МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ
ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

«До захисту допущено»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
“___”_____20__ р.

# МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

на тему: **«ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА ТА ОСОБЛИВОСТІ ЇЇ ОРГАНІЗАЦІЇ»**

**Студент групи** УБДМ-61 Панченко Вячеслав Геннадійович _____
(підпис)

**Науковий керівник:** к.е.н., доцент Мордас Ірина Василівна _____
(підпис)

**Нормоконтроль:** к.держ.упр. Мужанова Тетяна Михайлівна _____
(підпис)

Київ – 2020

**Державний університет телекомунікацій**
**Навчально-науковий інститут захисту інформації**
**Кафедра управління інформаційною та кібернетичною безпекою**

«Затверджую»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
“___”_____20__ р.

# ЗАВДАННЯ

**на магістерську атестаційну роботу**
студенту Панченку Вячеславу Геннадійовичу

**1. Тема роботи:** «ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА ТА ОСОБЛИВОСТІ ЇЇ ОРГАНІЗАЦІЇ» затверджена наказом ректора від «___» _____ 20__ р. № __.

**2. Термін здачі** студентом оформленої роботи: «___» _____ 20__ р.

**3. Об’єкт дослідження:** інформаційна безпека підприємства.

**4. Предмет дослідження:** особливості організації інформаційної безпеки підприємства.

**5. Мета дослідження:** вивчення підходів до організації інформаційної безпеки підприємства.

**6. Перелік питань, які мають бути розроблені:**

1. Основні вимоги до організації інформаційної безпеки підприємства на сучасному етапі в Україні.
2. Функціонування системи інформаційної безпеки підприємства.
3. Напрямки та методи вдоконалення організації інформаційної безпеки підприємства.

**7. Дата видачі завдання:** «___» _____ 20__ р.

**Науковий керівник:** Мордас І. В.

**Завдання прийнято до виконання:** Панченко В. Г.

**Державний університет телекомунікацій**
**Навчально-науковий інститут захисту інформації**
**Кафедра управління інформаційною та кібернетичною безпекою**

# КАЛЕНДАРНИЙ ПЛАН

**виконання магістерської атестаційної роботи**
студентом Панченком Вячеславом Геннадійовичем

Дата видачі завдання: «__» _____ 20__ р.

| № з/п | Етапи виконання магістерської атестаційної роботи | Термін виконання етапів | Примітка |
|---|---|---|---|
| 1. | Визначення об’єкту, предмету, мети та завдань дослідження. | 10.10.2019 | |
| 2. | Збір та аналіз літератури. | 18.10.2019 | |
| 3. | Написання 1-го розділу роботи. | 31.10.2019 | |
| 4. | Написання 2-го розділу роботи. | 14.11.2019 | |
| 5. | Написання 3-го розділу роботи. | 28.11.2019 | |
| 6. | Формулювання висновків за результатами проведеного дослідження. | 05.12.2019 | |
| 7. | Оформлення роботи. | 12.12.2019 | |
| 8. | Оформлення презентації. | 19.12.2019 | |
| 9. | Отримання рецензії на роботу. | 26.12.2019 | |
| 10. | Захист в ДЕК. | __.01.2020 | |

**Студент групи** УБДМ-61 Панченко Вячеслав Геннадійович _____
(підпис)

**Науковий керівник:** к.е.н., доцент Мордас Ірина Василівна _____
(підпис)

**Нормоконтроль:** к.держ.упр. Мужанова тетяна Михайлівна _____
(підпис)

# РЕФЕРАТ

Робота містить вступ, три розділи з підрозділами, висновки та список використаних джерел. Загальний обсяг роботи – 99 сторінок.

Об’єкт дослідження – інформаційна безпека підприємства.

Предмет дослідження – особливості організації інформаційної безпеки підприємства.

Мета дослідження – вивчення підходів до організації інформаційної безпеки підприємства.

У магістерській атестаційній роботі проаналізовано основні вимоги до організації інформаційної безпеки підприємства на сучасному етапі в Україні; досліджено функціонування системи інформаційної безпеки підприємства; визначено напрямки та методи вдоконалення організації інформаційної безпеки підприємства.

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА, ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА, ОРГАНІЗАЦІЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

DPL – технології запобігання витоків конфіденційної інформації

SIEM (Security information and event management) – об'єднання двох термінів, що позначають область застосування програмного забезпечення: SIM (Security information management) - управління інформаційною безпекою, і SEM (Security event management) - управління подіями безпеки.

ОТЗС – основні технічні засоби і системи

IPsec - набір протоколів для забезпечення захисту даних, що передаються по міжмережевому протоколу IP

ІБ – інформаційна безпека

ІС – інформаційні системи

# ВСТУП

*Актуальність теми.* Захист інформації – це сукупність організаційних, правових та технічних заходів, які спрямовані на запобігання нанесенню збитків інтересам її власника. Основними об’єктами захисту інформації є: по-перше – інформація з обмеженим доступом ( інформаційні ресурси, які містять відомості таємного або конфіденційного характеру ); по-друге, технічні засоби зберігання, приймання, передавання та обробки інформації, а саме засоби та автоматизовані системи управління, системи інформатизації, програмні засоби; й по-третє, допоміжні технічні системи і засоби.

Проблеми інформаційної безпеки, удосконалення методів та принципів інформаційного забезпечення, фінансово-економічної та інформаційної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів України в сучасних умовах надзвичайно актуальні та потребують поглибленого вивчення. Термін «безпека» розуміється як стан захищеності життєво важливих інтересів особистості, суспільства, підприємства, держави від внутрішніх і зовнішніх загроз. Але його зміст у науковому розумінні ще не визначено повністю.

У цілому інформаційна безпека повинна відображати стан захищеності як національних інтересів від зовнішніх і внутрішніх загроз як для самої держави або суспільства, так і окремих підприємств та організацій сфери економіки, бізнесу та фінансів. Інформаційна безпека є одночасно і елементом у системі вищого рівня − міжнародного, національного, місцевого. Але сьогодні ряд підсистем, що входять в цю макросистему, ще не вивчені на належному рівні, а також не мають комплексного, системного дослідження з виходом на сучасні конструкції та пропозиції. Наведене вище стосується проблем інформаційної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів в Україні.

З огляду на зазначене тема магістерської роботи є актуальною, а використання її результатів сприятиме підвищенню рівня організації інформаційної безпеки на підприємствах.

*Мета і завдання дослідження. Мета* роботи полягає у вивченні підходів до організації інформаційної безпеки на підприємстві.

Для досягнення цієї мети в роботі необхідно виконати наступні *завдання:*

1. Провести аналіз основних вимог до організації інформаційної безпеки підприємства на сучасному етапі в Україні.

2. Дослідити функціонування інформаційної безпеки підприємства, зокрема представити схему моделі.

3. Визначити напрямки та методи вдосконалення організації інформаційної безпеки підприємства.

*Об'єкт* дослідження – інформаційна безпека підприємства.

*Предмет* дослідження – особливості організації інформаційної безпеки підприємства.

*Методи дослідження.* У роботі були використані методи аналізу та синтезу, індукції та дедукції, аналогії, порівняння та ін.

*Практичне значення одержаних результатів.* Запропонована модель і методи організації інформаційної безпеки підприємства можуть використовуватися на етапах розробки захисту інформації для оцінки їх ефективності.

# РОЗДІЛ 1
# ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

На сьогоднішній день об’єктивна та своєчасна інформація є тим важливим фактором виробництва, який розглядають як один з основних ресурсів розвитку суспільства. Сучасні інформаційні технології та системи є засобом підвищення ефективності та продуктивності роботи працівників [1]. Але глобальна комп’ютеризація у багатьох сферах виробництва та управління супроводжується появою принципово нових загроз інтересам особистості, підприємства, держави та суспільства [2].

Паралельно з розвитком і ускладненням засобів, методів, форм автоматизації процесів обробки інформації підвищується залежність суб’єктів підприємництва від ступеню безпеки використовуваних ними інформаційних технологій [3]. Постійна робота в сфері підтримки інформаційної безпеки на належному рівні є необхідною умовою ефективності підприємницької діяльності [4].

Водночас інформаційна безпека має розглядатися як важлива складова загальної безпеки підприємства. Причому необхідна розробка концепції інформаційної безпеки, в якій слід передбачити не тільки заходи, пов’язані з інформаційними технологіями (криптозахист, програмні засоби адміністрування прав користувачів, їх ідентифікації та автентифікації, брандмауери для захисту входів-виходів мережі тощо), але і відповідні заходи адміністративного та технічного характеру [5].

## 1.1 Основні вимоги до організації інформаційної безпеки підприємства на сучасному етапі в Україні

Підприємствам різних галузей доводиться функціонувати в умовах високої складності, невизначеності і динамічності навколишнього середовища. За рахунок інформатизації світового ринку суб’єкти господарювання мають

доступ до будь-якої інформації, що створює конкуренцію у виробничій сфері. У зв’язку з цим виникає потреба у створенні не тільки єдиного інформаційного простору, але й адекватного механізму організації інформаційної безпеки на підприємствах. Ця діяльність набуває особливої актуальності на сучасному етапі, коли поширюються різноманітні способи ворожого конкурентного впливу [6].

Сьогодні спеціалізовані організації пропонують широкий спектр засобів захисту інформаційних систем з урахуванням їх вартості та функціональних можливостей. Найбільш прийнятним підходом при виборі того чи іншого варіанту є дотримання принципу «розумної достатності», суть якого полягає в тому, що визначальними при проектуванні політики інформаційної безпеки повинні бути: розмір підприємства, його ресурсні та фінансові можливості, поточний рівень інформаційної безпеки, стадія функціонування організації. Постійна робота в сфері підтримки інформаційної безпеки на належному рівні є необхідною умовою ефективності підприємницької діяльності [7].

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, обробки, зберігання, пошуку та надання користувачам. Ці технології мають враховувати особливості інформації, які роблять її цінною, а також давати змогу користувачам різних категорій ефективно працювати з інформаційними ресурсами [7].

### 1.1.1 Сутність та поняття інформаційної безпеки підприємства

Поняття інформаційної безпеки, в залежності від його використання, розглядається в декількох ракурсах. У загальному випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держави [8]. Під інформаційним середовищем розуміють сферу

діяльності суб’єктів, пов’язану зі створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно ділиться на три основні предметні частини: – розповсюдження та створення вихідної та похідної інформації; − формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг; – споживання інформації, і дві забезпечувальні предметні частини: − створення і застосування інформаційних систем, інформаційних технологій та засобів їх забезпечення; – створення і застосування засобів і механізмів інформаційної безпеки. Більш розгорнуте формулювання інформаційної безпеки − це стан захищеності потреб в інформації особистості, суспільства та держави, при якому забезпечується їх існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Слід зазначити, що задоволення в будь-якому ступені потреб в інформації призводить до оволодіння відомостями про навколишній світ і процеси, що протікають в ньому.

Стан інформованості визначає ступінь адекватності сприйняття суб’єктами навколишньої дійсності і, як наслідок, обґрунтованість рішень і дій, які приймаються [9, 10]. Залежно від виду загроз інформаційну безпеку можна розглядати наступним чином: − як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації; – інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб; – інформаційних прав і свобод громадянина. В інформаційному праві інформаційна безпека − це одна із сторін розгляду інформаційних відносин у рамках інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на погрози, механізми усунення або запобігання таких загроз правовими методами [9, 11, 12].

Питання інформаційної безпеки, які наведені в юридичній та спеціальній літературі, і базуються на розумінні інформаційної безпеки як складової національної безпеки України. По суті це є вірним, оскільки завданням заходів

з інформаційної безпеки є мінімізація шкоди за неповноти, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації [13, 14, 15]. Саме тому інформаційна безпека передбачає наявність певних державних інститутів і умов існування її суб'єктів, встановлених міжнародним і вітчизняним законодавством [16]. Крім цього, інформаційна безпека повинна забезпечуватися шляхом проведення цілісної державної програми відповідно до Конституції та чинного законодавства України і норм міжнародного права шляхом реалізації від- 18 повідних доктрин, стратегій, концепцій і програм, що стосуються національної інформаційної політики України [11, 12].

Інформаційна безпека має на увазі можливість безперешкодної реалізації суспільством і окремими його членами своїх конституційних прав, пов'язаних з можливістю вільного одержання, створення і поширення інформації. Поняття інформаційної безпеки слід також розглядати в контексті: − забезпечення безпечних умов існування інформаційних технологій, що включають питання захисту інформації; − інформаційної інфраструктури держави; − інформаційного ринку та створення умов існування і розвитку інформаційних процесів. Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення і нейтралізацію тих обставин, факторів і дій.

### 1.1.2 Вимоги методичних матеріалів до організації інформаційної безпеки

Розвиток глобального процесу інформатизації суспільства, що спостерігається в останні роки, спричинив нову світову проблему – інформаційну безпеку. Багато найважливіших інтересів підприємства в даний час значною мірою визначається станом навколишнього інформаційного середовища. Планомірні або ненавмисні впливи на інформаційну сферу з боку

зовнішніх або внутрішніх джерел можуть завдавати серйозної шкоди інтересам і становлять загрози та ризики для інформаційної безпеки.

Будь-яка недружня акція, спрямована проти інтересів господарського суб'єкта, починається зі збору інформації: навіть дрібне розкрадання звичайно випереджає вивчення особою зі злочинними задумами можливості протиправних дій, і без відповідного інформаційного забезпечення не представляються такі деструктивні прояви, як відведення активів підприємства або рейдерське захоплення [17].

Питання інформаційної безпеки знайшли відображення у таких законах України: «Про основи національної безпеки України», «Про концепцію національної програми інформатизації», «Про національну програму інформатизації», а також у Стратегії національної безпеки України, яка затверджена Указом Президента. У Законі «Про основи національної безпеки України» надано офіційну оцінку значущості й системної сутності інформаційної безпеки як невід'ємної складової національної безпеки України.

У Стратегії національної безпеки, присвяченій стану інформаційної безпеки в нашій державі, зазначено[18]:

- посилюється негативний зовнішній вплив на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності;
- недостатніми залишаються обсяги вироблення конкурентоспроможного національного інформаційного продукту;
- наближається до критичного стан безпеки інформаційно-комп'ютерних систем у фінансовій і банківській сфері, сфері державного управління, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо.

Зі зростанням науково-технічного прогресу буде зростати важливість питання інформаційної безпеки. Інформація стала чинником, який може призвести до значних технологічних аварій, військових та політичних конфліктів, дезорганізувати державне управління, фінансову систему. Чим вищий рівень інформатизації суспільства, тим потрібнішою стає надійна

інформаційна безпека, оскільки реалізація інтересів, суспільства та держав усе більше здійснюється за допомогою інформатизації. Ураховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися кругозір та мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів скритого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і суперечать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах [19, 35-38].

Погіршення на підприємстві таких параметрів інформації, як конфіденційність, цілісність, доступність, вірогідність тощо, може призвести до досить негативних наслідків:

- розголошення відомостей, що становлять комерційну й інші види таємниць;
- збоїв у функціонуванні систем управління технологічними процесами й іншими критичними системами;
- несанкціонованого доступу до персональних даних фізичних осіб тощо.

Результатом перерахованого можуть стати:

- погіршення ділових відносин між партнерами;
- втрата вигідних контрактів, зриви переговорів;
- невиконання договірних зобов'язань;
- необхідність проведення додаткових ринкових досліджень;
- відмовлення від рішень, що стали неефективними через розповсюдження інформації, і, як наслідок, – фінансові втрати, пов'язані з новими розробками;
- втрата можливості запатентувати результат науково-технічної діяльності або продати ліцензію;
- зниження цін або обсягів реалізації;
- втрати ділової репутації;
- більш жорсткі умови одержання кредитів;
- труднощі в постачанні і придбанні устаткування тощо.

У визначених ситуаціях зневага питаннями захисту інформації може призвести до повного банкрутства. Дії внутрішніх порушників, такі як недбалість співробітників, крадіжки інформаційних ресурсів та IT-устаткування, фінансові й інші види шахрайства з використанням інформаційних систем і ресурсів тощо, набагато рідше стають предметом уваги при розв'язанні проблем інформаційної безпеки у випадку, якщо вони розглядаються у відриві від загальних завдань забезпечення економічної безпеки.

Людський фактор завжди був і є одним із найважливіших ризиків будь-якого бізнесу, оскільки більшість інцидентів відбуваються саме з вини співробітників. Навмисний відплив часто важко відрізнити від ненавмисного, однак це не завжди потрібно, оскільки наслідки для підприємства при будь-якому із цих варіантів можуть бути катастрофічними. Те, що більшість керівників не знають джерел внутрішніх загроз, говорить про те, що бізнесом приділяється недостатньо уваги інформаційній безпеці, що, утім, є одним із найважливіших факторів існування підприємства. Поза увагою залишаються питання потенційних внутрішніх ризиків, що виходять від співробітників, які мають доступ до критично важливих систем і секретної інформації. Хоча керівники усвідомлюють існування таких ризиків, турбота про зовнішню інформаційну безпеку часто переважує інші питання. Але значною є кількість порушень та випадків несанкціонованого доступу і використання інформації самими співробітниками, що ставить під загрозу основу бізнесу багатьох підприємств.

Фахівці у сфері інформаційної безпеки дотримуються двох думок.

Перша полягає у такому: інформаційною безпекою на підприємстві можна взагалі не займатися, не витрачаючи коштів. У цьому випадку не виключений такий варіант, що прийнятий ризик себе цілком виправдає.

Другий погляд: необхідно витратити на створення системи захисту інформації чимало грошей (навчання персоналу, програмне забезпечення тощо) і тим самим забезпечити належний рівень безпеки. Але при цьому також

залишиться деяка вразливість, що рано або пізно призведе до відпливу або розкрадання конфіденційної інформації.

В обґрунтуванні витрат на інформаційну безпеку можна використати нижченаведений підхід. Необхідно застосувати на практиці інструментарій визначення рівня інформаційної безпеки. Керівництво підприємства залучається до оцінки вартості інформаційних ресурсів, визначення оцінки потенційного збитку від порушень інформаційної безпеки. Від результатів цих оцінок буде багато в чому залежати подальша діяльність керівників у сфері інформаційної безпеки. Якщо інформація нічого не коштує, істотних загроз для інформаційних активів немає, а потенційний збиток мінімальний, то проблемою забезпечення інформаційної безпеки можна не займатися. Якщо ж інформація має значну вартість, загрози і потенційний збиток ясні, тоді постає питання про внесення в бюджет витрат на підсистему інформаційної безпеки. У цьому випадку слід заручитися підтримкою керівництва підприємства в усвідомленні проблем інформаційної безпеки й побудові системи захисту інформації. Надійно гарантувати бізнес від перерахованих негативних явищ можна тільки на основі формування ефективної системи забезпечення інформаційної безпеки. Однак тут існують певні проблеми при створенні системи інформаційної безпеки.

Першою і найбільшою проблемою у створенні системи інформаційної безпеки є відсутність розуміння в керівництва необхідності створення такої системи. Багато керівників підприємств не усвідомлюють, що створювати систему інформаційної безпеки просто необхідно, бо своєчасне створення її позбавить підприємство збитків, а іноді навіть і врятує бізнес.

Друга проблема при створенні системи інформаційної безпеки – відсутність достатньої кількості фінансових коштів. Відсутність фінансування з мінімального бюджету для створення системи інформаційної безпеки зустрічається також дуже часто.

Третьою найнебезпечнішою проблемою є ситуація, коли є розуміння керівництва та необхідні кошти, але створення системи інформаційної безпеки

доручають фахівцям, що не мають ані відповідної освіти, ані достатнього досвіду. Найчастіше це бувають системні адміністратори або відділ технічної підтримки. Вони, у свою чергу, розцінюють це як установку і налаштування антивірусу. Наявність внутрішнього зловмисника, найчастіше, узагалі не береться до уваги. У результаті таких дій кошти витрачені, а інформаційна безпека на колишньому рівні. Багато керівників підприємств можуть не бачити очевидного зв'язку між утратою доходів і відсутністю фінансових ресурсів у системі інформаційного захисту.

Тому в першу чергу необхідно подати проблему у зрозумілому для бізнесу вигляді. Це завдання лягає на керівництво служби інформаційної безпеки господарюючого суб'єкта, що має виявити і наочно показати власникам підприємства весь спектр загроз в інформаційній сфері, а також переконати, що протистояти їм можна тільки на основі створення і упровадження ефективних систем захисту інформації.

По-перше, для ефективного захисту інформаційних ресурсів потрібна реалізація цілої низки різнорідних заходів, які можна розділити на три групи: юридичні, організаційно-економічні й технологічні.

По-друге, хоча розробкою заходів у кожній із трьох груп повинні займатися фахівці відповідних галузей знань, які застосовують свої способи і методи для досягнення заданих цілей, кінцевий успіх значною мірою буде залежати від того, наскільки в рамках системного підходу вдасться визначити і реалізувати взаємні зв'язки між відповідними визначеннями, принципами, способами і механізмами захисту.

У сучасному поданні рольових функцій служби інформаційної безпеки можна виділити чотири напрями, які зазначені на рис. 1.1 [20, с.64-70].

У рамках першого напряму мають розв’язуватися такі основні завдання [21]:

- аналіз і узагальнення потенційних загроз і таких, що реалізувалися, причин порушень вимог інформаційної безпеки;


Рис. 1.1 Напрями функцій служби інформаційної безпеки

- аналіз ступеня забезпечення безперервності бізнес-процесів, що використовують IT, з точки зору інформаційної безпеки;
- пошук нових загроз і вразливостей, пов'язаних з інформаційною взаємодією;
- побудова методик оцінки інформаційних ризиків;
- інформаційне обстеження підприємства та інформаційних ресурсів;
- розробка методів захисту інформації та IT і методик їх упровадження в діяльність підприємства;
- розробка і модифікація концепції та політики забезпечення інформаційної безпеки;
- створення локальної нормативної бази із цих питань з урахуванням комплексного підходу до економічної безпеки;

- розробка методик оцінки рівня інформаційної безпеки і визначення достатності захисту інформації та ІТ з урахуванням потреб бізнесу, а також існуючої і перспективної нормативної бази;
- аналіз виконання вимог інформаційної безпеки всіх використовуваних процедур створення, обробки, пересилання, збереження, знищення інформації, у тому числі:
- процедур інформаційної взаємодії підрозділів підприємства між собою і із зовнішніми організаціями;
- порядків доступу співробітників підприємства і суміжних організацій, а також клієнтів до інформаційних ресурсів і зовнішніх комп'ютерних мереж;
- проектів розвитку ІТ, включаючи системи зв'язку і телекомунікацій;
- проектів договорів із зовнішніми організаціями, з якими здійснюється обмін інформацією;
- проектів інших нормативних документів, що передбачають інформаційну взаємодію;
- підготовка аналітичних записок, що містять висновки із проведеного аналізу і пропозиції щодо реалізації захисту інформації.

