вид-во Європ. ун-ту, 2004. – 170с.
6. ISO/IEC TR 13335 – 1. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 1. Концепції і моделі безпеки IT.
7. ISO/IEC TR 13335 – 3. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 3. Методи керування захистом IT.
8. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи. – К.:2003. – 472с.
9. Грабовецький Б.Є. Економічне прогнозування і планування. – К.: Центр навчальної літератури, 2003. – 188с.
10. Згуровський М.З. Сценарний аналіз як системна методологія передбачення // системні дослідження та інформаційні технології. – 2002. - №1. –С.5-36.
11. Архипов О.Є. Касперський І.П. Проблеми методики отримання та обробки оціночних суджень членів експертних комісій створюваних державними експертами з питань таємниць // Правова інформатика, 2006, №4 (12), С.80-87.

12. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
13. Архипов О.Є., Муратов О.Є. Деякі проблемні аспекти менеджменту інформаційної безпеки//Актуальні проблеми забезпечення інформаційної безпеки держави: Зб. матеріалів наук.-практ. конф., Київ, 20 березня 2009р./НА СБ України, Ін-т захисту інформації з обмеженим доступом.- К.: Наук.-вид. відділ НА СБ України, 2009 – 200с., С. 80-84.
14. Архипов О.Є., Бородавко І.Т., Ворожко В.П. Оцінювання ефективності системи охорони державної таємниці. – К.: Наук.-вид. відділ НА СБ України, 2007. – 63с.
15. ISO/IEC 27001:2005, Information Technology – Security techniques – Information security management systems – Requirements.
16. ISO/IEC 27002:2007, Information Technology – Security techniques – Code of practice for information security management.
17. ISO/IEC 27005, Information Technology – Security techniques – Information security risk management.
18. Дмитрієв А.А. Внутрішній аудит системи менеджменту інформаційної безпеки за вимогами ISO/IEC 27001. Один з варіантів реалізації процесу / Das Management. – 2011. – № 2. – С. 58-64.
19. Скотт Б. Розробка правил інформаційної безпеки / Бармен Скотт. – М. : Вільямс, 2002. – 208 с.
20. Семененко В.А. Інформаційна безпека : навчальний посібник / В.А. Семененко – М. : МГИУ, 2004 – 215 с.
21. Носок С.О., Фаль О.М., Ткач В.М.. Управління інформаційною безпекою. Конспект лекцій [Електронний ресурс]. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.
22. Novikov, Oleksii, Shreider, Mariia, Stopochkina, Iryna, Ilin, Mykola. Cyber Attacks Simulation for Modern Energy Facilities / CEUR Workshop Proceedings. Selected Papers of the XXIII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2023). – С. 35–49. – URL: https://ceur-ws.org/Vol-3887/.
23. Styopochkina, Iryna, Rybak, Oleksandr, Ilin, Mykola. Probabilities estimating for attacks on supply chain for critical infrastructure facilities /

Theoretical and Applied Cybersecurity. – 2024. – Т. 6, № 1. – С. 62–71. – DOI: https://doi.org/10.20535/tacs.2664-29132024.1.307939.
24. Chornyi, A., Stopochkina, I. Graph-based analysis of information flows in telegram for cybersecurity threat detection / Кібербезпека: освіта, наука, техніка. – 2025. – Т. 3, № 27. – С. 368–380. – DOI: https://doi.org/10.28925/2663-4023.2025.27.746.
25. Chalyi, O., Stopochkina, I. Information retrieval and deanonymization in the tasks of early detection of potential attacks on critical infrastructure / Кібербезпека: освіта, наука, техніка. – 2024. – Т. 2, № 26. – С. 305–322. – DOI: https://doi.org/10.28925/2663-4023.2024.26.694
26. Методи штучного інтелекту в кібербезпеці [Електронний ресурс] : навч. посіб. для здобувачів спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: О.М. Новіков, І.В. Стьопочкіна. – Електронні текстові дані (1 файл: 19,4 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. – 82 с. – URL: https://ela.kpi.ua/handle/123456789/47605.
27. Теорія та методи соціальної інженерії в кібербезпеці: Лабораторний практикум /[Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека», уклад. Ільїн К.І., Стьопочкіна І.В., 2023. URL: https://ela.kpi.ua/handle/123456789/67176
28. Стьопочкіна, І., Ільїн, К. Профілювання користувачів для підвищення стійкості персоналу об’єктів критичної інфраструктури до кібератак, які використовують людський фактор / Information Technology: Computer Science, Software Engineering and Cyber Security. – 2024. – № 3. – С. 159–168. – DOI: https://doi.org/10.32782/IT/2024-3-17.