Другий напрям передбачає такі основні завдання[21]:

- планування на основі координації діяльності всіх підрозділів робіт із забезпечення інформаційної безпеки підприємства;
- організація й участь у впровадженні методів забезпечення інформаційної безпеки в діяльність підприємства.
- робота з персоналом, партнерами і клієнтами;
- узгодження заявок на доступ і порядку доступу співробітників і зовнішніх організацій до інформаційних ресурсів підприємства;
- процедур інформаційної взаємодії підрозділів із зовнішніми організаціями;
- договорів, з якими здійснюється інформаційна взаємодія; проектів наказів, розпоряджень, інших нормативно-розпорядницьких документів;

- розв’язання поточних практичних питань з інформаційної безпеки, що виникають у підрозділах.

У рамках третього напряму мають розв’язуватися такі основні завдання[21]: підтримка ключових структур, використовуваних у зовнішніх і вбудованих засобах криптографічного захисту інформації; підтримка роботи інших засобів інформаційної безпеки.

Четвертий напрям передбачає розв’язання таких основних завдань[21]:

- перевірка виконання вимог інформаційної безпеки працівниками підприємства й іншими особами, що мають доступ до інформаційних ресурсів;
- моніторинг дій користувачів ІТ (несанкціонованої модифікації інформації, використання різних поштових та інших сервісів мережі Інтернет для відправлення конфіденційної інформації за межі підприємства тощо);
- контроль своєчасної зміни прав користувачів в інформаційних системах; блокування облікових записів звільнених (переведених на іншу роботу) користувачів;
- контроль дотримання настроювань безпеки, включаючи парольну політику, інші вбудовані системи інформаційної безпеки, зовнішні засоби захисту інформації;
- моніторинг роботи систем виявлення (запобігання) мережних атак, систем оцінки якості побудови мережі й інших автоматизованих систем комп'ютерної безпеки;
- участь у розборі виявлених порушень інформаційної безпеки і вимог нормативних документів із цих питань.
- підготовка пропозицій щодо попередження порушень;
- проведення внутрішнього аудиту питань інформаційної безпеки;
- підготовка пропозицій щодо використання зовнішнього аудиту;
- проведення моніторингу можливого випливу конфіденційної інформації технічними каналами.

З огляду на міждисциплінарний характер питань, що входять у блок інформаційної безпеки, деякі з перелічених функцій можуть виконуватися тільки разом з іншими структурними службами підприємства (службою по роботі з персоналом, юридичною, господарською службою тощо). Для цього необхідно визначити політику безпеки підприємства – сукупність керівних принципів, правил, процедур і практичних прийомів сфери інформаційної безпеки, що регулюють управління, захист і розподіл цінної інформації на підприємстві. У загальному випадку такий набір правил становить деяку функціональність програмного продукту, необхідного для його використання в конкретній організації. Якщо підходити до політики безпеки більш формально, то вона є набором певних вимог до функціональності системи захисту, закріплених у відомчих документах.

Головною причиною появи політики безпеки звичайно є вимога наявності такого документа від організації, що визначає правила роботи підприємств даної галузі. У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності. Крім того, визначені вимоги та рекомендації ставлять галузеві або загальні, місцеві або міжнародні стандарти. Звичайно це виражається у вигляді зауважень зовнішніх аудиторів, що проводять перевірки діяльності підприємства [22]. Відсутність політики спричиняє негативну оцінку, що у свою чергу впливає на публічні показники підприємства – позиції в рейтингу, рівень надійності тощо. Далі випливає з'ясування, наскільки серйозні втрати може принести підприємству настання інформаційного ризику на кожен конкретний інформаційний об'єкт.

Оцінку ймовірності появи атаки краще довіряти технічним співробітникам підприємства. З різних організаційних схем функціонування підрозділів, що відповідають за інформаційну безпеку підприємства (функції такого підрозділу покладаються на системних адміністраторів; зазначений підрозділ знаходиться у структурі служби інформаційної безпеки, що підкоряється вищому керівництву), найкращим є варіант, при якому підрозділ інформаційної безпеки

входить до складу служби економічної безпеки підприємства. Саме в цьому випадку створюються найкращі можливості розв’язання проблем інформаційної безпеки в контексті загальних завдань безпеки бізнесу.

Таким чином, у сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки господарюючого суб'єкта. У свою чергу, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, але й національної економіки в цілому.

### 1.1.3 Основні складові організації інформаційної безпеки

Сьогодні інформаційні системи відіграють ключову роль в забезпеченні ефективності роботи комерційних і державних підприємств. Повсюдне використання інформаційних систем для зберігання, обробки і передачі інформації робить актуальними питання про те, як забезпечити безпеку інформаційних систем, особливо з огляду на глобальну тенденцію до зростання числа інформаційних атак, що приводять до значних фінансових і матеріальних втрат. Але перед тим, як перейти до питання організації системи інформаційної безпеки, потрібно детальніше розглянути основні складові організації інформаційної безпеки на підприємстві (рис. 1.2).

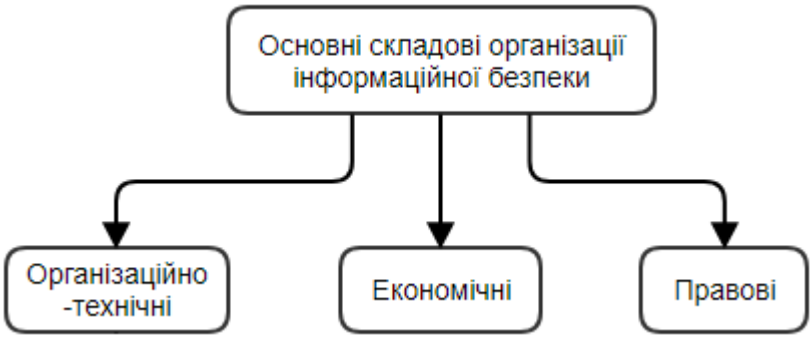


Рис. 1.2 Основні складові організації інформаційної безпеки

Організаційно-технічна складова інформаційної безпеки включає:

- систему забезпечення інформаційної безпеки (під нею ми маємо на увазі комплекс заходів (внутрішні правила роботи з даними, регламент передачі відомостей, доступ до них і т. д.)) і технічних засобів (використання програм і приладів для збереження конфіденційності даних);
- розробку (створення нових), експлуатацію і вдосконалення вже наявних засобів захисту інформації;
- перманентний контроль над дієвістю заходів, що вживаються в галузі забезпечення інформаційної безпеки.

Організаційний захист інформації знаходиться в зведенні правил, складених на основі правових актів, покликаних запобігти неправомірне заволодіння конфіденційними даними.

Організаційний метод забезпечення інформаційної безпеки має складові, які вказані на рис. 1.3.

Захист інформаційної інфраструктури від несанкціонованого доступу забезпечується регламентацією доступу суб'єктів (працівників) до об'єктів (носіїв даних і каналам їх передачі). Організаційний метод забезпечення інформаційної безпеки не має на увазі використання технічного інструментарію. Така інформаційна безпека часто складається, наприклад, у видаленні ОТЗС за периметр території, що охороняється на максимально можливу відстань.

Застосування ж технічного обладнання і різних програм для забезпечення інформаційної безпеки, включаючи системи управління базами даних, прикладне програмне забезпечення, різні шифрувальники, DLP-системи і SIEM-системи, що виключають виток даних через комп'ютерну мережу, вже належить до технічного методу забезпечення інформаційного захисту [23, с. 17].

Організаційно-технічні заходи в обов'язковому порядку повинні відповідати правовим методам забезпечення інформаційної безпеки,

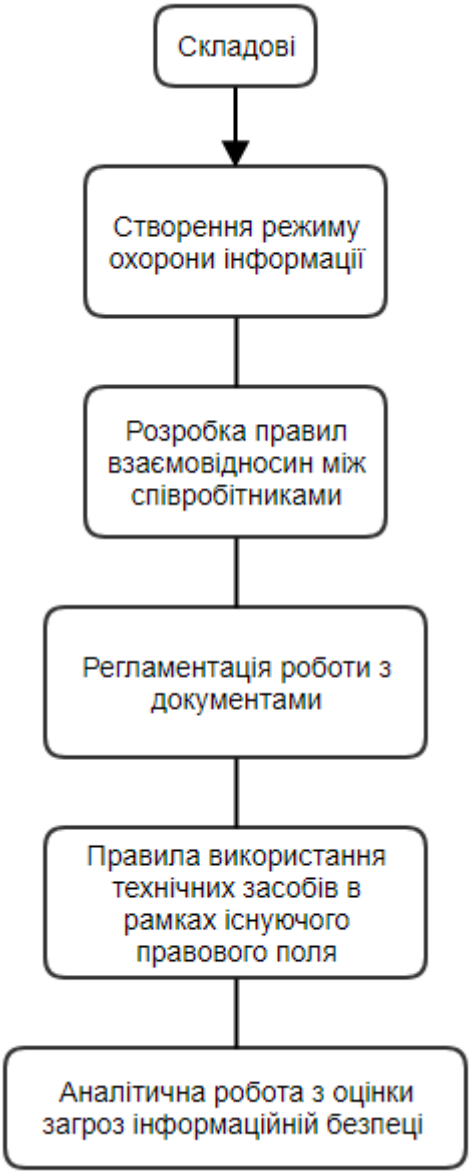


Рис. 1.3 Складові організаційного методу інформаційної безпеки

запропонованим нормативними документами. Політіка інформаційної безпеки розробляється з урахуванням існування безлічі підсистем, включаючи:

- підсистему надання доступу;
- підсистему реєстрації та обліку;
- підсистему щодо забезпечення безпеки за рахунок використання шифрів.

Також важливу роль відіграє захист мовної інформації на підприємстві. Для забезпечення інформаційного захисту акустичної інформації рекомендується компактно розташувати захищаючі приміщення, чітко

встановити периметр території, що охороняється, регламентувати допуск працівників на територію, на яку поширюється інформаційний захист.

Інформаційна безпека також полягає в тому, щоб регулярно обстежувати приміщення і встановлені в них технічні засоби на предмет наявності пристосувань для несанкціонованого отримання інформації. Для посилення інформаційної безпеки можна використовувати віброізоляцію, та звукоізоляцію, екранування, автономізацію ОТЗС в межах території, що охороняється, а також тимчасове відключення ОТЗС. Также використовуються активні та пасивні механізми забезпечення мовної безпеки (див.рис. 1.4).

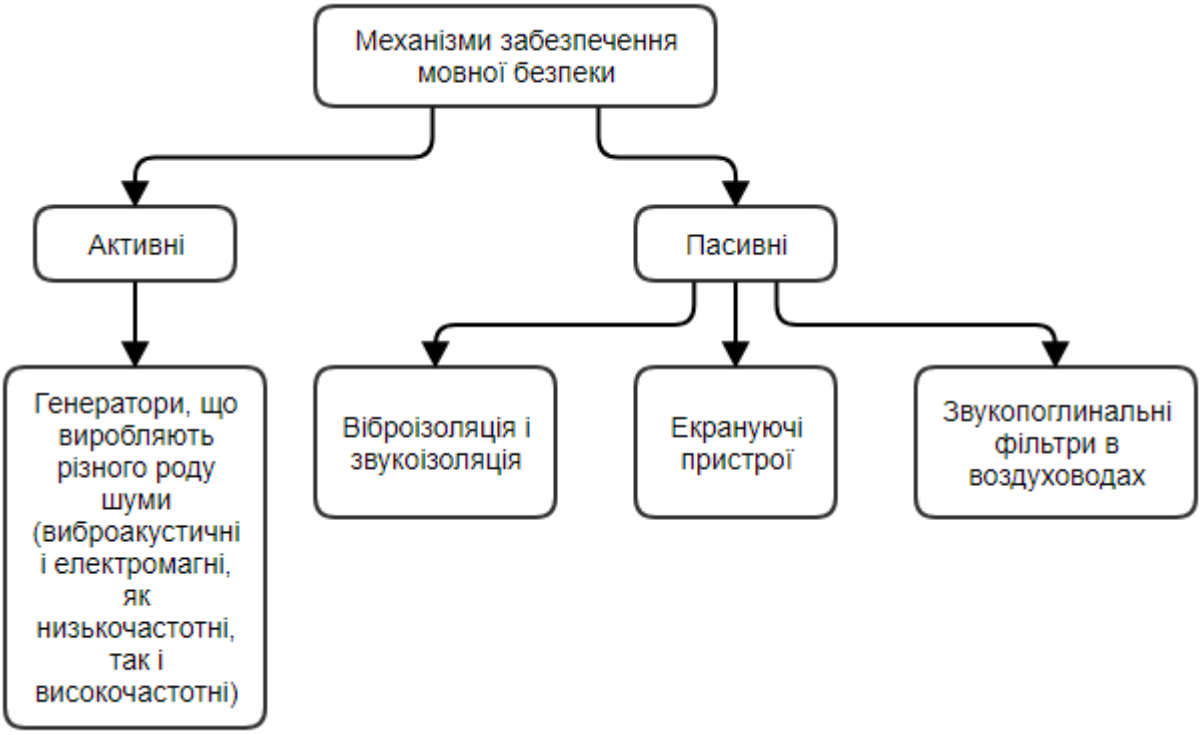


Рис. 1.4 Механізми забезпечення мовної безпеки на підприємстві

Для забезпечення інформаційного захисту даних, що зберігаються і передаються технічними засобами використовують: аутентифікацію; регламентування доступу до об'єктів; шифруючу систему файлів; ключі; безпечні з'єднання; IPsec.

Економічна складова інформаційної безпеки включає [24]:

- складання програм по забезпеченню інформаційної безпеки;

- визначення джерел їх фінансового забезпечення;
- розробку порядку фінансування;
- створення механізму страхування інформаційних ризиків.

Основне правило економічного методу - вартість системи інформаційної безпеки не повинна бути вище, ніж вартість захищаючих відомостей.

Правова складова інформаційної безпеки включає [24]:

- ліцензування діяльності в частині забезпечення інформаційної безпеки;
- сертифікації технічних засобів інформаційного захисту;
- атестації об'єктів інформатизації згідно відповідності нормам інформаційної безпеки.

Таким чином, були приведені вимоги методичних матеріалів до організації інформаційної безпеки, які дають можливість врахувати їх при організації системи інформаційної безпеки підприємства.

## 1.2 Організація інформаційної безпеки підприємства

Організація – процес поділу, групування та координації робіт, видів діяльності і ресурсів для досягнення поставлених цілей[25]. Реалізація функції організації здійснюється у процесі організаційної діяльності.

Організаційний процес – це достатньо складний вид діяльності який потребує певного досвіду та високого рівня фахових знань і вмінь[26]. Кінцевим результатом організаційної діяльності є вибір певної позиції у діапазонах всіх елементів організаційної діяльності (рис 1.5).

Поділ праці - поділ загальної роботи на окремі складові частини, достатні для виконання окремим працівником відповідно до його кваліфікації та здібностей [25];

Створення підрозділів (департаменталізація) - групування робіт та видів діяльності у певні блоки (підрозділи: групи, відділи, сектори, цехи, виробництва тощо) [25];

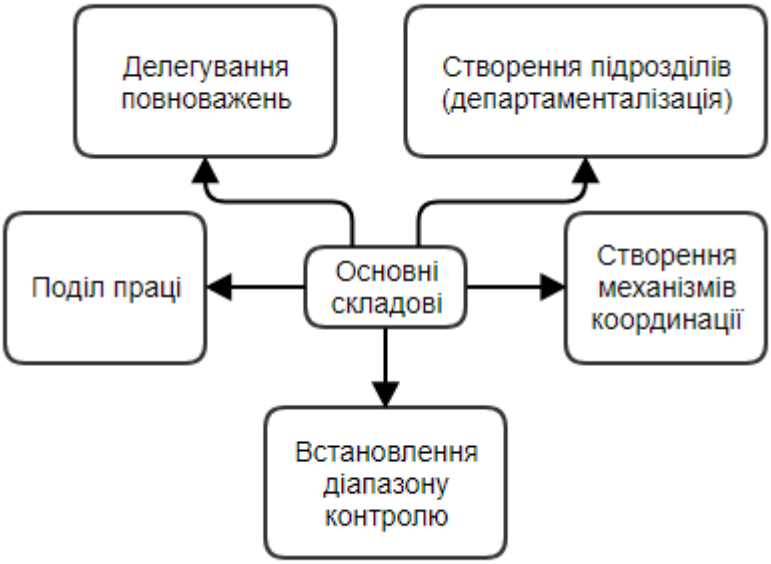


Рис. 1.5 Основні складові організаційного процесу (організаційної діяльності)

Делегування повноважень - підпорядкування кожного підрозділу керівникові, встановлення обовязків та повноважень керівників, створення системи підпорядкування [25];

Встановлення діапазону контролю - визначення кількості працівників, безпосередньо підлеглих кожному менеджерові [25];

Створення механізмів координації - забезпечення вертикальної та горизонтальної координації робіт та видів діяльності за рахунок розроблення алгоритму прийняття рішень, створення комунікаційних каналів, систем обліку, звітності, зворотного звязку [25].

Підприємства та організації сфери економіки, бізнесу та фінансів – найбільш численні структури, в яких створюється найбільший обсяг (кількість) інформації, яка містить державну і конфіденційну таємницю. У них проводиться конкретна і різноманітна робота по захисту інформації. Система інформаційної безпеки підприємства повинна базуватися на принципах, які зазначені на рис.1.6.

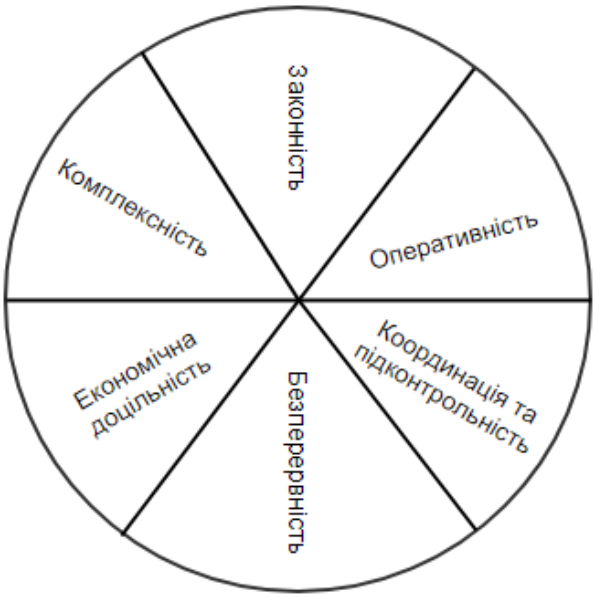


Рис. 1.6 Принципи системи інформаційної безпеки підприємства

Законність передбачає, що діяльність осіб, які забезпечують інформаційну безпеку, повинна носити законний характер, інакше весь захисний механізм може виявитися ненадійним з вини самого суб'єкта підприємницької діяльності. В якості несприятливих наслідків можливі різноманітні санкції правоохоронних органів, залучення в якості відповідача в суд, шантаж з боку кримінальних структур і т.д [27].

Комплексність, тобто можлива взаємодія всіх підрозділів підприємства з метою забезпечення необхідного рівня захисту, створення клімату співпраці та довіри.

Економічна доцільність, означає, що в першу чергу слід організовувати інформаційну безпеку тих об'єктів, витрати на захист яких менше, ніж втрати від незаконного їх використання. У цьому випадку повинні враховуватися також фінансові можливості організації.

Безперервність припускає, що функціонування комплексної системи забезпечення інформаційної безпеки підприємництва має здійснюватися постійно.

Оперативність забезпечується швидкодією спеціальних інформаційних служб та ефективністю проведених заходів щодо доведення потрібної

інформації з технологічних ланцюжків, а також своєчасним інформуванням адміністрації підприємства.

Координація та підконтрольність системи забезпечення інформаційної безпеки керівництву суб'єкта підприємницької діяльності необхідно, по-перше, для того, щоб локальна система безпеки не виявилася зорієнтована на вирішення вузьких завдань, без урахування інтересів партнерів та інших структурних підрозділів; по-друге, для правильної оцінки ефективності системи інформаційного забезпечення підприємства та її можливого вдосконалення.

В рамках підприємства має бути забезпечено організацію служби інформаційної безпеки [28]. Серед суб'єктів, які забезпечують захист інформаційної безпеки підприємницької діяльності, найбільше значення має служба власної безпеки, звичайно, при наявності у підприємців необхідних для цього фінансових коштів. Можна виділити ряд етапів, рекомендованих підприємцям при забезпеченні інформаційної безпеки (див. рис. 1.7).

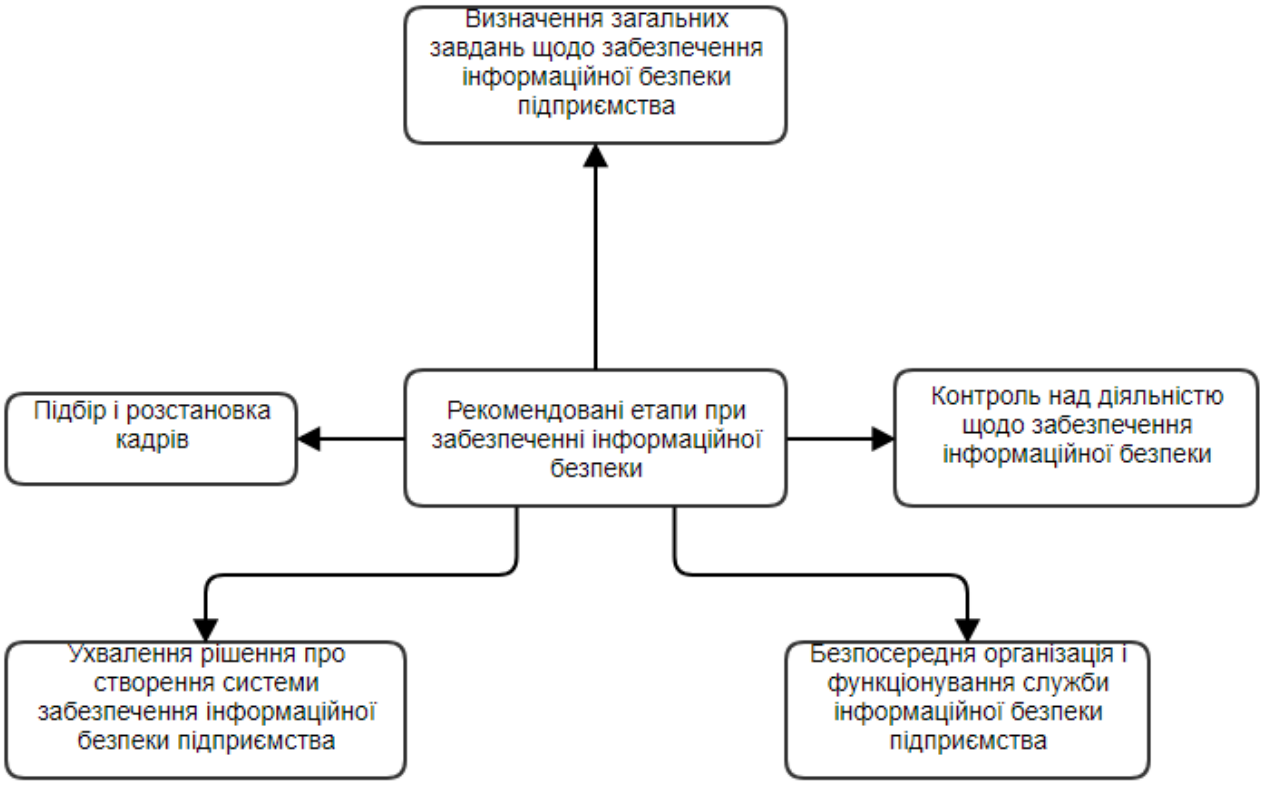


Рис. 1.7 Ряд рекомендованих підприємцям етапів, при забезпеченні інформаційної безпеки

Ухвалення рішення про створення системи забезпечення інформаційної безпеки підприємства повинно виникнути в момент прийняття рішення про організацію юридичної фірми в залежності від обраного виду діяльності, характеру передбачуваних послуг, використання приватної інформації, кількості працівників і т.д. На загальних зборах засновникам заздалегідь необхідно передбачити можливість створення спеціальної служби і розподілити обов'язки. Після державної реєстрації організації керівниками приймається остаточне рішення, визначаються відповідальні особи, які будуть безпосередньо займатися організацією служби інформаційної безпеки.

До визначення загальних завдань щодо забезпечення інформаційної безпеки підприємства, входять визначення передбачуваних загроз, їх попередження, встановлення конкретних об'єктів захисту (інформація, комп'ютерні системи, ключі доступу, безпека приміщень), та розробка положення про забезпечення інформаційної безпеки підприємства, визначення структури та кадрового складу осіб, які займаються даною роботою.

Під час організації системи інформаційної безпеки підприємства, також важливу роль відіграє підбір і розстановка кадрів. Працівниками служби інформаційної безпеки можуть бути люди, які мають спеціальні навички і вміють працювати з інформаційними технологіями. Важливим і ключовою умовою є саме професійна підготовка.

Безпосередня організація і функціонування служби інформаційної безпеки підприємства є невід’ємним етапом при забезпеченні інформаційної безпеки. Робота структурного підрозділу з інформаційної безпеки регламентується цілим рядом локальних актів, які слід розробити в рамках підприємства. Особам, які забезпечують інформаційну безпеку, забороняється надавати інші послуги, не пов'язані з роботою власного підприємства. У процесі діяльності значну роль відіграє вміла розстановка кадрів, розподіл прав і обов'язків. Важливим фактором є гнучка система стимулювання працівників служби. Фінансування зазвичай здійснюється з прибутку. Економія коштів, як правило, обертається набагато більшими втратами.

Якщо брати до уваги контроль над діяльністю щодо забезпечення інформаційної безпеки, то для підтримки високого рівня виробничої дисципліни, а також ефективної протидії різним зломів і інформаційним атакам необхідно здійснення постійного контролю та аналізу результатів даної діяльності. Для цього здійснюються:

- регулярні поточні звіти працівників, які займаються забезпеченням інформаційної безпеки, перед керівництвом підприємства;
- позапланові звіти щодо захисту від конкретних загроз і про вжиті організаційних і технічних заходи;
- аналіз звітів і формування позиції керівництва щодо ефективності системи інформаційної безпеки підприємства. Важливим елементом підтримання високого рівня захисту є вдосконалення ділових навичок працівників, зайнятих забезпеченням інформаційної безпеки, що досягається постійним підвищенням їх кваліфікації та перепідготовкою (не рідше ніж кожні три роки).

### 1.3 Аналіз загроз та ризиків інформаційної безпеки підприємства

Загрозою інформації називають потенційно можливий вплив або вплив на автоматизовану систему з подальшим нанесенням збитку чиїмось потребам. На сьогоднішній день існує більше ста позицій і різновидів загроз інформаційній системі. Важливо проаналізувати всі ризики за допомогою різних методик діагностики[29].

Загрози інформаційної безпеки проявляються не самостійно, а через можливу взаємодію з найбільш слабкими ланками системи захисту, тобто через фактори уразливості. Загроза призводить до порушення діяльності систем на конкретному об'єкти-носії. Основні уразливості виникають унаслідок дії наступних факторів:

- недосконаліть програмного забезпечення, апаратної платформи;

- різні характеристики будови автоматизованих систем в інформаційному потоці;
- частина процесів функціонування систем є неповноцінною;
- неточність протоколів обміну інформацією та інтерфейсу;
- складні умови експлуатації і розташування інформації.

Найчастіше джерела загрози запускаються з метою отримання незаконної вигоди внаслідок заподіяння шкоди інформації. Але можливо і випадкове дію загроз через недостатній мірі захисту і масового дії загрозливого фактора. Існує поділ вразливостей за класами, вони можуть бути: об'єктивними, випадковими і суб'єктивними. Якщо усунути або як мінімум послабити вплив вразливостей, можна уникнути повноцінної загрози, спрямованої на систему зберігання інформації.

Випадкові види вразливостей залежать від непередбачених обставин і особливостей оточення інформаційного середовища. Їх практично неможливо передбачити в інформаційному просторі, але важливо бути готовим до їх швидкого усунення. Усунути такі неполадки можна за допомогою проведення інженерно-технічного розгляду та відповідного удару, завданого загрозою інформаційній безпеці.

На рис. 1.8 та рис. 1.9 зображені випадкові види вразливостей.

Об'єктивні різновиди вразливостей безпосередньо залежать від технічної побудови обладнання на об'єкті, що вимагає захисту, і його характеристик. Повноцінне позбавлення від цих чинників неможливо, але їх часткове усунення досягається за допомогою інженерно-технічних прийомів, наступними способами:

Зміни, пов'язані з технічними засобами випромінювання:

- електромагнітні методики (побічні варіанти випромінювання і сигналів від кабельних ліній, елементів техзасобів);
- звукові варіанти (акустичні або з додаванням вібросигналів);
- електричні (прослизання сигналів в ланцюжки електричної мережі, за наведенням на лінії і провідники, по нерівномірного розподілу струму).

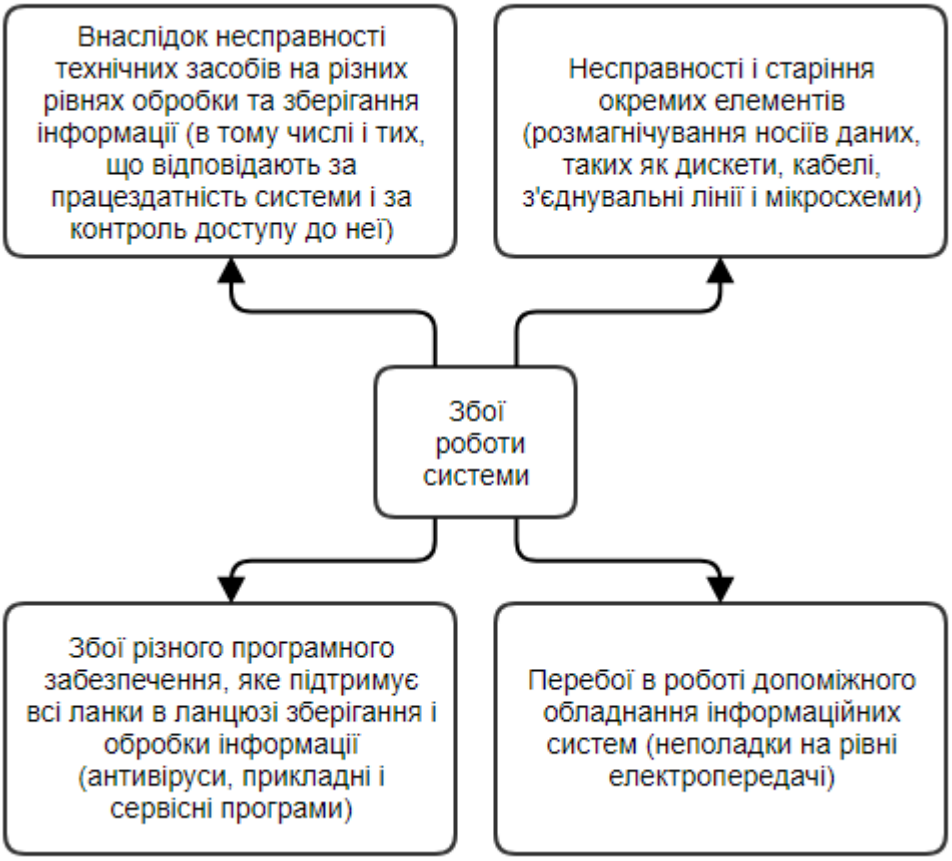


Рис. 1.8 Збої роботи системи

| Фактори які послабляють інформаційну безпеку | |
|---|---|
| Пошкодження комунікацій на зразок водопостачання або електропостачання, а також вентиляції, каналізації | Несправності в роботі захисних пристроїв (паркани, перекриття в будинку, корпусу обладнання, де зберігається інформація) |

Рис. 1.9 Фактори які послабляють інформаційну безпеку

Однією з найнебезпечніших на сьогоднішній день загроз інформаційної безпеки є комп'ютерні віруси. Це підтверджується багатомільйонним збитком, який несуть компанії в результаті вірусних атак[30]. В останні роки істотно збільшилася їх частота і рівень шкоди. На першому місці як і раніше залишається пошта, але, віруси здатні проникати і через програми обміну повідомленнями, такі як ICQ та інші. Збільшилася і кількість об'єктів для можливих вірусних атак [31]. Сьогодні віруси здатні впливати і на міжмережеві екрани, комутатори, мобільні пристрої, маршрутизатори. Останнім часом

особливо активні стали так звані віруси-шифрувальники. Навесні і влітку цього року мільйони користувачів постраждали від атак вірусів WannaCry, Petya, Misha. Епідемії показали, що жертвою вірусної атаки можна стати, навіть якщо не відкривати підозрілі листи. За інформацією Intel вірусом WannaCry заразилися 530 тисяч комп'ютерів, а загальний збиток компаній склав більше 1 млрд доларів [30].

Наряду з комп’ютерними вірусами, велику загрозу становлять DDoS атаки. Distributed-Denial-of-Service - «розподілена відмова від обслуговування» - це потік помилкових запитів від сотень тисяч географічно розподілених хостів, які блокують обраний ресурс одним з двох шляхів. Перший шлях - це пряма атака на канал зв'язку, який повністю блокується величезною кількістю непотрібних даних. Другий - атака безпосередньо на сервер ресурсу. Недоступність або погіршення якості роботи публічних веб-сервісів в результаті атак може тривати досить тривалий час, від декількох годин до декількох днів. Зазвичай подібні атаки використовуються в ході конкурентної боротьби, шантажу компаній або для відвернення уваги системних адміністраторів від деяких протиправних дій на кшталт викрадення грошових коштів з рахунків. Іноді керівники компаній намагаються заощадити на покупці ліцензійного ПЗ. Але слід знати, що неліцензійні програми не дають захисту від шахраїв, зацікавлених в крадіжці інформації за допомогою вірусів. Володар неліцензійного ПЗ не отримує технічної підтримки, своєчасних оновлень, що надаються компаніями-розробниками. Разом з ним він купує і віруси, здатні завдати шкоди системі комп'ютерної безпеки.

Об’єктивні уразливості:

- технологічні виходи з програм, що об'єднується терміном «програмні закладки»;
- закладки апаратури - фактори, які впроваджуються безпосередньо в телефонні лінії, в електричні мережі або просто в приміщення.

Суб'єктивні уразливості в більшості випадків являють собою результат неправильних дій співробітників на рівні розробки систем зберігання і захисту

інформації і тому усунення таких факторів можливо за допомогою методик з використанням апаратури і ПЗ (рис. 1.10).

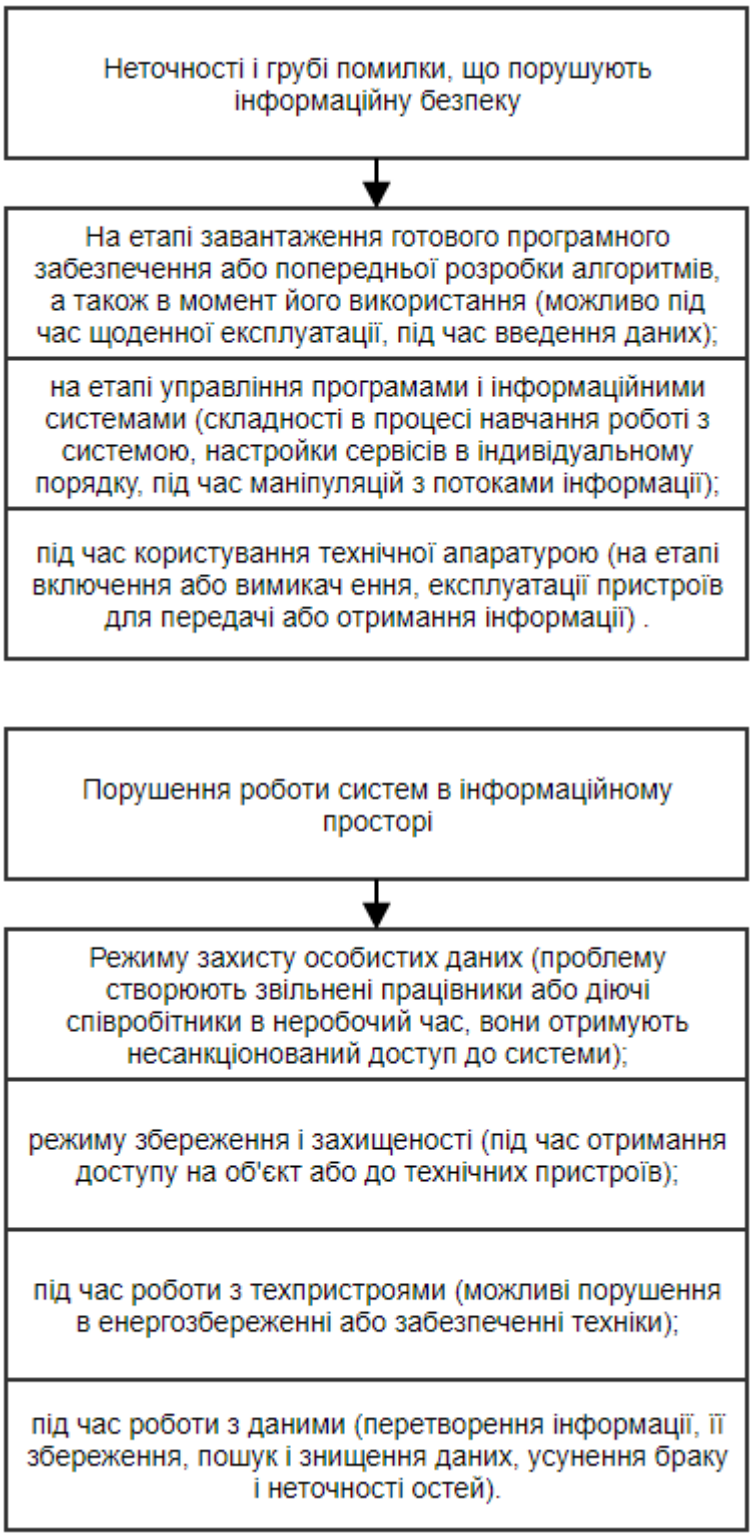


Рис. 1.10 Суб’єктивні уразливості інформаційної безпеки підприємства

Кожна вразливість повинна бути врахована і оцінена фахівцями. Тому важливо визначити критерії оцінки небезпеки виникнення загрози і ймовірності поломки або обходу захисту інформації [32]. Показники підраховуються за допомогою застосування ранжирування. Серед всіх критеріїв виділяють три основних:

Доступність - це критерій, який враховує, наскільки зручно джерела загроз використовувати певний вид уразливості, щоб порушити інформаційну безпеку. У показник входять технічні дані носія інформації (на кшталт габаритів апаратури, її складності і вартості, а також можливості використання для злому інформаційних систем неспеціалізованих систем і пристроїв) [33].

Фатальність - характеристика, яка оцінює глибину впливу уразливості на можливості програмістів впоратися з наслідками створеної загрози для інформаційних систем. Якщо оцінювати тільки об'єктивні уразливості, то визначається їх інформативність - здатність передати в інше місце корисний сигнал з конфіденційними даними без його деформації [33].

Кількісність - характеристика підрахунку деталей системи зберігання та реалізації інформації, яким притаманний будь-який вид уразливості в системі. Результати всіх аналізів зводяться в одну таблицю, ступінь впливу розбивається по класах для зручності підрахунку коефіцієнта уразливості системи [33].

Якщо описувати класифікацію загроз, які обходять захист інформаційної безпеки, то можна виділити кілька класів (рис. 1.11). Поняття класів обов'язково, адже воно спрощує і систематизує всі фактори без винятку.

Ранг навмисності здійснення втручання в інформаційну систему захисту:

- загроза, яку викликає недбалість персоналу в інформаційному вимірі;
- загроза, ініціатором якої є шахраї, і роблять вони це з метою особистої вигоди.

Характеристики появи загроз:

- загроза інформаційній безпеці, яка провокується руками людини і є штучною;

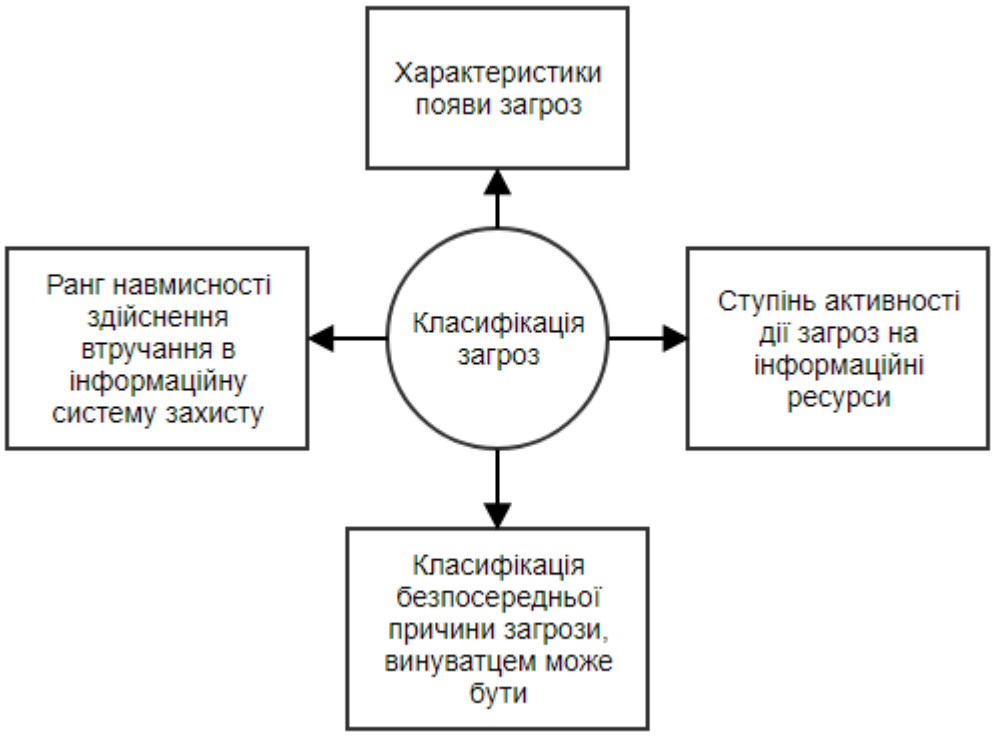


Рис. 1.11 Класифікація загроз, які обходять захист інформаційної безпеки підприємства

- природні загрозливі фактори, непідконтрольні інформаційними системами захисту і викликається стихійними лихами.

Класифікація безпосередньої причини загрози, винуватцем може бути:

- людина, яка розголошує конфіденційну інформацію, орудуючи за допомогою підкупу співробітників компанії;
- природний фактор, що приходить у вигляді катастрофи або локального лиха;
- програмне забезпечення із застосуванням спеціалізованих апаратів або впровадження шкідливого коду в техзасоби, що порушує функціонування системи;
- випадкове видалення даних, санкціоновані програмно-апаратні фонди, відмова в роботі операційної системи.

Ступінь активності дії загроз на інформаційні ресурси:

- в момент оброблення даних в інформаційному просторі (дія розсилок від вірусних утиліт);
- в момент отримання нової інформації;
- незалежно від активності роботи системи зберігання інформації (в разі розкриття шифрів або криптографічного захисту інформаційних даних).

Ще одна класифікація джерел загроз інформаційній безпеці, заснована на інших параметрах і також враховується під час аналізу несправності системи або її злому. До уваги береться наступне:

Стан джерела загрози:

- в самій системі, що призводить до помилок в роботі і збоїв при реалізації ресурсів АС;
- в межах видимості АС, наприклад, застосування підслуховуючої апаратури, викрадення інформації в роздрукованому вигляді або крадіжка записів з носіїв даних;
- шахрайство поза зоною дії АС.

Випадки, коли інформація захоплюється під час проходження по шляхах зв'язку, побічний захоплення з акустичних або електромагнітних випромінювань устройств.

Степінь впливу: активна загроза безпеки, яка вносить корективи в структуру системи і її сутність, наприклад, використання шкідливих вірусів або троянів; пасивна загроза - та різновид, яка просто краде інформацію способом копіювання, іноді прихована. Вона не вносить своїх змін в інформаційну систему.

Можливість доступу співробітників до системи програм або ресурсів: шкідливий вплив, то є загроза інформаційним даними може реалізуватися на кроці доступу до системи (несанкціонованого); шкода завдається після згоди доступу до ресурсів системи.

Способи доступу до основних ресурсів системи виділяють наступні загрози:

- застосування нестандартного каналу шляху до ресурсів, що включає в себе несанкціоноване використання можливостей операційної системи;
- використання стандартного каналу для відкриття доступу до ресурсів, наприклад, незаконне отримання паролів і інших параметрів з подальшим маскуванням під зареєстрованого в системі користувача.

Розміщення інформації, яка зберігається в системі: вид погроз доступу до інформації, яка розташовується на зовнішніх пристроях пам'яті, начебто несанкціонованого копіювання інформації з жорсткого диска, отримання доступу до інформації, яка показується терміналу, наприклад, запис з відеокамер терміналів; незаконне проникнення в канали зв'язку і підключення до них з метою отримання конфіденційної інформації або для підміни реально існуючих фактів під виглядом зареєстрованого співробітника.

При цьому не варто забувати про такі загрози, як випадкові і навмисні. В системах дані регулярно піддаються різним реакціям на всіх стадіях циклу обробки і зберігання інформації, а також під час функціонування системи. Як джерело випадкових реакцій виступають такі фактори, як:

- збої в роботі апаратури;
- періодичні шуми і фони в каналах зв'язку через вплив зовнішніх факторів (враховується пропускна здатність каналу, смуга пропускання);
- неточності в програмному забезпеченні;
- помилки в роботі співробітників або інших службовців в системі;
- специфіку функціонування середовищ и Ethernet;
- форс-мажори під час стихійних лих або частих відключень електропостачання.

Похибки і в функціонуванні програмного забезпечення зустрічаються найчастіше, а в результаті з'являється загроза. Всі програми розробляються людьми, тому не можна усунути людський фактор і помилки. Робочі станції, маршрутизатори, сервери побудовані на роботі людей. Чим вище складність програми, тим більше можливість розкриття в ній помилок і виявлення вразливостей, які призводять до погроз інформаційної безопасності. Частина

цих помилок не призводить до небажаних результатів, наприклад, до відключення роботи сервера, несанкціонованого використання ресурсів, непрацездатності системи. Такі платформи, на яких була викрадена інформація, можуть стати майданчиком для подальших атак і становлять загрозу інформаційній безпеці. Щоб забезпечити безпеку інформації в такому випадку, потрібно скористатися оновленнями. Встановити їх можна за допомогою паків, що випускаються розробниками. Встановлення несанкціонованих або неліцензійних програм може тільки погіршити ситуацію. Також можливі проблеми не тільки на рівні ПЗ, але і в цілому пов'язані з захистом безпеки інформації в сеті. Навмисна загроза безпеці інформації асоціюється з неправомірними діями злочинця. В якості інформаційного злочинця може виступати співробітник компанії, відвідувач інформаційного ресурсу, конкуренти або наймані особи. Причин для вчинення злочину може бути кілька: грошові мотиви, невдоволення роботою системи і її безпекою, бажання самоствердитися. Є можливість змоделювати дії зловмисника заздалегідь, особливо якщо знати його мета і мотиви вчинків: людина володіє інформацією про функціонування системи, її даних і параметрах.

Мастерство і знання шахрая дозволяють йому діяти на рівні розробника. Зловмисник здатний вибрати найвразливіше місце в системі і вільно проникнути до інформації, стати загрозою для нее. Заінтересованою особою може бути будь-яка людина, як свій співробітник, так і сторонній зловмисник.

Несанкціонірованний доступ - один з методів комп'ютерних правопорушень. Тобто особистість, яка здійснює несанкціонований доступ до інформації людини, порушує правила, які зафіксовані політикою безпеки. При такому доступі відкрито користуються похибками в системі захисту і проникають до ядра інформації. Некоректні настройки і установки методів захисту також збільшують можливість несанкціонованого доступу. Доступ і загроза інформаційній безпеці відбуваються як локальними методами, так і спеціальними апаратними установками. За допомогою доступу шахрай може не

тільки проникнути до інформації і скопіювати її, а й внести зміни, видалити дані. Робиться це за допомогою:

- перехоплення непрямих електромагнітних вилікуваних від апаратури або її елементів, від каналів зв'язку, електроживлення або сіток заземлення;
- технологічних панелей регулювання;
- локальних ліній доступу до даних (термінали адміністраторів системи або співробітників);
- міжмережевих екранів;
- методів виявлення помилок.

Зі всіх методів доступу і загроз інформації можна умовно виділити основні (рис 1.12):

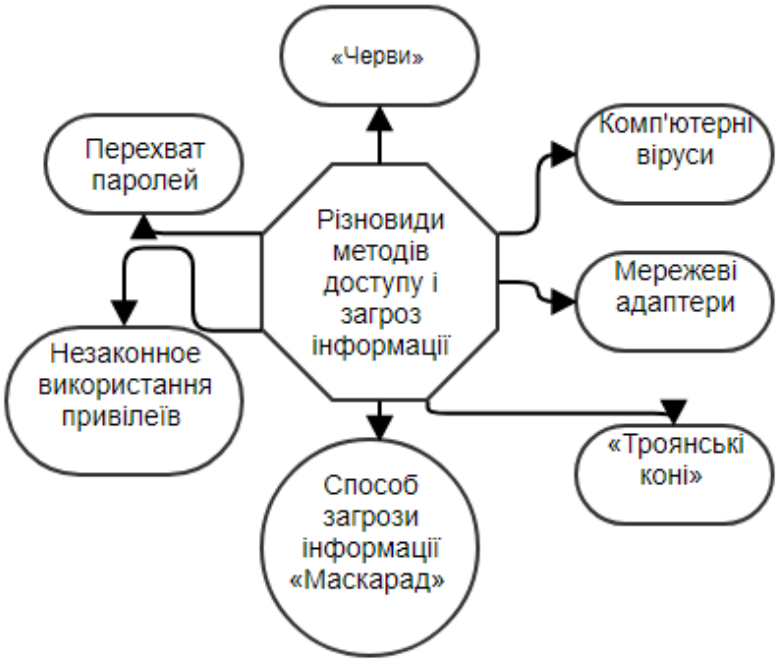


Рис. 1.12 Різновиди методів доступу і загроз інформації

Перехват паролів - поширена методика доступу, з якої стикалося більшість співробітників і тих, хто займається забезпеченням інформаційної безпеки. Це шахрайство можливо за участю спеціальних програм, які імітують на екрані

монітора віконце для введення імені і пароля. Введені дані потрапляють до рук зловмисника, і далі на дисплеї з'являється повідомлення про неправильну роботу системи. Потім можливе повторне спливання віконця авторизації, після чого дані знову потрапляють в руки перехоплювача інформації, і так забезпечується повноцінний доступ до системи, можливе внесення власних змін. Є й інші методики перехоплення пароля, тому варто користуватися шифруванням паролів під час передачі, а зробити це можна за допомогою спеціальних програм або RSA.

Способ загрози інформації «Маскарад» багато в чому є продовженням попередньої методики. Суть полягає в діях в інформаційній системі від імені іншої людини в мережі компанії. Існують такі можливості реалізації планів зловмисників в системі:

- передача помилкових даних в системі від імені іншої людини;
- авторизація в інформаційну систему під даними іншого співробітника і подальше вчинення дій (з попередніми перехопленням пароля).

Особливо небезпечний «Маскарад» в банківських системах, де маніпуляції з платежами призводять компанію в збиток, а вина і відповідальність накладаються на іншу людину. Крім того, страждають клієнти банка.

Незаконное використання привілеїв - назва різновиду розкрадання інформації і підриву безпеки інформаційної системи говорить сама за себе. Саме адміністратори наділені максимальним списком дій, ці люди і стають жертвами зловмисників. При використанні цієї тактики відбувається продовження «маскараду», коли співробітник або третя особа отримує доступ до системи від імені адміністратора і чинить незаконні маніпуляції в обхід системи захисту інформації. Але є нюанс: в цьому варіанті злочину потрібно перехопити список привілеїв з системи попередньо. Це може статися і з вини самого адміністратора. Для цього потрібно знайти похибку в системі захисту і проникнути в неї несанкціонірованно. Загроза інформаційної безпеки може здійснюватися на навмисному рівні під час транспортування даних. Це актуально для систем телекомунікацій і інформаційних сіток. Умисне

порушення не варто плутати з санкціонованими модифікаціями інформації. Останній варіант виконується особами, які мають повноваження і обґрунтовані завдання, що вимагають внесення змін. Порушення призводять до розриву системи або повного видалення данних. Існує також загроза інформаційній безпеці, яка порушує конфіденційність даних і їх секретність. Всі відомості отримує третя особа, тобто стороння людина без права доступу. Порушення конфіденційності інформації має місце завжди при отриманні несанкціонованого доступу до системи. Загроза захисту безпеки інформації може порушити працездатність компанії або окремого співробітника. Це ситуації, в яких блокується доступ до інформації або ресурсів її отримання. Один співробітник створює навмисно або випадково блокує ситуацію, а другий в цей час натикається на блокування і отримує відмову в обслуговуванні.

Наприклад, збій можливий під час комутації каналів або пакетів, а також загроза виникає в момент передачі інформації по супутникових систем. Їх відносять до первинних або безпосередніх варіантів, оскільки створення веде до прямого впливу на дані, що знаходяться під захистом.

Комп'ютерні віруси, що порушують інформаційну безпеку. Вони впливають на інформаційну систему одного комп'ютера або мережі ПК після попадання в програму і самостійного розмноження. Віруси здатні зупинити дію системи, але в основному вони діють локально.

«Черви» - модифікація вірусних програм, що призводить інформаційну систему в стан блокування і перевантаження. ПЗ активується і розмножується самостійно, під час кожного завантаження комп'ютера. Відбувається перевантаження каналів пам'яті і зв'язку.

«Троянські коні» - програми, які впроваджуються на комп'ютер під виглядом корисного забезпечення. Але насправді вони копіюють персональні файли, передають їх зловмисникові, руйнують корисну інформацію. Навість захисна система комп'ютера являє собою ряд загроз захисту безпеки. Тому програмістам необхідно враховувати загрозу огляду параметрів системи захисту.

Іноді загрозою можуть стати і нешкідливі мережеві адаптери. Важливо визначити конфігурацію системи захисту, її характеристики і передбачити можливі шляхи обходу. Після ретельного аналізу можна зрозуміти, які системи вимагають найбільшою мірою захищеності (акцент на вразливості). Розкриття параметрів системи захисту відносять до непрямих загроз безпеки. Справа в тому, що розкриття параметрів не дасть реалізувати шахраєві свій план і скопіювати інформацію, внести в неї зміни. Зловмисник тільки зрозуміє, за яким принципом потрібно діяти і як реалізувати пряму загрозу захисту безпеки інформації.

На великих підприємствах методами, що захищають інформаційну безпеку, повинна займатися спеціальна служба безпеки компанії. Її співробітники повинні шукати способи впливу на інформацію і усувати всілякі прориви зловмисників. За локальним актам розробляється політика безпеки, яку важливо строго дотримуватися. Варто звернути увагу і на виключення людського фактору, а також підтримувати в справності всі технічні засоби, пов'язані з безпекою інформації. Збитки, які наносяться загрозами степені і прояви шкоди можуть бути різними (рис. 1.13).

| Збитки | |
|---|---|
| Моральний і матеріальний збиток, нанесений фізичним особам, чия інформація була викрадена | Фінансовий збиток, нанесений шахраєм в зв'язку з витратами на відновлення систем інформації |
| Матеріальні витрати, пов'язані з неможливістю виконання роботи через зміни в системі захисту інформації | Моральний збиток, пов'язаний з діловою репутацією компанії або спричинив порушення взаємин на світовому рівні |
| Можливість заподіяння шкоди є у особи, яка вчинила правопорушення (отримало несанкціонований доступ до інформації, або стався злам систем захисту) | Також збиток може бути завдано незалежно від суб'єкта, який володіє інформацією, а внаслідок зовнішніх факторів і впливів (техногенних катастроф, стихійних лих). |

Рис. 1.13 Збитки, які наносяться загрозами степені і прояви шкоди

У першому випадку вина лягає на суб'єкта, а також визначається склад злочину і виноситься покарання за допомогою судового розгляду. Можливо вчинення діяння: з злочинним умислом (прямим або непрямим); по необережності (без умисного заподіяння шкоди). Відповідальність за правопорушення по відношенню до інформаційних систем вибирається згідно з чинним законодавством країни, зокрема, за кримінальним кодексом у першому випадку. Якщо злочин скоєно з необережності, а збиток нанесений в малих розмірах, то ситуацію розглядає громадянське, адміністративне або арбітражне право. Збитком інформаційного простору вважаються невигідні для власника (в даному випадку інформації) наслідки, пов'язані з втратою матеріального майна. Наслідки проявляються в результаті правопорушення. Висловити збиток інформаційних систем можна в вигляді зменшення прибутку або її недоотримання, що розцінюється як упущена вигода. Головне, вчасно звернутися до суду і з'ясувати склад злочину. Збиток потрібно класифікувати згідно з правовими актам і довести його в судовому процесі, а ще важливо виявити розмір діяння особистостей, розмір їх покарання на основі законодавства. Такими злочинами і безпекою найчастіше займається кіберполіція або служба безпеки країни в залежності від обсягу і значимості втручання в інформацію.

Етап захисту інформації сьогодні вважається актуальним і потрібно будь-якому підприємству. Захищати треба не тільки ПК, але і всі техпристрої, що контактують з інформацією. Всі дані можуть стати зброєю в руках зловмисників, тому конфіденційність сучасних IT-систем повинна знаходитися на вищому рівні. Ще не придуманий універсальний спосіб, який підходить кожному і дає стовідсотковий захист інформаційній безпеці підприємства. Важливо зупинити проникнення зловмисників на ранньому рівні.

## 1.4 Аналіз людського фактору як фактора безпеки підприємства

Забезпечення інформаційної безпеки підприємства, в якій з розвитком і ускладненням техніки пропорційно зростає значення людського фактора, можна знайти вже в багатьох сферах професійної діяльності людини. У ризикових професійних системах (виробнича, транспортна енергетична, інформаційна та ін.), швидше, ніж в інших місцях, людина звільняється від необхідності виконувати приватні операції і починає регулювати потужні потоки енергії та інформації. При цьому лавиноподібно зростають рівень його відповідальності і ціна допускаються помилок.

Не дивлячись на це, у всіх існуючих системах управління безпеки не враховується факт, що найбільша загроза є сама людина. Сучасні технічні засоби спостереження, контролю та обробки інформації не мають і не будуть ще довго мати здатність до мислення і швидку комплексну оцінку виниклої ситуації. Тому, єдине ефективне рішення проблеми оптимізації безпеки може бути тільки реалізація ідеї створення єдиної людини - технічної системи управління безпеки, де провідну роль буде мати людина. Один з підходів дослідження впливу людини на безпеку, це використання комплексного або часткового факторного аналізу. Тут, прикладений підхід розкриває багатогранність проблеми і намагається назвати основні чинники, що представляють собою складові частини поняття «людський фактор», як наприклад - професійна підготовка, фізичний стан та обмеження, психологічні особливості, фактори навколишнього середовища, фактори соціального середовища, фактори культури, чинники екіпажу , фактори об'єкта експлуатації та ін.

В основі комплексного факторного аналізу дослідження впливу людини на безпеку ставитися можливість вирішення загального завдання через реалізацію приватних блоків, пов'язаних з урахуванням людського фактора (рис. 1.14).

Розподіл на блоки, з позначенням основних напрямків діяльності компаній в кожному з них, з одного боку, дозволяє виробити напрямки їх зусиль в цих областях, з іншого боку, становить основу для оцінки ефективності системи безпеки підприємства, експертами.

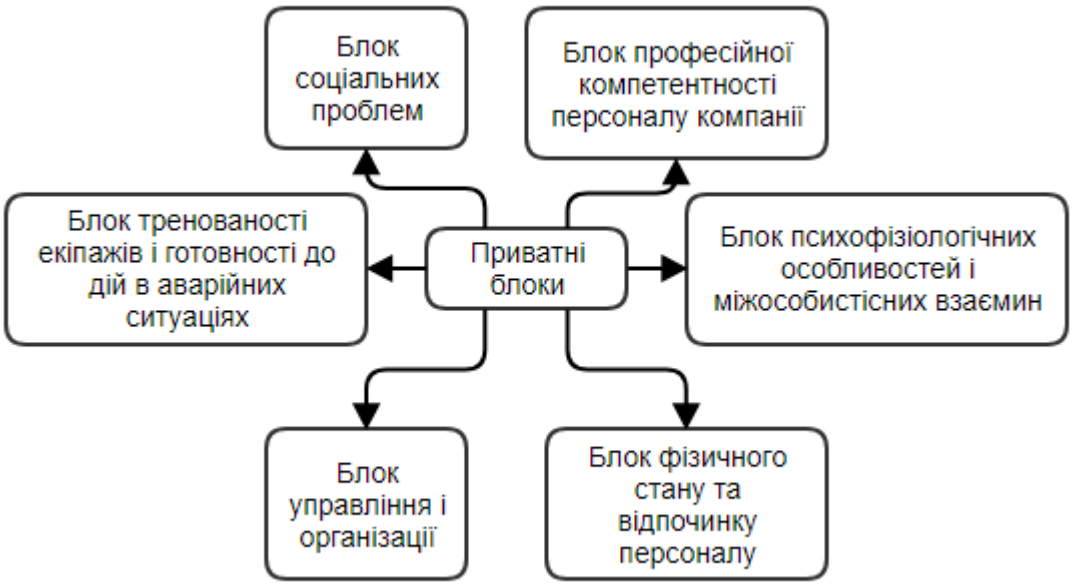


Рис. 1.14 Приватні блоки в основі комплексного факторного аналізу дослідження впливу людини на безпеку

Інший підхід, це дослідження процесів виникнення помилок і можливостей прогнозування переходу ситуації в аварійну. Підходи проведення комплексного або часткового факторного аналізу для вирішення проблем людського впливу на безпеку пов'язані безпосередньо з можливостями повного визначення і врахування всіх факторів, що впливають на ймовірність здійснення помилок і виникнення аварійної ситуації. Щоб полегшити визначення ступеня впливу різних дестабілізуючих факторів, необхідно розробити модель розвитку кожної досліджуваної аварійної ситуації. Така модель повинна розділити дестабілізуючі фактори по групах (напрямках) і повинна дозволити врахувати індивідуальних особливостей людей. Основною ланкою пропонованої моделі є керівник, який повинен враховувати всі фактори, як технічні, так і психофізіологічні. Після аналізу окремих ситуацій і обліку дестабілізуючих чинників необхідно визначити ймовірність здійснення помилок операторів.

Помилки, що здійснюються людьми, зазвичай класифікуються як - порушення, небезпечні помилки, критичні помилки (в залежності від тяжкості наслідків від настання помилки). Крім того повинні бути розроблені способи

запобігання виникненню помилок і методи зменшення наслідків здійснення помилок.

Незалежно від кількості і якості накопичених показників психофізіологічного стану людини, однозначно визначити залежність його помилки від різних дестабілізуючих факторів на сьогоднішній день не представляється можливим.

Детальна процедура повинна включати наступні етапи вирішення цього завдання:

- визначення та класифікація узагальнених експлуатаційних ситуацій;
- розподіл кожної ситуації на окремі етапи і простіших "під - ситуацій";
- описати всіх послідовних окремих операцій, що здійснюються людиною в кожній з виявлених ситуацій;
- визначення і ранжування дестабілізуючих чинників як за ймовірністю їх прояви, так і за наслідками від скоєних під їх тиском людських помилок;
- визначення "правил дій" людей в різних ситуаціях; визначення основних типів помилок операторів для кожної ситуації;
- розрахунок ймовірність появи помилок при виконанні окремих дій;
- складання професіограми і псіхограмми кожного оператора;
- розробка методики визначення індивідуальних особливостей людей;
- вивчення "законів поведінки" людей в різних ситуаціях;
- визначення залежності між дестабілізуючими факторами і індивідуальними особливостями операторів;

Передбачити всі помилки людини і розкрити закономірності впливу дуже різноманітного комплексу дестабілізуючих факторів на безпеку підприємства, поки є невозможним. Від людини оператора систем штучного інтелекту можна передати, як прості функцій спостереження і контролю, так і більш інтелектуальні, пов'язані з виробленням рішення по оцінку і прогнозом обстановки, а також з управління професійної ситеми (як у простих, так і в позаштатних ситуацій). При використанні таких інтелектуальних систем, кваліфікація людини - оператора жодною мірою не ставиться під сумнівом.

Створені системи підтримки прийняття рішень підвищують значно обґрунтованість рішень, прийнятих в ординарних умовах, але не можуть надавати реальну підтримку керівникам на етапах виникнення, розвитку та ліквідації аварійних ситуацій. Самим доступним способом оптимізації впливу «людського фактора» на безпеку вважається удосконалення і розвиток системи професійної підготовки.

На підставі аналізу зазначених та інших існуючих підходів врахування впливу людського фактора на безпеку, можна зробити деякі узагальнення висновків. Основний недолік цих та інших подібних підходів полягає в описовості виробничих процесів у відповідності зі стандартами якості і в визначенні правил дій без детального визначення та обліку "законів поведінки" людей. Визначення "законів поведінки", в свою чергу, пов'язано зі створенням психологічної служби та щоденного психологічного забезпечення професійної діяльності всіх працівників компанії, що на практиці є нездійсненним.

В кінцевому підсумку вони залишаються невирішеними завданнями для визначення впливу людського фактора на безпеку:

- детальна класифікація дестабілізуючих чинників;
- уточнення умов переходу штатних ситуацій в небезпечних і критичних;
- розробка методику обліку індивідуальних особливостей поведінки людей в різних умовах їх професійної діяльності;

Найважливіша особливість результатів дослідження людської поведінки відбудеться в тому, що практично ніде не вказується на будь-яких чинників, які можуть бути постійним корективом для оцінки і прогнозування поведінки людини в різних життєвих ситуаціях. Дослідження природи людської поведінки, як в ординарних, так і в екстремальних ситуаціях поки знаходиться на початковому стадії розвитку. Тут перешкодою є багатоваріантність модельованих процесів, яка веде до несистематичності в дослідженнях і не дозволяє повністю розкрити всіх закономірностей впливу виявлених психогенних факторів. Можна вказати на різні підходи дослідження людської поведінки як, наприклад вивчення "Психологія колективу (екіпажу)", роботи з

дослідження "культури безпеки", роботи зі складання деякої матриці індивіда таким чином, щоб можна було передбачити його поведінку.

Зараз, прогнозування поведінки людей зводитися зазвичай до діагностики когнітивних здібностей, тестування особистісних властивостей людини в рамках профвідбору та профорієнтації, дослідження окремих характеристик темпераменту або розкриття людських потреб. Але проблема впливу людського «фактора» на безпеку може бути вирішена тільки шляхом проведення комплексного теоретичного і експериментального дослідження людської поведінки, з охопленням всіх психодинамічних процесів, що супроводжують його діяльності.

Риси людини - зручні інструменти для аналізу індивідуальної структури людських потреб, консультування з питань вибору професії, але непридатні для аналізу причин небезпечної поведінки людини. Для повного врахування впливу людини на всіх аспектах безпеки підприємства потрібен новий підхід - підхід розгляду безпеки як «стан середовища» професійної діяльності. Такий підхід передбачає врахування людського поведінки у всіх трьох компонентах трудового процесу - технічний засіб (об'єкт), людина (суб'єкт) і умови роботи. Людина зі своїми рішеннями впливає як на стан об'єкта (якість проектування і виробництва), так і на надійність його експлуатації. Людина або оцінює, або сама визначає своєю поведінкою, всі умови проведення безпеки. Від нього залежить також рівень проведених заходів за чотирма найважливішими функціями забезпечення безпеки як такої - прогнозування очікуваних загроз, моніторинг обстановки, аналіз ситуацій і дій по забезпеченню безпеки.

Для реалізації запропонованого підходу необхідно вирішити такі головні завдання:

- розробка принципів і підходів оптимізації впливу людської поведінки як базовий фактор досягнення безпеки;
- розробка методологічних і організаційних основ оптимізації впливу людської поведінки на безпеку;

- обгрунтування комплексів критерій і заходів щодо вдосконалення систем управління безпекою;

Для реалізації завдання щодо оптимізації людської поведінки необхідно провести комплексне теоретичне і практичне дослідження в наступних напрямках:

- обгрунтування єдиної моделі людської поведінки, яка розкриває логіку мотивації і цілісну динаміку процесу прийняття рішення;
- розкриття «природних законів» поведінки людини і невідповідності їм існуючих правил;
- диференціація факторів, що впливають на безпеку, людської діяльності в різних ситуаціях;
- розробку науково-обґрунтованої методики обліку, оцінки, нормування та прогнозування дій виведених поведінкових факторів;
- теоретичному і експериментальному вивченні специфічних проблем безпеки окремих видів діяльності та виявлення випливають, в зв'язку з цим, особливостей людської поведінки;
- розробку методик перетворення і реорганізації всіх існуючих аспектів людської діяльності, на основі розроблених принципів і критеріїв обліку людського фактора.

Таким чином, був проведен аналіз людського фактору як фактора безпеки підприємства, що дає можливість врахувати їх при организації системи інформаційної безпеки підприємства.

**Висновки до першого розділу**

В першому розділі роботи було розглянуте: поняття та зміст організації інформаційної безпеки, описано методи та засоби забезпечення інформаційної безпеки та їх основні характеристики; вимоги щодо організації інформаційної безпеки підприємства в Україні; основні елементи та складові організації інформаційної безпеки підприємства в наш час. Також було розглянуто, як саме

людина впливає на інформаційну безпеку підприємства, та які загрози вона собою представляє.

Організація інформаційної безпеки є одною з найважливіших функцій під час функціонування підприємства в наш час. Тому, також немаловажним є побудова системи інформаційної безпеки на підприємстві.

# Розділ 2
# ПОБУДОВА СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У наш час багато підприємтсв і державних установ вирішують завдання створення системи інформаційної безпеки (СІБ), яка відповідала б стандартам інформаційної безпеки. Така проблема постає як перед молодими компаніями (які тільки починають свою діяльність), так і перед підприємствами і організаціями, давно присутніх на ринку, які приходять до необхідності модернізувати існуючу у них інформаційну інфраструктуру, що часто складніше, ніж створити всю систему з нуля. Тому проблема побудови системи інформаційної безпеки є немаловажною частиною при забезпеченні інформаційної безпеки на підприємтсві.

## 2.1 Методичні підходи до побудови системи інформаційної безпеки підприємства

Головною метою будь-якої системи інформаційної безпеки є забезпечення сталого функціонування об'єкта, запобігання загрозам його безпеки, захист законних інтересів від протиправних посягань, недопущення розкрадання фінансових коштів, розголошення, втрати, витоку, перекручування та знищення службової інформації, забезпечення нормальної виробничої діяльності всіх підрозділів об'єкта. Іншою метою системи інформаційної безпеки є підвищення якості послуг, що надаються і гарантій безпеки майнових прав та інтересів клієнтів.

Модель системи безпеки підприємста в інформаційній сфері (див.рис. 2.1) побудована відповідно до стандарту (ISO 15408) і даних аналізу ризиків (ISO/IEC 27002). Ця модель відповідає спеціальним нормативним документам із гарантування інформаційної безпеки, прийнятих в Україні, міжнародному стандарту ISO/IEC 15408 "Інформаційна технологія - методи захисту, критерії

оцінки інформаційної безпеки", стандарту ISO/IEC 27002 "Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів" і враховує тенденції розвитку вітчизняної нормативної бази з питань інформаційної безпеки.

Подана на рис. 2.1 модель інформаційної безпеки відображує сукупність об'єктивних зовнішніх і внутрішніх чинників та їх вплив на стан інформаційної безпеки на об'єкті і на збереження матеріальних або інформаційних ресурсів.

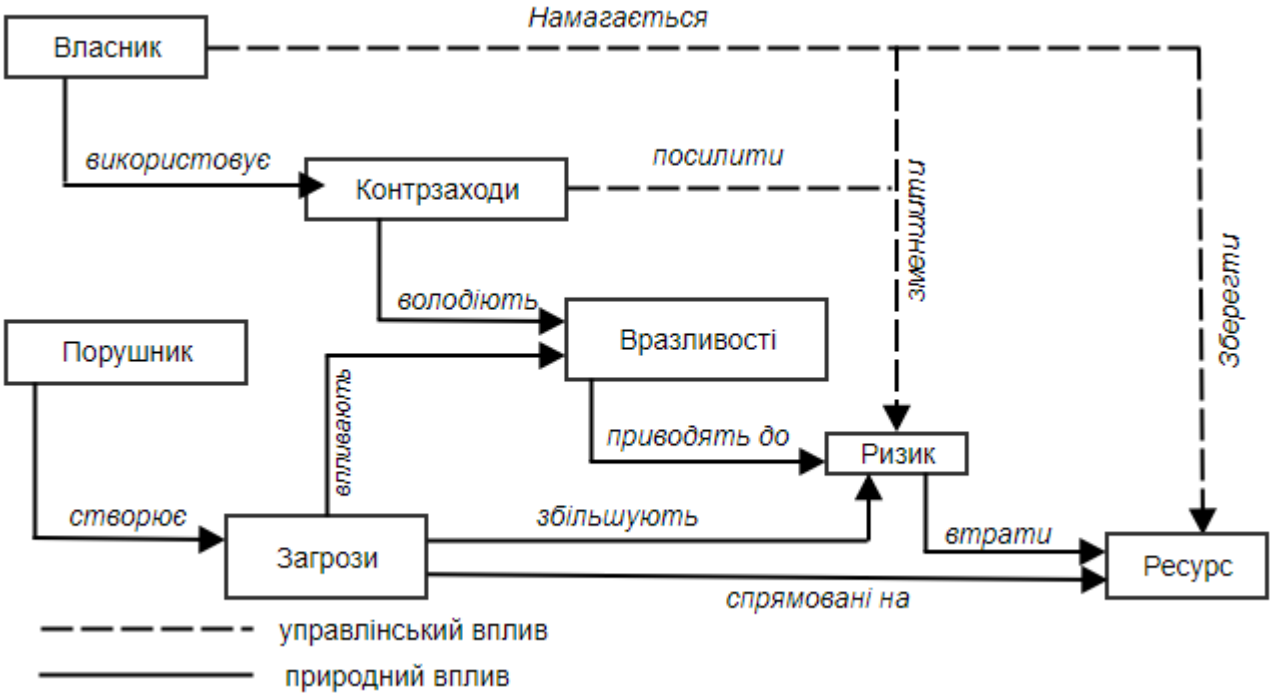


Рис. 2.1 Модель системи безпеки підприємства в інформаційній сфері [34]

Об'єктивні чинники моделі:

- загрози інформаційній безпеці, що характеризуються вірогідністю реалізації;
- вразливі місця інформаційної системи або системи контрзаходів (системи інформаційної безпеки);
- ризик - чинник, що відображує можливий збиток організації в результаті реалізації загрози інформаційної безпеки: просочування інформації та її неправомірного використання (ризик відображає вірогідні фінансові втрати - прямі або непрямі).

Для побудови збалансованої системи інформаційної безпеки потрібно спочатку провести аналіз ризиків у сфері інформаційної безпеки. Потім визначити оптимальний рівень ризику для організації на основі заданого критерію. Систему інформаційної безпеки (контрзаходи) потрібно будувати так, щоб досягти заданого рівня ризику.

Методика проведення аналітичних робіт дає змогу повністю проаналізувати і документально оформити вимоги щодо гарантування інформаційної безпеки послуг, що надаються, і гарантій безпеки майнових прав та інтересів клієнтів.

Досягти поставлених цілей можна при вирішенні таких основних завдань [35]:

- віднесення інформації до категорії обмеженого доступу (службова таємниця);
- прогнозування і своєчасне виявлення загроз безпеці інформаційних ресурсів причин і умов, що сприяють фінансовим, матеріальним і моральним збиткам, порушенню нормального функціонування і розвитку об'єкта;
- створення умов функціонування з найменшою вірогідністю реалізації загроз безпеці інформаційних ресурсів і зумовлення різних видів збитку;
- створення механізму і умов оперативного реагування на загрози інформаційній безпеці та прояви негативних тенденцій у функціонуванні, ефективне припинення посягань на ресурси на основі правових, організаційних і технічних заходів, засобів гарантування безпеки;
- створення умов для максимально можливого відшкодування і локалізації збитку, завданого неправомірними діями фізичних і юридичних осіб, ослаблення негативного впливу наслідків порушення інформаційної безпеки на досягнення стратегічних цілей.
- уникнути витрат на зайві заходи безпеки, що можливі у разі суб'єктивної оцінки ризиків;

- надати допомогу в плануванні і здійсненні захисту на всіх стадіях життєвого циклу інформаційних систем;
- забезпечити проведення робіт в короткі терміни;
- подати обґрунтування вибору заходів протидії;
- оцінити ефективність контрзаходів, порівняти різні варіанти їх.

У процесі виконання робіт мають бути встановлені межі дослідження. Для цього слід виділити ресурси інформаційної системи, щодо яких надалі будуть зроблені оцінки ризиків. При цьому необхідно розділити ці ресурси і зовнішні елементи, з якими здійснюється взаємодія. Ресурсами можуть бути засоби обчислювальної техніки, програмне забезпечення, дані. Прикладами зовнішніх-елементів є мережі зв'язку та інші засоби.

Наступною моделлю є, побудова моделі інформаційної технології. При побудові моделі слід враховувати взаємозв'язки між ресурсами. Наприклад, вихід із ладу якогось устаткування може призвести до втрати даних або виходу з ладу іншого критично важливого елемента системи. Подібні взаємозв'язки визначають основу побудови моделі організації з огляду на інформаційну безпеку. Цю модель, відповідно до пропонованої методики, будують такі: для виділених ресурсів визначають їх цінність огляду як на асоційовані з ними можливі фінансові втрати, так і на зниження репутації організації, дезорганізацію її діяльності, нематеріальні збитки від розголошування конфіденційної інформації і т. д. Потім описують взаємозв'язки ресурсів, визначають загрози безпеці й оцінюють вірогідність їх реалізації.

На основі побудованої моделі можна обґрунтовано вибрати систему контрзаходів, які знижують ризики до допустимих рівнів і мають найбільшу цінову ефективність. Частиною системи контрзаходів є рекомендації щодо проведення регулярних перевірок ефективності системи захисту.

Управління ризиком можна розглянути на методологічній основі процесу розробки і реалізації ризикових управлінських рішень. Підвищені вимоги до інформаційної безпеки припускають відповідні заходи на всіх етапах життєвого циклу інформаційних технологій. Планують ці заходи після закінчення етапу

аналізу ризиків і вибору контрзаходів. Обов'язковою складовою частиною цих планів є періодична перевірка відповідності існуючого режиму інформаційної безпеки політиці безпеки, сертифікації інформаційної системи (технології") на відповідність вимогам певного стандарту безпеки.

На завершення треба визначити міру гарантування безпеки інформаційного середовища замовника з оцінкою, на основі якої можна довіряти інформаційному середовищу об'єкта. Цей підхід припускає, що таке гарантування пов'язане з великими зусиллями при оцінювані безпеки.

Адекватність оцінки можлива при [36]:

- залученні до процесу оцінювання якомога більшої кількості елементів інформаційного середовища об'єкта замовника;
- досягнення певного рівня захищеності за рахунок використання при проектуванні системи гарантування безпеки більшої кількості проектів і описів деталей виконання;
- суворості робіт, яка полягає у застосуванні більшої кількості інструментів пошуку і методів виявлення менш очевидних слабких місць або на зменшення вірогідності їх наявності.

Мета процесу оцінювання ризиків полягає у визначенні їх характеристик в інформаційній системі та її ресурсах. На основі таких даних вибирають необхідні засоби управління інформаційною безпекою (рис. 2.2).

Ризик - це небезпека, якій може піддаватися система і організація, що використовує її. Він залежить від:

- показників цінності ресурсів;
- вірогідності завдання збитку ресурсам (що виражається через вірогідність реалізації загроз для ресурсів);
- ступеня легкості, від якого системи захисту вразливості можуть бути використані при виникненні загроз;
- існуючих або планованих засобів забезпечення інформаційної безпеки.

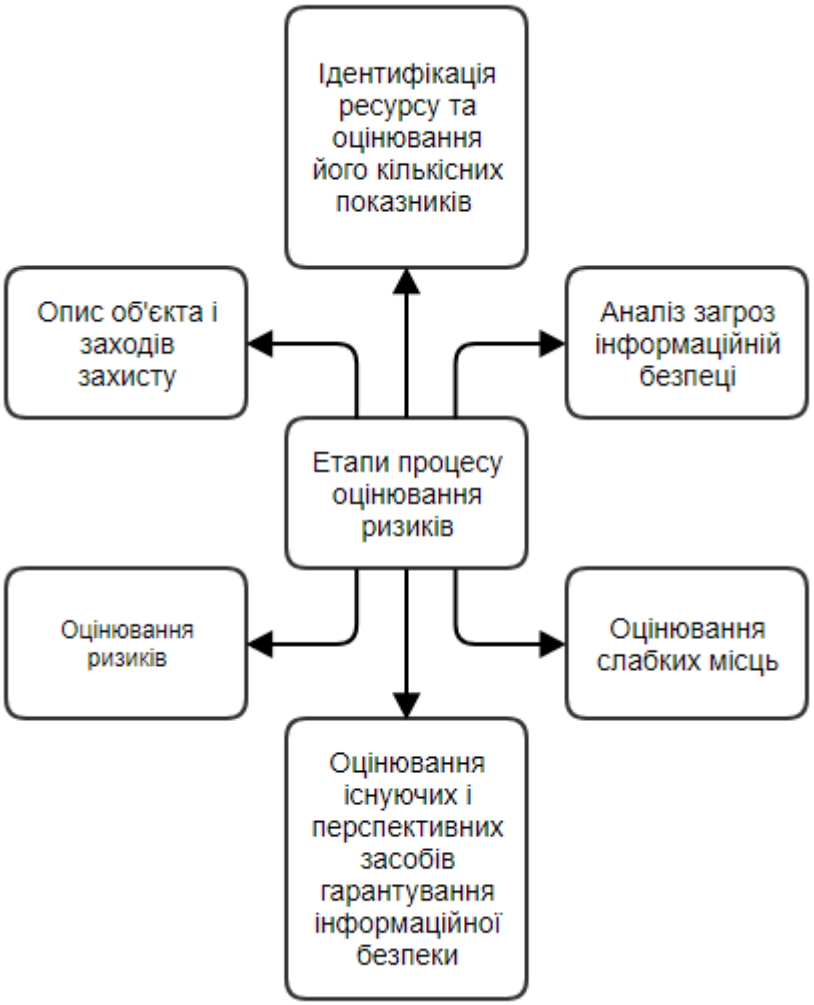


Рис. 2.2 Етапи процесу оцінювання ризиків

Обчислюють ці показники математичними методами, що мають такі характеристики, як обґрунтування і параметри точності.

На етапі побудови профілю захисту, розробляють план проектування системи захисту інформаційного середовища замовника; оцінюють доступні засоби, здійснюють аналіз і планують розроблення й інтеграцію засобів захисту. Необхідним елементом роботи є наявність у замовника допустимого ризику об'єкта захисту.

Роботу з побудови плану захисту об'єкта починають з побудови профілю захисту цього об'єкта. При цьому частина цієї роботи вже була виконана при проведенні аналізу ризиків (див.рис. 2.3).

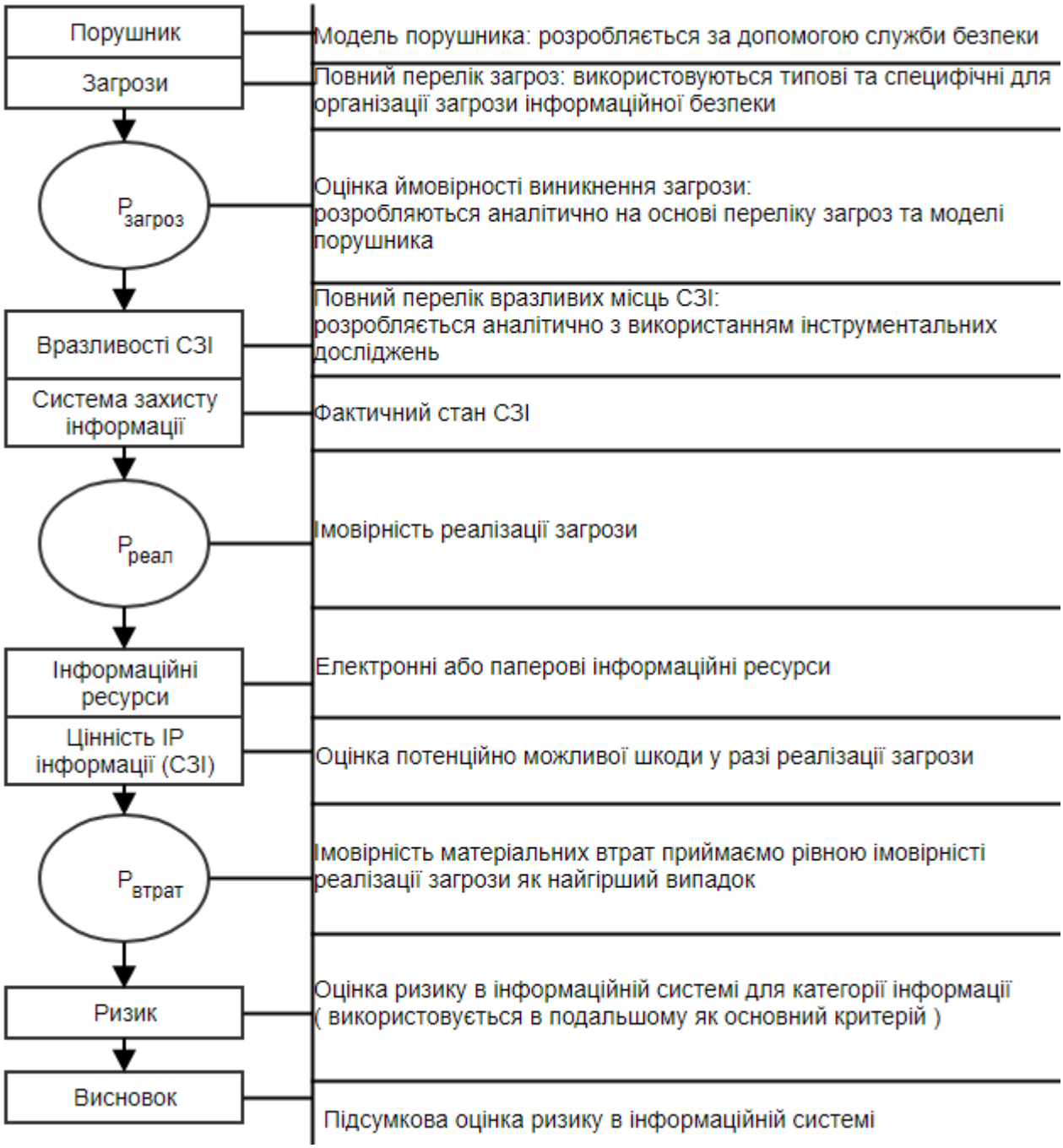


Рис. 2.3 Можливий алгоритм оцінювання інформаційних ризиків [37]

Перш ніж пропонувати будь-які технічні рішення за системою інформаційної безпеки об'єкта, слід розробити для нього політику безпеки. Власне організаційна політика безпеки описує порядок надання й використання прав доступу користувачів, а також вимоги звітності користувачів про свої дії з питань безпеки.

Система інформаційної безпеки об'єкта ефективна тоді, коли вона надійно підтримує виконання правил політики безпеки, і навпаки. Кроками побудови організаційної політики безпеки є:

- внесення до опису об'єкта автоматизації структури цінності і проведення аналізу ризиків;
- визначення правил будь-якого процесу користування цим видом доступу до ресурсів об'єкта автоматизації, що мають цей ступінь цінності.

Організаційну політику безпеки оформляють у вигляді документа, який узгоджують із замовником, затверджують.

Перш ніж визначити функціональні вимоги безпеки, потрібне формулювання цілей безпеки об'єкта. Деталізований опис загальної мети побудови системи безпеки об'єкта замовника виражається сукупністю чинників або критеріїв, які уточнюють мету. Сукупність чинників є основою визначення вимог до системи (вибір альтернатив). Чинники безпеки можна поділити на технологічні, технічні й організаційні.

Функціональні вимоги профілю захисту визначають з добре відомими, відпрацьованими і узгодженими функціональними вимогами безпеки. Всі вимоги до функцій безпеки можна поділити на два типи: управління доступом до інформації і управління потоками інформації. На цьому етапі потрібно правильно визначити для об'єкта компоненти функцій безпеки. Компонент функції безпеки описує певний набір вимог безпеки - найменший вибраний набір вимог безпеки для введення у профіль захисту. Між компонентами можуть існувати залежності.

Структура вимог гарантії досягнутої захищеності аналогічна структурі функціональних вимог і охоплює класи, групи, компоненти й елементи гарантій, а також рівні гарантії. Класи і групи гарантування відображають такі питання, як розроблення, управління конфігурація, робоча документація, підтримка етапів життєвого циклу, тестування, оцінка уразливості. Вимоги гарантування захисту виражаються оцінкою функцій служби інформаційної безпеки об'єкта. Таку оцінку роблять на рівні окремого механізму захисту, що

дає змогу визначити здатність відповідної функції безпеки протистояти ідентифікованим загрозам. Залежно від відомого потенціалу нападу сила функції захисту визначається, наприклад, категоріями "базова", "середня", "висока". Потенціал нападу визначають за допомогою експертизи можливостей, ресурсів і мотивів нападаючого. Пропонується використовувати зведення рівнів гарантованості захисту. Рівні гарантії мають ієрархічну структуру, де кожен наступний рівень надає гарантії і включає всі вимоги попереднього.

Формування переліку вимог до системи інформаційної безпеки, ескізний проект, план захисту - це вимоги безпеки інформаційного середовища об'єкта замовника, які можуть містити посилання на відповідний профіль захисту, а також чітко сформульовані вимоги [36].

У загальному вигляді технічної документації передбачає:

- уточнення функцій захисту;
- вибір архітектурних принципів побудови системи інформаційної безпеки;
- розроблення логічної структури системи інформаційної безпеки (чіткий опис інтерфейсів);
- уточнення вимог функцій забезпечення гарантоздатності системи інформаційної безпеки;
- розроблення методики і програми випробувань на відповідність сформульованим вимогам.

На етапі оцінки досягнутої захищеності, оцінюють рівень гарантування безпеки інформаційного середовища об'єкта автоматизації на основі оцінки, за якої після виконання рекомендованих заходів можна довіряти інформаційному середовищу об'єкта. Базові положення цієї методики припускають, що ступінь гарантування залежить від ефективності зусиль, докладених до оцінювання безпеки.

Збільшення цих зусиль означає [38]:

- значну кількість елементів інформаційного середовища об'єкта, що беруть участь у процесі оцінювання;

- розширення типів проектів і описів деталей виконання під час проектуванні системи гарантування безпеки;
- суворість проведення робіт, яка полягає у застосуванні більшої кількості інструментів пошуку і методів виявлення менш очевидних слабких місць або зменшення вірогідності їх наявності.

## 2.2 Використання моделей системи інформаційної безпеки підприємства для проведення досліджень

Ключовою моделлю, що використовується у сфері управління інформаційною безпекою (УІБ), є процесна модель, що знайшла відображення в усіх стандартних підходах до УІБ і являє собою основу ISO/IEC 27005. Це не математична модель, але вона дає перелік і послідовність таких необхідних для управління ризиками ІБ процесів, як планування, реалізація, перевірка, дія.

На етапі планування визначаються політика та методологія управління ризиками, а також здійснюється оцінювання ризиків, яке передбачає інвентаризацію активів, складання профілів загроз і вразливостей, оцінювання ефективності контрзаходів і потенційного збитку, визначення допустимого рівня залишкових ризиків.

На етапі реалізації виконуються роботи з обробки інформації про ризики, оцінювання критичності ризиків, планування та впровадження заходів щодо кожного з ризиків. Відповідно до результатів першого етапу керівництво організації приймає одне з чотирьох рішень стосовно кожного з ідентифікованих ризиків: проігнорувати, уникнути, передати зовнішній стороні або мінімізувати. Після цього розробляється і впроваджується план протидій по кожному з ризиків.

На етапі перевірки здійснюється аналіз функціонування відповідних механізмів мінімізації ризиків, відстежуються зміни факторів ризику (активів, загроз, вразливостей), проводяться аудити, виконуються інші процедури контролю.

На етапі дії за результатами безперервного моніторингу та проведених перевірок виконуються певні коригувальні дії, які можуть включати в себе, зокрема, переоцінювання ризиків, коригування політики і методології управління ризиками, а також план обробки ризиків [39, с.358].

Класичні реалізації таких методик, як CRAMM, FRAP, OCTAVE, Risk Watch, базуються на використанні процесної моделі з опитувальною схемою, пропонуючи вже готові стандарти, з яких необхідно вибрати ті, що притаманні системі користувача, та оцінити їх за запропонованою системою критеріїв оцінювання [40]:

- класифікація та певний перелік ресурсів: визначений перелік якісних і чисельних (у тому числі складених) критеріїв оцінювання ресурсів; класифікація та певний набір вразливостей: визначений перелік якісних і чисельних (у тому числі складених) критеріїв оцінювання вразливостей;
- класифікація та певний набір ризиків: визначений перелік якісних і чисельних (у тому числі складених) критеріїв оцінювання ризиків;
- класифікація та певний набір засобів і заходівбезпеки;
- визначений перелік якісних і чисельних (у тому числі складених) критеріїв оцінювання вартості та надійності засобів і заходів безпеки.

Після відповідей на запитання за запропонованою схемою класичні методології УРІБ обчислюють показники та виводять за пріоритетністю перелік вразливостей, ризиків, набір протидій та дані щодо ефективності їх впровадження [41, с. 96-97].

Головними цікавими відмінностями класичних методологій УІБ є саме набір критеріїв оцінювання ресурсів, вразливостей, ризиків та формалізація обчислення кількісних показників. Наприклад, за методологією CRAMM цінність даних і програмного забезпечення визначається в таких ситуаціях:

- недоступність ресурсу протягом певного періоду часу;
- руйнування ресурсу − втрата інформації, отриманої з часу останнього резервного копіювання, або повне руйнування бази даних;

- порушення конфіденційності у випадках отримання несанкціонованого доступу штатними співробітниками або сторонніми особами;
- модифікація, яка розглядається для випадків дрібних ненавмисних помилок персоналу (помилки введення), програмних помилок, навмисних помилок;
- помилки, пов'язані з передачею інформації: відмова від доставки, неповна доставка інформації, доставка за невірною адресою.

Для оцінювання можливого збитку CRAMM рекомендує використовувати такі параметри [42]:

- збитки для репутації організації; порушення чинного законодавства;
- збитки для здоров'я персоналу;
- збитки, пов'язані з розголошуванням персональних даних окремих осіб;
- фінансові втрати від розголошування інформації;
- фінансові втрати, пов'язані з відновленням ресурсів;
- втрати, пов'язані з неможливістю виконання певних зобов'язань;
- дезорганізація діяльності.

Програмне забезпечення CRAMM для кожної групи ресурсів і кожного із закладених у цій методології 36 типів загроз генерує список питань, що допускають однозначну відповідь. Рівень загроз оцінюється, залежно від відповідей, як дуже високий, високий, середній, низький і дуже низький, рівень вразливості − як високий, середній і низький. На основі цієї інформації розраховуються рівні ризику в дискретній шкалі з градаціями від 1 до 7.

Методика Facilitated Risk Analysis Process (FRAP) передбачає, що на початковому етапі в системі відсутні засоби і механізми захисту. Таким чином, оцінюється рівень ризику для незахищеної інформаційної системи, що надалі дозволяє показати ефект від впровадження системи захисту інформації (СЗІ).

Оцінювання здійснюється для ймовірності виникнення загрози і збитку від неї.

Оцінка визначається відповідно до правила [43], що задається матрицею ризику (табл. 2.1), де А – роботи з виправлення мають бути виправленні

негайно; B – роботи з виправленням слід виконувати найближчим часом; C – необхідно моніторити ситуацію; D – дії з виправлення на даний час не потрібні.

Таблиця 2.1 Матриця ризику за методом FRAP

| P \ I | Високий | Середній | Низький |
|---|---|---|---|
| Висока | A | B | C |
| Середня | B | B | C |
| Низька | B | C | D |

Методика OCTAVE передбачає три фази аналізу ризику [44]:

- розробка профілю загроз, пов'язаних з акти загрози від людини-порушника, яка діє через мережу передавання даних;
- ідентифікація інфраструктурних вразливостей;
- розробка стратегії та планів безпеки.

Профіль загрози визначає ресурс, тип доступу до ресурсу, джерело загрози або суб’єкт загрози, тип порушення, результат і посилання на опис загрози в загальнодоступних каталогах. Відповідно до типу джерела, загрози в OCTAVE поділяються на такі класи:

- загрози від людини-порушника, яка використовує фізичний доступ;
- загрози, пов'язані зі збоями в роботі системи;
- результатом реалізації загрози може бути розкриття, зміна, втрата або руйнування інформаційного ресурсу, відсутність доступу до ресурсу або відмова в обслуговуванні.

Методика OCTAVE пропонує скласти «профіль загроз» та «дерево варіантів». При створенні профілю загроз рекомендується уникати великої кількості технічних деталей − це завдання другої фази дослідження. А на першій потрібно стандартизованим чином описати поєднання загрози та ресурсу. Наприклад, на підприємстві є інформаційний ресурс − база даних (БД) відділу кадрів. Профіль, що відповідає загрозі класу, пов’язаного з крадіжками

інформації співробітником підприємства, наведено в табл. 2.2, а дерево варіантів – на рис. 2.4 [45, с. 352].

Таблиця 2.2 Профіль загрози за методом OCTAVE

| | |
|---|---|
| Ресурс | БД відділу кадрів |
| Тип доступу | Через мережу передачі даних |
| Джерело загрози | Внутрішня |
| Тип порушення | Навмисне |
| Вразливість | Помилка при делегуванні прав доступу; Неблагонадійність співробітників. |
| Наслідки | Розкриття даних |
| Посилання на каталог вразливостей | US-CERT |

Вразливості виявляються сканерами безпеки рівня операційної системи, мережевими сканерами безпеки, спеціалізованими сканерами (для конкретних web-серверів, систем керування БД тощо) за допомогою списків вразливостей, тестових скриптів.

Для кожного компонента визначаються:

- список вразливостей, які потрібно усунути негайно;
- список вразливостей, які потрібно усунути найближчим часом;
- список вразливостей, які не вимагають негайних дій.

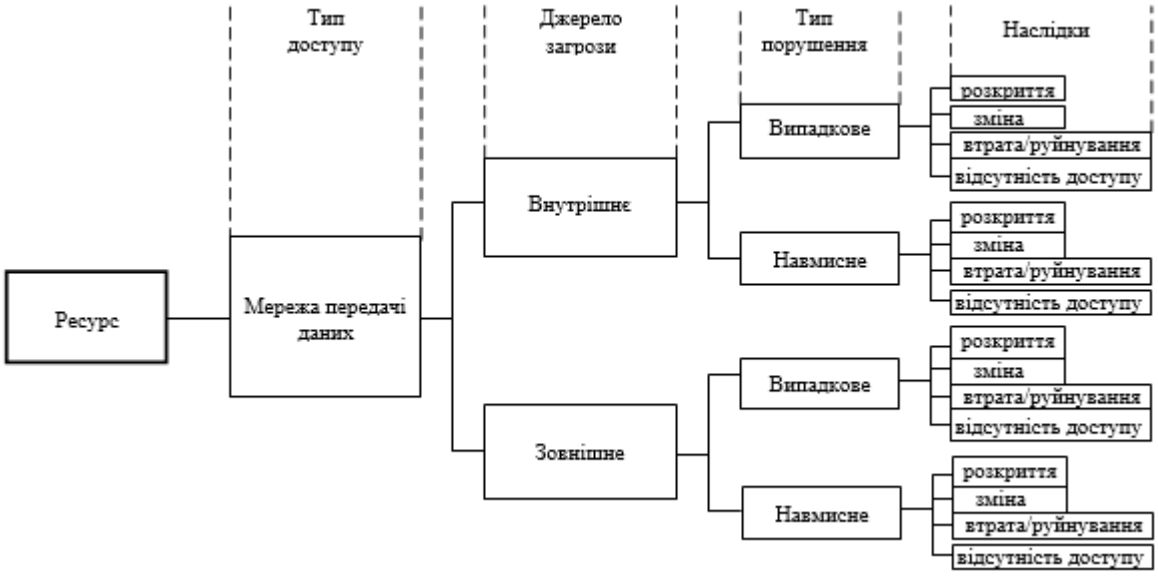


Рис. 2.4 Дерево варіантів, що використовується при описі профілю загрози

За результатами цієї фази формується звіт із зазначенням списку виявлених вразливостей, впливу, який вони можуть здійснити на виділені раніше ресурси (активи), а також заходів щодо усунення вразливостей [46].

Розробка стратегії та планів безпеки − третя фаза дослідження системи. Вона починається з оцінювання ризику, яке проводиться на базі звітів за двома попередніми фазами. В OCTAVE дається лише оцінка очікуваного збитку, без визначення ймовірності реалізації загрози. Шкала оцінювання ризику: високий, середній, низький. Обчислюються фінансові збитки, збитки стосовно репутації компанії, життя та здоров'я клієнтів і співробітників, збитки, що їх може викликати судове переслідування в результаті того або іншого інциденту. Описуються значення, відповідні кожній градації шкали.

Як приклад в [47] запропонована адаптована методика управління ризиками при забезпеченні живучості та неперервності функціонування СЗІ в інформаційно-телекомунікаційних системах на основі методики OCTAVE. Адаптована методика управління ризиками при забезпеченні живучості та неперервності функціонування СЗІ в ІТС враховує позитивні якості основних методик і мінімізує їх недоліки.

У методиці RiskWatch формула обчислення ризику зазнала певних змін у зв'язку з тим, що RiskWatch використовує визначені Американським інститутом стандартів (NIST) оцінки, які називаються LAFE і SAFE. Local Annual Frequency Estimate (LAFE) показує, скільки разів на рік в середньому певна загроза буде реалізована в даному місці (наприклад, в межах міста). Standard Annual Frequency Estimate (SAFE) визначає, скільки разів на рік в середньому певна загроза буде реалізована в цій "частині світу". Вводиться також поправочний коефіцієнт, який дозволяє врахувати, що в результаті реалізації загрози ресурс, що необхідно захистити може бути знищений не повністю, а лише частково [48, с. 747].

Отже, оцінка ризику за методикою RiskWatch розраховується як оцінка очікуваних річних втрат для одного конкретного ресурсу від реалізації однієї загрози ALE:

$$ALE = AV \times EF \times F, \quad (2.1)$$

де AV − вартість даного активу (даних, програм, апаратури); EF − коефіцієнт дії, що показує, яка частина (у відсотках) від вартості активу піддається ризику; F − частота виникнення небажаної події;

Розглянуті вище моделі УІБ базуються на процесній моделі і пропонують якісні й кількісні показники оцінювання ризиків. У більшості випадків, якщо показник має якісну характеристику, то цю якість прив’язують до чисельної шкали й перетворюють показник у кількісний. Розглянемо декілька підходів до формалізації обчислення ризиків.

Класична формула [49, с.154] − оцінювання ризику (R) виконується за двома факторами: ймовірність реалізації загрози ($P_{реалізації}$) і розмір збитку (D):

$$R = P_{реалізації} \times D. \quad (2.2)$$

Подальша деталізація ймовірності реалізації загрози може бути визначена формулою, яка враховує ймовірність виникнення загрози та ймовірність появи вразливості:

$$P_{реалізації} = P_{загрози} \times P_{вразливості.} \quad (2.3)$$

Більшість інших методів обчислення рівня ризиків інформаційної безпеки являють собою різні модифікації наведених вище формул. Наприклад, рівень ризику по всій системі – це сума ризиків по всіх активах та кожній загрозі; ефект від вжитих контрзаходів обчислюється як різниця між сумою запланованих витрат на контрзаходи та сумарною оцінкою збитків при визначеному рівні ризику по всій системі.

## 2.3 Дослідження функціонування системи інформаційної безпеки підприємства в Україні (на прикладі)

Систему управління інформаційною безпекою розуміють як частину загальної системи управління, базою якої є аналіз ризиків, а призначенням – створення, реалізація, контроль та вдосконалення заходів у сфері інформаційної безпеки [50].

Задля реалізації ефективної політики забезпечення інформаційної безпеки необхідне досягнення таких основних цілей:

- захищеність інформації (конфіденційність та унеможливлення доступу сторонніх осіб);
- цілісність (захист від спотворення інформації у будь-якому її вигляді);
- доступність (забезпечення доступу до інформації зацікавлених осіб).

Основні проблеми підприємства ТОВ «Феракс» у сфері інформаційної безпеки зазначені на рис. 2.5.

Проблематика інформаційної безпеки підприємства ТОВ «Феракс» викликана дією загроз, які за природою виникнення поділяються на внутрішні та зовнішні (рис. 2.6).

| Основні проблеми підприємства ТОВ «Феракс» | |
|---|---|
| Підтримка інформаційної безпеки | Зовнішні та внутрішні канали витоку інформації |
| Грошові втрати від інформаційних інцидентів | Атаки на конфіденційну інформацію |
| Недосконалість програмного забезпечення підприємств | Персональні мобільні пристрої, що мають доступ до акаунтів з конфіденційною та персональною інформацією |

Рис. 2.5 Основні проблеми підприємства ТОВ «Феракс»


Рис. 2.6 Джерела внутрішніх та зовнішніх загроз інформаційній безпеці підприємства ТОВ «Феракс»

Враховуючи зазначене вище, представимо систему інформаційної безпеки як процес управління ризиками та небезпеками і зобразимо у вигляді моделі управління ризиками на ТОВ «Феракс» (рис. 2.7).

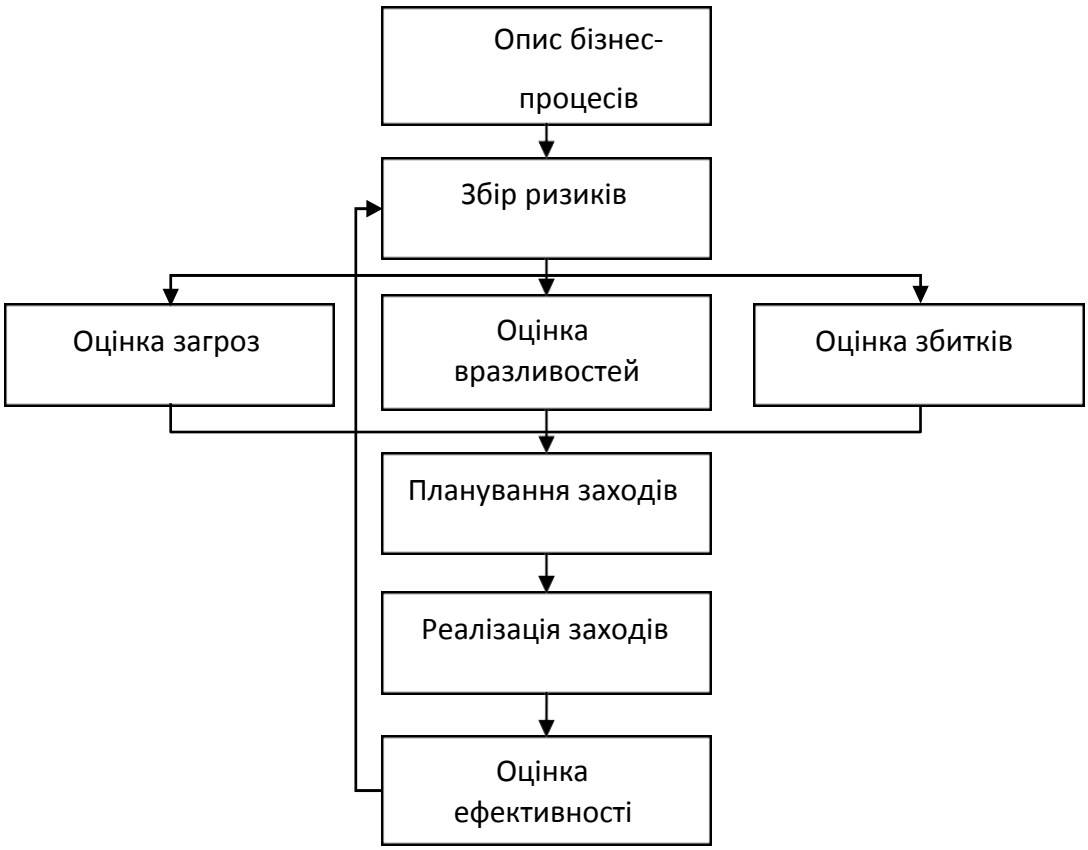


Рис. 2.7 Модель управління ризиками для системи інформаційної безпеки на ТОВ «Феракс»

Важливим фактором у процесі боротьби з проблемами та ризиками є визначення організаційної структури системи управління інформаційною безпекою підприємства. Вона включає систему правових, технічних та організаційних засобів, що забезпечують нормалізацію діяльності у сфері безпеки.

Організаційна структура системи управління базується на основі розмежування функціональних повноважень між підрозділами підприємства ТОВ «Феракс». На підприємстві ТОВ «Феракс» основними суб'єктами організаційної структури управління інформаційною безпекою є:

- генеральний директор;
- начальник департаменту безпеки;
- директори територіальних підрозділів;
- відділ інформаційної безпеки;

- аутсорсингові компанії;
- співробітники тощо.

Незважаючи на різноманіття суб’єктів, основним є відділ інформаційної безпеки – підрозділ, що приймає безпосередню участь в організації і відповідає за забезпечення інформаційної безпеки в рамках своїх повноважень. Співробітники цього відділу згідно функціональних обов’язків виконують наступні роботи у сфері інформаційної безпеки:

- розробка проектів і реалізація стратегій забезпечення інформаційної безпеки;
- визначення вимог до бізнес-проектів, засобів їх реалізації та автоматизації;
- розробка внутрішньої нормативної бази;
- координація діяльності підрозділів з урахуванням певних пріоритетних напрямів розвитку інформаційної безпеки;
- формулювання і обґрунтування пропозицій до проекту бюджету або фінансового плану підприємства;
- робота по виявленню та оцінці загроз, аналіз ризиків і підтримка їх в актуальному стані;
- розрахунок результатів оцінки ризиків для керівництва, а також пропозиції шляхів і засобів обробки ризиків з урахуванням їх ефективності;
- розробка пропозицій по удосконаленню механізмів забезпечення інформаційної безпеки та контроль реалізації вимог до інформаційної безпеки;
- розслідування за фактами інцидентів;
- контроль виконання вимог щодо процесу управління доступом до інформаційних систем і ресурсів користувачів, штатного персоналу, впровадження і підтримки систем.

Алгоритм удосконалення системи управління інформаційною безпекою на підприємстві ТОВ «Феракс», характеризується низкою ознак, які зазначені на рис. 2.8.

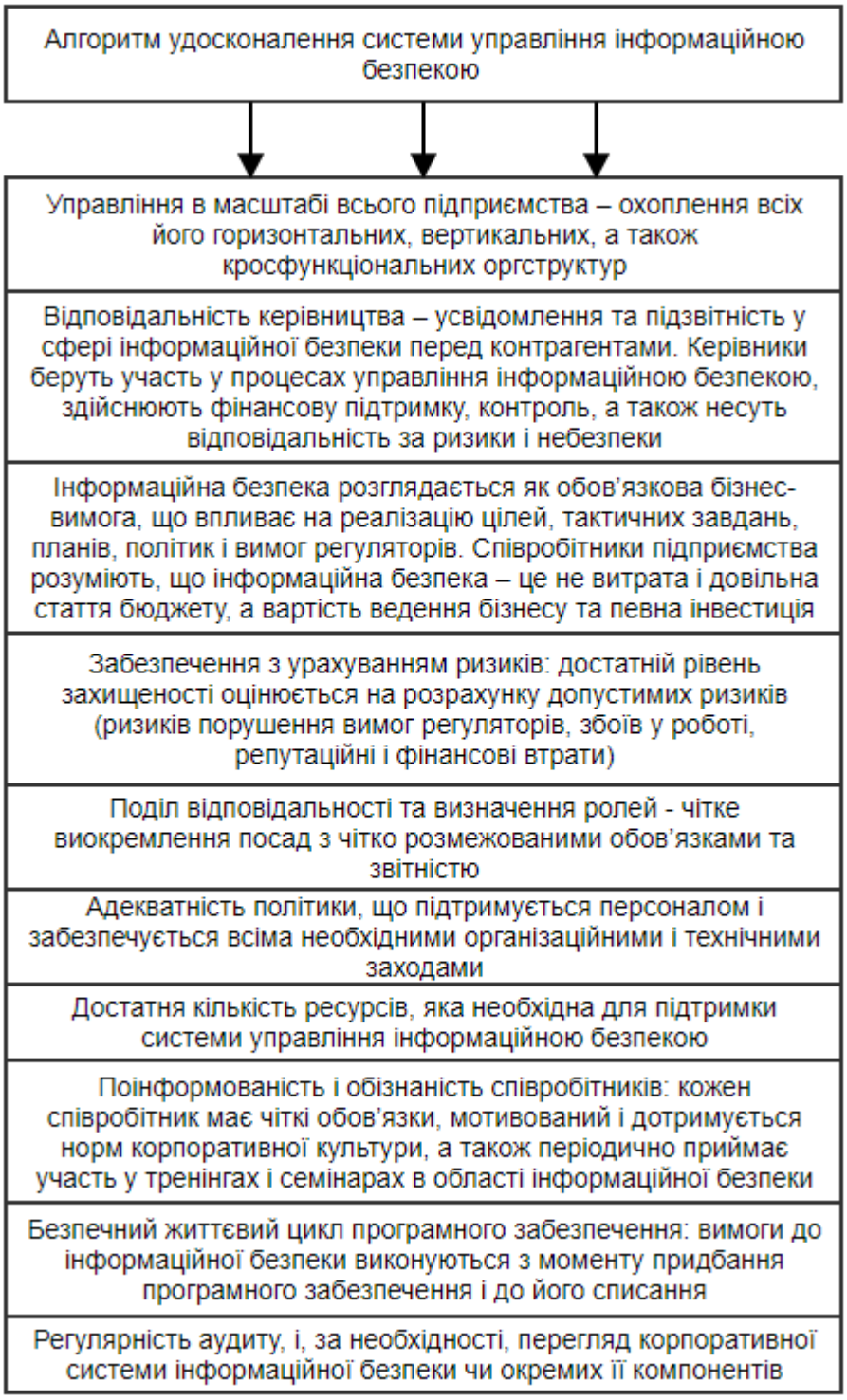


Рис. 2.8 Алгоритм удосконалення системи управління інформаційною безпекою на підприємстві ТОВ «Феракс»

Формуючи і удосконалюючи організаційну структуру системи управління інформаційною безпекою, важливим є дотримання певних правил і принципів [51]:

- законність – функціонування у відповідності до законодавства, стандартів, положень, керівних документів, а також локальних нормативних документів;
- централізація – функціонування за єдиними функціональними, організаційними та методичними принципами;
- безперервність – безперервний процес, що складається з етапів планування, впровадження, оцінки ефективності, покращення контролю, приведення можливих ризиків до прийнятного рівня.

Сутність викладеного вище дає підстави стверджувати, що однією з ключових частин формування системи захищеності підприємства ТОВ «Феракс» є інформаційна безпека. Для збереження цілісності підприємства, розвитку, а також конкурентоспроможності на ринку, необхідне створення ефективної системи управління інформаційною безпекою. Без належного захисту інформаційного середовища підприємство ТОВ «Феракс» унеможливлюється забезпечення економічної безпеки.

**Висновки до другого розділу**

У даному розділі були розглянуті методичні підходи до побудови системи інформаційної безпеки підприємства, проаналізовані ризики та вразливості підприємства в інформаційній сфері. Дослідили функціонування системи інформаційної безпеки на прикладі підприємства ТОВ «Феракс».

В наступному розділі роботи потрібно проаналізувати функціонування інформаційної безпеки підприємства, вже на вивчених даних, та розглянути методи вдосконалення організації інформаційної безпеки підприємства ТОВ «Феракс».

# Розділ 3
# РЕКОМЕНДАЦІЇ ПО ВДОСКОНАЛЕННЮ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

## 3.1 Аналіз результатів досліджень функціонування інформаційної безпеки підприємства

Під інформаційною безпекою (ІБ) промислового підприємства розуміються всі елементи системи управління підприємством, пов’язані з визначенням, досягненням конфіденційності, цілісності, доступності, неспростовності, підзвітності, автентичності та достовірності інформації або засобів її обробки [52].

Для забезпечення ефективного функціонування всіх вище визначених елементів необхідно використання комплексного підходу. Це означає, насамперед, що в межах системи управління не може бути створено окремої підсистеми, яка б відповідала за інформаційну безпеку, при повному збереженні існуючих на промисловому підприємстві бізнес-процесів.

Зловживання інформацією, що циркулює в ІС або передається по каналах зв'язку, удосконалювалися не менш інтенсивно, ніж заходи захисту від них. В даний час для забезпечення захисту інформації потрібно не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів, морально-етичних заходів протидії і т.д.). Комплексний характер захисту виникає з комплексних дій зловмисників, які намагаються будь-якими засобами добути важливу для них інформацію. Сьогодні народжується нова сучасна технологія - технологія захисту інформації в комп'ютерних інформаційних системах і мережах передачі даних.

Для ефективного виконання такого завдання необхідна система відповідного методичного забезпечення. Основними елементами такої системи

є принципи побудови системи ІБ, цільові характеристики системи, її завдання, основні загрози та заходи щодо нейтралізації загроз.

Достатня стійкість інформаційної безпеки виражається в тому, що потенційні зловмисники повинні зустрічати перешкоди у вигляді досить складних обчислювальних завдань. Наприклад, необхідно, щоб злом паролів доступу вимагав від хакерів неадекватно великих проміжків часу і/або обчислювальних потужностей.

Мінімізація дублювання передбачає мінімізацію ідентичних процедур. Цей принцип інформаційної безпеки полягає в тому, що в системі ІБ не повинно бути загальних для декількох користувачів процедур, таких як введення пароля. У цьому випадку масштаб можливої хакерської атаки буде менше.

Побудована за наведеними принципами система ІБ має бути налаштована на досягнення визначених цілей, специфіка яких буде великою мірою визначати як структуру системи так і основні параметри її функціонування. Для промислового підприємства основними цілями досягнення високого рівня інформаційної безпеки є забезпечення конфіденційності, цілісності, доступності, достовірності та неспростовності інформації.

Розглянемо кожну цільову характеристику інформації докладно:

Конфіденційність - це стан доступності інформації тільки авторизованим користувачам, процесів і пристроїв [52]. Необхідно підкреслити, що конфіденційність є однією з основних цільових характеристик інформації, а її забезпечення – найголовнішою функцією системи інформаційної безпеки. Категорія конфіденційності є особливо важливою для промислових підприємств на етапі проведення НДДКР та впровадження інновацій. Основними методами забезпечення конфіденційності інформації є (рис. 3.1): закриття, шифрування, приховування та подрібнення.

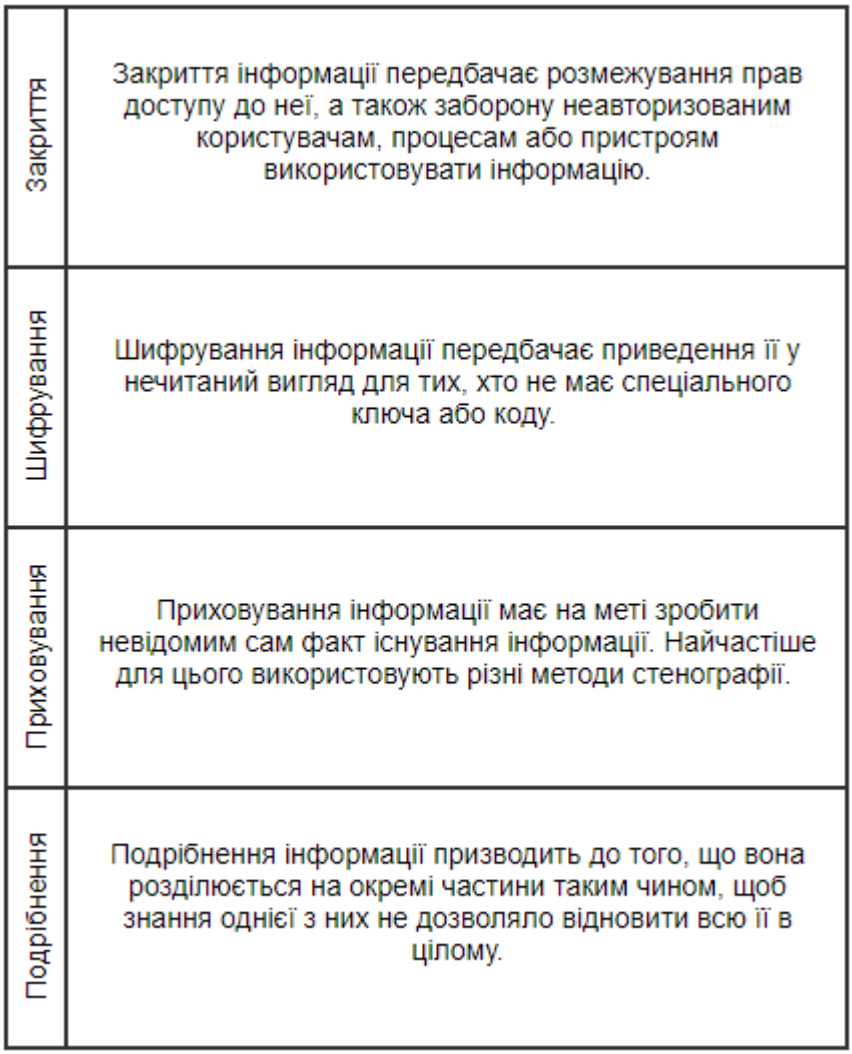


Рис. 3.1 Основні методи забезпечення конфіденційності інформації

Цілісність - це відсутність неправомочних спотворень, доповнень або знищення інформації[53]. Гарантія цілісності особливо важлива в тих випадках, коли інформація представляє велику цінність і не повинна бути втрачена, а також коли дані можуть бути навмисно змінені з метою дезінформації одержувача. Як правило, від стирання інформацію захищають методами, що забезпечують конфіденційність, і резервним копіюванням, а відсутність спотворень перевіряють з допомогою хешування.

Доступність - це забезпечення своєчасного і надійного доступу до інформації і інформаційних сервісів[54]. Типовими випадками порушення доступності є збій в роботі програмних/апаратних засобів і розподілена атака типу «відмова в обслуговуванні» (DDoS). Від збоїв інформаційну систему

захищають усуненням причин збоїв, а від DDoS-атак - відсіканням паразитного трафіку.

Справжність або автентичність - можливість однозначно ідентифікувати автора/джерело інформації[55]. Автентичність електронних даних часто засвідчується таким засобом, як електронно-цифровий підпис.

Неспростовність - неможливість зречення від авторства інформації, а також факту її відправки або отримання[55]. Неспростовність можна гарантувати електронно-цифровим підписом та іншими криптографічними засобами і протоколами. Неспростовність актуальна, наприклад, у системах електронних торгів, де вона забезпечує відповідальність друг перед іншому продавців і покупців.

Також на підприємстві ТОВ «Феракс» система інформаційної безпеки може бути спрямована на забезпечення специфічних властивостей інформації, наприклад підзвітність, адекватність та інші.

Для досягнення названих цілей система ІБ повинна бути спроможною виконувати наступні завдання:

- забезпечення захищеного зберігання інформації на різних носіях;
- захист даних, що передаються по каналах зв'язку;
- розмежування доступу до різних видів документів;
- створення резервних копій, післяаварійне відновлення інформаційних систем.

Забезпечення інформаційної безпеки підприємства ТОВ «Феракс» можливо тільки при системному і комплексному підході до захисту. В системі ІБ повинні враховуватися всі актуальні комп'ютерні загрози та вразливості (рис 3.2).

Загрози інформаційній безпеці - це можливі дії або події, які можуть вести до порушень ІБ. Вони також є кінцевими цілями (або результатами) діяльності її порушників. Види загроз інформаційної безпеки дуже різноманітні і мають безліч класифікацій [56].


Рис. 3.2 Загрози інформаційній безпеці підприємства ТОВ «Феракс»

Повноцінна інформаційна безпека підприємства передбачає безперервний контроль в реальному часі всіх важливих подій і станів, що впливають на безпеку даних. Захист має здійснюватися цілодобово і цілорічно і охоплювати весь життєвий цикл інформації - від її надходження або створення до знищення або втрати актуальності.

На рівні підприємства за інформаційну безпеку відповідають відділи інформаційних технологій, економічної безпеки, кадрів та інші служби.

Необхідно також відзначити, що рівень загроз і, відповідно рівень інформаційної безпеки підприємства, постійно змінюються під дією різних факторів. Найбільш впливовими з них є наступні:

- розширення співпраці підприємства з партнерами;
- автоматизація бізнес-процесів на підприємстві;
- розширення кооперації виконавців при побудові і розвитку інформаційної інфра-структури підприємства;
- зростання обсягів інформації підприємства, яка передається по відкритих каналах зв'язку;
- ріст комп'ютерних злочинів.

Для досягнення задовільного рівня інформаційної безпеки на підприємстві ТОВ «Феракс» необхідно застосування комплексу організаційних і технічних заходів, спрямованих на захист корпоративних даних. Організаційні заходи включають документовані процедури і правила роботи з різними видами інформації, ІТ-сервісами, засобами захисту і т. д. Технічні заходи полягають у використанні апаратних і програмних засобів контролю доступу, моніторингу витоків, антивірусного захисту, міжмережевого екранування, захисту від електромагнітних випромінювань і ін.

При виборі програмно-технічних рішень із забезпечення ІБ підприємства, перевага віддається рішень, що забезпечує дотримання основних принципів ІБ, а також відповідаючих наступним критеріям:

- підтримка міжнародних, національних, промислових та Інтернет стандартів (перевага віддається міжнародним стандартам);
- підтримка найбільшою мірою інтеграції з корпоративними програмно-апаратними платформами і використовуваними СЗІ;
- уніфікація розробників і постачальників використовуються продуктів;
- уніфікація засобів і інтерфейсів управління підсистемами ІБ.

Таким чином, за результатами проведених досліджень, можна сформувати методичний підхід до побудови системи інформаційної безпеки підприємства ТОВ «Феракс» (рис. 3.3).

Із наведеного рис. 3.3 видно, що основні елементи методичного підходу до формування системи управління ІБ розділені на чотири рівні, кожному з яких відповідає визначений рівень управління підприємством.

Так, принципи формування системи ІБ, що віднесені до теоретико-методологічного рівня запропонованого підходу, є тим елементом системи, за формування якого відповідає вище керівництво підприємства.

Також на цьому рівні мають бути сформовані основні вимоги до необхідного підприємству рівня ІБ. Далі ІТ служби відповідають за виконання заходів, віднесених до методичного та інструментального рівня, тобто вони

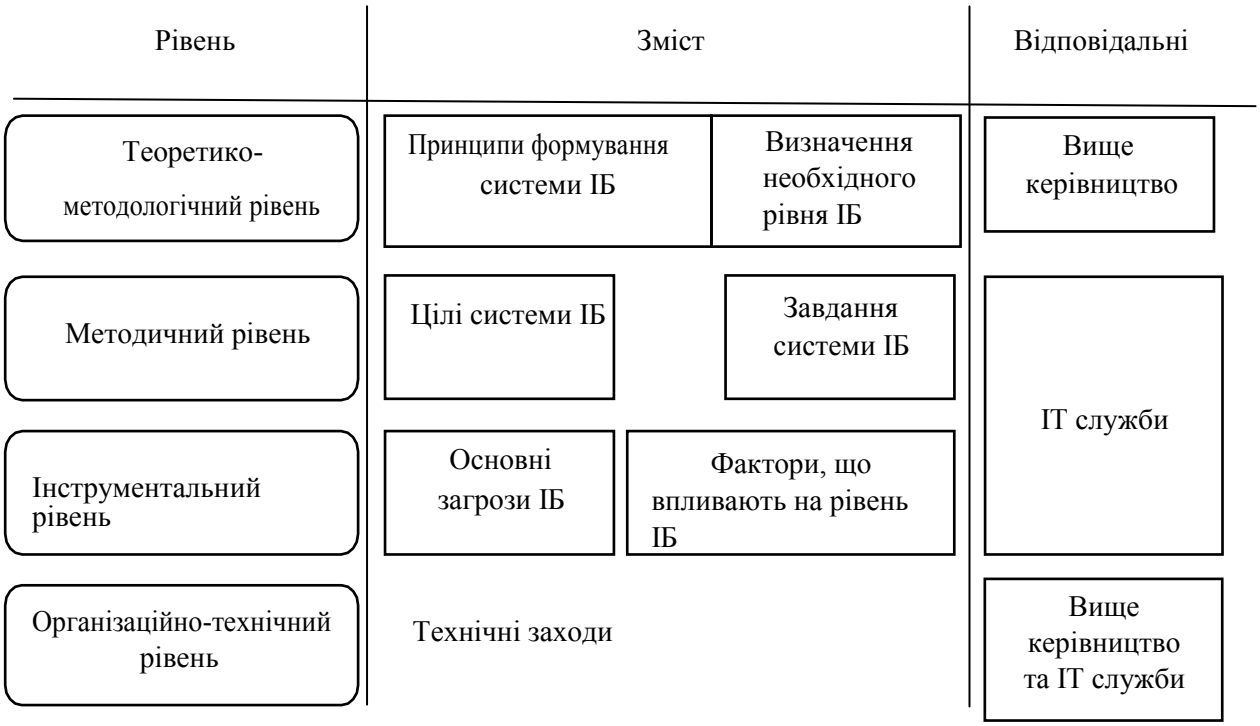


Рис. 3.3 Методичний підхід до формування системи ІБ підприємства ТОВ «Феракс»

повинні сформулювати основні цілі та завдання системи ІБ, а також визначити основні загрози ІБ та фактори, що впливають на її рівень. Після цього, ІТ служби мають розробити план технічних ат організаційних заходів, спрямованих на досягнення визначеного рівня ІБ. Після цього план погоджується вищим керівництвом підприємства і розпочинаються роботи по його практичному впровадженню. Особливо слід відзначити необхідність обов'язкової участі вищого керівництва підприємства у реалізації заходів організаційно-технічного рівня.

На цьому етапі керівництво підприємства повинно зрозуміти, що просте впровадження «додаткових заходів» без зміни всієї системи управління не забезпечить необхідного рівня ІБ.

Важливою умовою ефективного функціонування системи інформаційної безпеки є її повна інтеграція в оперативну діяльність компанії. Її впровадження неодмінно буде вимагати коригування, а іноді і докорінної зміни більшості бізнес процесів. Можлива поява принципово нових бізнес-процесів, пов'язаних

із забезпеченням функціонування системи ІБ. Це вимагає внесення змін в описі бізнес-процесів, регламентацію всіх нововведень та визначення нових меж відповідальності виконавців. Також необхідно ввести в практику постійні навчання та тренування з питань ІБ.

## 3.2 Напрямки та методи вдосконалення організації інформаційної безпеки підприємства

Сучасний стан інформаційної безпеки відрізняється її нестабільністю. Це означає, що підприємство повинно застосовувати щоденні методи захисту, які відповідали б його специфіці.

Найбільш важливими факторами становлення системи інформаційної безпеки підприємств є [57]:

- відсутність єдиної державної політики в галузі забезпечення інформаційної безпеки підприємств;
- недосконаліть нормативної правової бази, що регулює відносини в галузі забезпечення інформаційної безпеки підприємств, а також недостатня правозастосовна практика;
- недостатній контроль за розвитком інформаційного ринку з боку державних структур і суспільства;
- низький рівень захищеності інтересів фізичних і юридичних осіб в інформаційній сфері.

Узагальнюючи сучасний стан інформаційної безпеки підприємств, можна визначити основні фактори і перспективи її розвитку [58]:

- удосконалення законодавства у сфері інформаційної безпеки сприятиме її розвитку, а також дотриманню всіх встановлених норм і правил;
- на підприємствах слід створювати і впроваджувати системи інформаційної безпеки, що сприятиме комплексному захисту інформації в країні в цілому;

- удосконалення методів захисту інформації – шлях до захисту від найбільш небезпечних загроз, які становлять небезпеку підприємству;
- для захисту комерційної інформації організацій, повинні залучатися державні кошти, так само, як виділяються кошти на захист державної таємниці. Часом витік комерційної інформації підприємства може привести до серйозних негативних наслідків, а також погіршення іміджу країни та інвестиційної привабливості;
- підприємствам слід створювати служби інформаційної безпеки, або покладати ці функції на співробітників, компетентних у даній сфері;
- підприємствам слід приділяти особливу увагу як при працевлаштуванні співробітників, так і при їх звільненні, дотримуючись усіх норм безпеки та попереджаючи витік інформації. Трудовий договір, що підписується співробітником, повинен неодмінно містити пункт про нерозголошення комерційної таємниці;
- суб’єктам господарювання слід користуватися виключно ліцензійними засобами захисту інформації і послугами перевірених фірм, що мають репутацію і пройшли ліцензування;
- підприємствам слід звести до мінімуму використання співробітниками портативних носіїв інформації на підприємстві, а також мати доступ до корпоративних досліджень.

Варто відмітити той факт, що збереження бізнесу, його розвиток і підтримка конкурентоспроможності підприємства потребують створення ефективної системи управління інформаційною безпекою, комплекс організаційних, технічних, програмних і криптографічних, засобів і заходів щодо захисту інформації в процесі традиційного документообігу при роботі виконавців із конфіденційними документами і відомостями, при обробці інформації в автоматизованих системах різного рівня та призначення, при передачі каналами зв'язку, при веденні конфіденційних переговорів.

Слід зазначити, що інформаційна безпека підприємства забезпечується власними силами суб'єктів господарювання, їх службою безпеки або

уповноваженою особою завданнями яких є забезпечення безпеки підприємства, виробництва, продукції та захист комерційної, промислової, фінансової, ділової та іншої інформації незалежно від її призначення і форми при всій різноманітності можливих каналів її розповсюдження та різноманітних дій конкурентів. Тому підбір кадрів повинен виконуватись на належному рівні, оскільки недостатні професійні знання, некомпетентність може призвести до серйозних наслідків, що можуть безпосередньо вплинути на фінансову діяльність і стійкість підприємства на ринку.

У галузі захисту інформації, завдання забезпечення інформаційної безпеки повинні вирішуватися системно, тобто різні засоби захисту (апаратні, програмні, фізичні, організаційні і т. д.) повинні застосовуватися одночасно і під централізованим управлінням. При цьому компоненти системи повинні "знати" про існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і від внутрішніх загроз.

Усе більшою популярністю для захисту інформації користуються криптографічні методи. Інтерес комерційних структур до них значно зріс у зв'язку зі зменшенням вартості перехоплення інформації, що передається електронною поштою чи функціонує в системі електронних платежів. Найпоширенішими вважаються методи кодування та шифрування інформації. Поряд з ними використовуються методи розділення та стиснення даних.

У процесі захисту передачі усної інформації використовують методи аналогового скемблірування та дискретизації мови з подальшим шифруванням[59].

Один із перспективних напрямів захисту інформації сформулювали сучасні методи стенографії, що базуються на різних принципах, забезпечують таємницю самого факту існування секретної інформації в тому чи іншому середовищі за допомогою відповідних засобів: невидимих чорнил, мікрофотознімків, таємних каналів та засобів зв’язку з плаваючими частотами тощо.

Для вдосконалення організації системи інформаційної безпеки підприємства ТОВ «Феракс», потрібно провести необхідні заходи. Для формування системи інформаційної безпеки необхідно розробити і затвердити політику інформаційної безпеки. Слід зазначити, що розробляюча політика повинна узгоджуватися з існуючими законами і правилами, які стосуються організації, тобто ці закони і правила необхідно виявляти і брати до уваги при розробці політики. Чим надійніше система, тим суворіше і різноманітніше повинна бути політика безпеки. Залежно від сформульованої політики можна вибирати конкретні механізми, що забезпечують безпеку системи.

Щоб поліпшити організацію системи інформаційної безпеки підприємства ТОВ «Феракс», можна запропонувати наступні заходи[60]:

- організація робіт з навчання персоналу навичкам роботи з новими програмними продуктами за участю кваліфікованих фахівців;
- розробка необхідних заходів спрямованих на вдосконалення системи економічної, соціальної та інформаційної безпеки підприємства;
- провести інструктаж для того, щоб кожен співробітник усвідомив всю важливість і конфіденційність ввіреної йому інформації, тому що, як правило, причиною розголошення конфіденційної інформації є недостатнє знання працівниками правил захисту комерційних секретів і нерозуміння (або нерозуміння) необхідності їх ретельного дотримання;
- строгий контроль дотримання співробітниками правил роботи з конфіденційною інформацією;
- контроль за дотриманням правил зберігання робочої документації співробітників підприємства;
- планове проведення зборів, семінарів, обговорень з питань інформаційної безпеки підприємства;
- регулярна (планова) перевірка і обслуговування всіх інформаційних систем та інформаційної інфраструктури на працездатність.

Програмно-технічні засоби є одними з найважливіших компонентів в реалізації інформаційної захисту підприємства, тому для підвищення рівня

захисту інформації підприємства ТОВ «Феракс» необхідно ввести і застосувати наступні заходи[60]:

- Введення паролів користувачів;
- розмежування доступу до файлів, каталогів, дисків. Розмежування доступу до файлів і каталогів буде здійснюватися системним адміністратором, який дозволить доступ до відповідних дисків, папок і файлів для кожного користувача конкретно;
- регулярне сканування робочих станцій і оновлення баз антивірусної програми. Дозволить виявляти і нейтралізувати шкідливі програми, ліквідувати причини заражень. Необхідно виконати роботи з установки, настройки і забезпечення функціонування засобів і систем антивірусного захисту.
- установка на комп'ютер-сервер мережевого екрану, який блокує атаки з мережі Інтернет;
- застосування джерел безперебійного живлення. Найбільш надійним засобом запобігання втрат інформації при короткочасному відключенні електроенергії в даний час є установка джерел безперебійного живлення (UPS). Різні за своїми технічними і споживчими характеристиками, подібні пристрої можуть забезпечити харчування всієї локальної мережі або окремого комп'ютера протягом якогось проміжку часу, достатнього для відновлення подачі напруги або для збереження інформації на магнітні носії. В іншому випадку використовується наступна функція подібних пристроїв - комп'ютер отримує сигнал, що UPS перейшов на роботу від власних акумуляторів і час такої автономної роботи обмежена. Тоді комп'ютер виконує дії щодо коректного завершення всі програми, і відключається (команда SHUTDOWN). Більшість джерел безперебійного живлення одночасно виконує функції і стабілізатора напруги, є додатковим захистом від стрибків напруги в мережі. Багато сучасні мережеві пристрої - сервери, концентратори, мости і т.д. - оснащені власними дубльованими системами електроживлення;

- криптографічний захист інформації надається з метою забезпечення режиму конфіденційності та цілісності інформації при її передачі по каналах передачі даних;
- протоколювання і аудит є невід'ємною частиною забезпечення інформаційної безпеки. Ці поняття мають на увазі збір, накопичення і аналіз подій, що відбуваються в інформаційній системі в реальному часі.

Реалізація протоколювання і аудиту вирішує наступні завдання:

- забезпечення підзвітності користувачів і адміністраторів;
- забезпечення можливості реконструкції послідовності подій;
- виявлення спроб порушень інформаційної безпеки;
- надання інформації для виявлення і аналізу проблем.

При протоколюванні події рекомендується записувати, по крайній мірі, наступну інформацію[60]:

- дата і час події;
- унікальний ідентифікатор користувача - ініціатора дії;
- тип події;
- результат дії (успіх або невдача);
- джерело запиту (наприклад, ім'я терміналу);
- імена порушених об'єктів (наприклад, що відкриваються або файлів, що видаляються);
- опис змін, внесених до баз даних захисту (наприклад, нова мітка безпеки об'єкта).

Проблема інформаційної безпеки має дуже загострений характер, оскільки разом з величезною кількістю методів захисту інформації, збільшується та урізноманітнюється кількість потенційних загроз і дестабілізуючих факторів. Таким чином, керівництво підприємства ТОВ «Феракс» повинно прогнозувати можливі чинники зниження захищеності інформації та оснащувати себе системами захисту від них.

На сьогодні, питання безпеки інформації потрібно розглядати не просто як розробку приватних механізмів захисту, а як реалізацію системного підходу,

що включає комплекс взаємопов'язаних заходів, які повинні розширюватись та вдосконалюватись. Тому впровадження регламентів інформаційної безпеки при використанні телекомунікацій, дотримання персоналом внутрішніх нормативних актів, а також досягнення конфіденційності, цілісності та доступності інформації дозволять не тільки підвищити результативність системи інформаційної безпеки, але і будуть сприяти зміцненню зовнішніх позицій підприємства.

**Висновки до третього розділу**

У даному розділі було проаналізовано функціонування інформаційної безпеки на підприємстві, та були запропоновані напрямки та методи вдосконалення організації інформаційної безпеки підприємства на прикладі ТОВ «Феракс». Слід звернути увагу на те, що тільки при спільному взаємодії персоналу, програмно-апаратних засобів та засобів захисту інформації можлива ефективність даних заходів.

На закінчення можна підкреслити, що ніякі апаратні, програмні та будь-які інші рішення з вдосконаленням організації інформаційної безпеки підприємства на прикладі ТОВ «Феракс» не зможуть гарантувати абсолютну надійність і безпеку даних в комп'ютерних мережах.

# ВИСНОВКИ

Головною метою забезпечення інформаційної безпеки є запобігання загроз його безпеки, створення умов функціонування підприємства, захист законних інтересів підприємства від незаконних посягань, недопущення розкрадання фінансових засобів, витоку службової інформації, її розголошення, втрати, знищення і спотворення. Виходячи з цього виникає проблема розробки засобів та заходів забезпечення інформаційної безпеки підприємства.

В ході виконання магістерської роботи були описані законодавчі, стандартизаційні та організаційно-технічні заходи забезпечення інформаційної безпеки, проаналізована модель для забезпечення системи інформаційної безпеки, яка визначає ймовірність виявлення загроз при порушенні ІБ.

В першому розділі роботи було висвітлено поняття та зміст організації інформаційної безпеки, описано методи та засоби забезпечення інформаційної безпеки та їх основні характеристики. Також здійснено огляд основних заходів, спрямованих на забезпечення інформаційної безпеки, а саме: законодавчі, стандартизаційні та організаційно-технічні заходи. Проте з появою все більшою кількістю загроз, які виникають в процесі діяльності підприємств, організацій, постала проблема для розробки та створення нових та більш ефективно дієвих засобів та заходів захисту інформації. Також, для вирішення проблем інформаційної безпеки необхідне сполучення законодавчих, організаційно-технічних і стандартизаційних заходів забезпечення інформаційної безпеки. Система управління інформаційною безпекою підприємства повинна включати: аутентифікацію (користувачів, даних, додатків, послуг, тощо); авторизацію (авторизований перелік цін, ключових торговельних документів, партнерів, користувачів, керівництва); аудит інформаційних ресурсів та послуг.

У другому розділі було роглянуто методичні підходи до побудови системи інформаційної безпеки підприємства, проаналізовані загрози та ризики ІБ підприємтсва. Для моделювання та оцінки інформаційної безпеки спочатку було визначено усі можливі загрози, які можуть призвести до порушення

роботи підприємства. Для того, щоб система захисту інформації на підприємстві працювала ефективно було проаналізовано використання моделей системи інформаційної безпеки.

Третій розділ магістерської роботи присвячено рекомендаціям по вдосконаленню організації ІБ підприємства ТОВ «Феракс». Формування ІБ підприємств є складним управлінським процесом, який потребує використання системного та комплексного підходів до управління. Для успішного впровадження на підприємствах ефективної системи організації інформаційної безпеки необхідне відповідне методичне забезпечення цього процесу. Сьогодні існує достатньо велика кількість методів забезпечення інформаційної безпеки: засоби шифрування інформації, що зберігається на комп'ютерах і передається по мережі; засоби ідентифікації та автентифікації користувачів; міжмережеві екрани; віртуальні приватні мережі; засоби антивірусного захисту; інструменти які перевіряють цілісність вмісту дисків; системи виявлення вразливостей мереж і аналізатори мережевих атак.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Про захист інформації в інформаційно-телекомунікаційних системах. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/ed19940705
2. Литвинюк А.А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування // А.А. Литвинюк [Електронний ресурс]. – Режим доступу: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf
3. Власова Л.А. Защита информации / Л.А. Власова. – Хабаровск: РИЦ ХГАЭП, 2017. – 84 с.
4. Матиев Д. Средства защиты информации: проблема выбора и соответствия / Д. Матиев [Електронний ресурс]. – Режим доступу: http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-i-sootvetstviya-5386161/
5. Замкова Т.В. Проблемы защиты информации в современных информационных системах / Т.В. Замкова [Електронний ресурс]. – Режим доступу: http://www.rae.ru/snt/?section=content&op=show_article&article_id=3893
6. Інформаційна безпека та методи захисту інформації [Електронний ресурс]. – Режим доступу: http://irbis-nbuv.gov.ua/cgi-bin/opac/search.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Vznu%5Feco%5F2016%5F1%5F21%2Epdf
7. Особливості організації інформаційної безпеки сучасного підприємства [Електронний ресурс]. – Режим доступу: http://sophus.at.ua/publ/2014_04_17_18_kampodilsk/sekcija_4_2014_04_17_18/osoblivosti_organizaciji_informacijnoji_bezpeki_suchasnogo_pidpriemstva/54-1-0-931

8. Інформаційна безпека [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1
9. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О. М. Горбатюк // Вісник Київського університету імені Т. Шевченка. − 2015. − № 14: Міжнародні відносини. − С. 46-48.
10. Литвиненко, О. Інформація і безпека / О. Литвиненко // Нова політика. – 1998. – № 1. – С. 47-49.
11. Про інформацію: закон України: [офіц. текст: за станом на 02 жовтня 1992 року]. − К.: Парламентське видво, 1996. − Т.4.
12. Про захист інформації в автоматизованих системах: закон України: [офіц. текст: за станом на 05 липня 1994 року]. – К.: Парламентське вид-во, 1996. – Т.7.
13. Баринов А. Информационный суверенитет или информационная безопасность? / А. Баринов // Національна безпека і оборона. – 2016. – № 1. – С. 70-76.
14. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О. М. Горбатюк // Вісник Київського університету імені Т. Шевченка. – 2015. – № 14 : Міжнародні відносини. – С. 46-48
15. Остроухов В. В. До проблеми забезпечення інформаційної безпеки України / В. В. Остроухов // Політичний менеджмент. – 2008. – № 4. – С. 135–141.
16. Бучило И. Л. Информационное право: основы практической информации: монографія / И. Л. Бучило. – М., 2011. – 253 с.
17. Забезпечення інформаційної безпеки на підприємстві [Електронний ресурс]. – Режим доступу: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/24811/st_51_18.pdf?sequence=1

18. Указ Президента "Про Стратегію національної безпеки України" від 6 травня 2015 року [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/287/2015
19. Роговец В. Информационные войны в современном мире: причины, механизмы, последствия / В. Роговец // Персонал. – № 5. – С. 34-40
20. Иванов О. В. Информационная составляющая современных войн / О. В. Иванов // Вестн. Моск. ун-та. Сер. 18: Социология и политология. – 2014. – № 4. – С. 64–70. 5
21. Забезпечення інформаційної безпеки на підприємстві [Електронний ресурс]. – Режим доступу: http://www.econindustry.org/arhiv/html/2010/st_51_18.pdf
22. Політика інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://wiki.tntu.edu.ua/%D0%9F
23. Апаратна і програмна ІБ [Електронний ресурс]. – Режим доступу: http://eir.zntu.edu.ua/bitstream/123456789/4885/1/MR_Vereshchaka.pdf
24. Герасименко О. В. Інформаційна безпека підприємства: поняття та методи її забезпечення / О. В. Герасименко, А. В. Козак. – 2015. – № 2.
25. Міжнародний менеджмент [Електронний ресурс]. – Режим доступу: http://pidruchniki.com/14940511/menedzhment/organizatsiya_mizhnarodnih_dilovih_operatsiy
26. Організація як процес [Електронний ресурс]. – Режим доступу: https://studopedia.info/ukr/1-443.html
27. Організація інформаційного забезпечення підприємницької діяльності [Електронний ресурс]. – Режим доступу: https://stud.com.ua/21268/pravo/organizatsiya/
28. Організація інформаційного забезпечення підприємницької діяльності [Електронний ресурс]. – Режим доступу: http://stud.com.ua/21268/pravo/organizatsiya_informatsiynogo_zabezpechennya_pidpriyemnitskoyi_diyalnosti

29. Угрозы информационной безопасности [Електронний ресурс]. – Режим доступу: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/
30. Ущерб от вируса WannaCry [Електронний ресурс]. – Режим доступу: https://www.rbc.ua/rus/news/ushcherb-virusa-wannacry-otsenili-1-mlrd-1495683784.html
31. Вирусы в Internet [Електронний ресурс]. – Режим доступу: https://itc.ua/articles/virusy_v_internet_jeto_dolzhen_znat_kazhdyj_483/
32. Угрозы информационной безопасности [Електронний ресурс]. – Режим доступу: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/
33. Загрози інформаційної безпеки [Електронний ресурс]. Режим доступу: http://vostokm.com.ua/info/2019/12/uk/bezopasnost-zagrozi-informacijnoi-bezpeki.aspx
34. Модель побудови системи інформаційної безпеки [Електронний ресурс]. – Режим доступу: http://pidruchniki.com/1237070651274/ekonomika/model_pobudovi_sistemi_informatsiynoyi_bezpeki
35. Безпека банківської діяльності [Електронний ресурс]. – Режим доступу: https://dn.khnu.km.ua/dn/k_default.aspx?M=k0786&T=01&lng=1&st=0
36. Залєвська І. Інформаціна безпека: нові підходи до визначення поняття [Електронний ресурс] / І. Залєвська // Український науковий журнал "ОСВІТА РЕГІОНУ". – 2016. – Режим доступу: http://social-science.com.ua/article/352.
37. Ортинський В. Л. Економічна безпека підприємств, організацій та установ. Модель побудови системи інформаційної безпеки / В. Л. Ортинський [Електронний ресурс]. – Режим доступу: http://westudents.com.ua/glavy/16530-model-pobudovi-sistemi-nformatsyno-bezpeki.html

38. Журавель М. М. Аналіз принципів побудови моделей інформаційної безпеки в корпоративних інформаційних системах [Електронний ресурс] / М. М. Журавель, С. В. Паршуков. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=4257
39. Аникин И. В. Теория информационной безопасности и методология защиты информации / И. В. Аникин, В. И. Глова, Л. И. Нейман, А. Н. Нигматуллина. – Казань: Изд-во Казан. гос. техн. ун-та, 2008. – 358с.
40. Возможная методика построения системы информационной безопасности предприятия [Електронний ресурс]. – Режим доступу: http://sec4all.net/konf2.html
41. Данчук В. Д. Удосконалення методів забезпечення інформаційної безпеки корпоративних інформаційних систем / В. Д. Данчук, В. Є. Ананченко, О. Є. Ананченко // Збірник наукових доповідей та тез науково-технічної конференції «Інформаційна безпека України» Київського національного університету ім. Т.Шевченка 12-13 березня 2015. – К. – С. 96-97.
42. Зегжда Д. П. Основи безпеки інформаційних систем / Д. П. Зегжда, А. М. Івашко. – М .: Інтуїт, 2016.
43. Журавель М. М. Проблеми захисту інформації [Електронний ресурс] / М. М. Журавель, С. В. Паршуков. – Режим доступу: http://informatika.udpu.org.ua/?page_id=1173
44. Процесні підходи до моделювання у сфері управління ризиками інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://cyberleninka.ru/article/n/protsesni-pidhodi-do-modelyuvannya-u-sferi-upravlinnya-rizikami-informatsiynoyi-bezpeki
45. Кавун С. В. Інформаційна безпека. Навчальний посібник. Ч.1 [Текст] / С. В. Кавун, В. В. Носов, О. В. Мажай. – Харків: Вид. ХНЕУ, 2013. – 352 с.
46. Коновал Д. Комплексный подход к организации системы защиты информации на предприятии: основные вопросы и технологии / Д. Коновал [Електронний ресурс]. – Режим доступу: http://www.epam-

group.ru/aboutus/news-and-events/articles/2009/aboutus-ar-gaz-prom-09-01-2009.html#sthash.qruifGvr.dpuf

47. Концептуальная модель информационной безопасности [Електронний ресурс]. – Режим доступу: http://www.pki-exam.narod.ru/ib/t2/p2.html.
48. Конев И. Р. Информационная безопасность предприятия [Текст] / И. Р. Конев, А. В. Беляев. – СПб.: БХВ-Петербург, 2013. – 747 с.
49. Корнюшин П. Н. Информационная безопасность [Текст] / П. Н. Корнюшин, С. С. Костерин. – Владивосток: ТИДОТ ДВГУ, 2013. – 154 с.
50. Обеспечение информационной безопасности предприятия [Електронний ресурс]. – Режим доступу: http://www.arinteg.ru/articles/informatsionnaya-bezopasnost-predpriyatiya-25799.html
51. Щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0365500-11
52. Конфіденційна інформація [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%9A%D0%BE
53. Цілісність інформації [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A6%D1%96%D0
54. Доступность информации [Електронний ресурс]. –Режим доступу: https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D1
55. Методичне забезпечення системи інформаційної безпеки промислових підприємств. [Електронний ресурс]. – Режим доступу: jeou.donnu.edu.ua/article/download/1041/1059
56. Загрози інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3
57. Інформаційна безпека: питання правового регулювання [Електронний ресурс]. – Режим доступу: http://elibrary.kubg.edu.ua/id/eprint/18860/1/A_Nashinets-Naumova_monografia_1_FPMV.pdf

58. Аналітичне забезпечення інформаційної безпеки [Електронний ресурс]. – Режим доступу: http://mpsesm.org/index.php/mpsesm/mpsesm7/paper/download/328/251
59. Сутність та сучасні принципи використання інформаційної безпеки на підприємстві [Електронний ресурс]. – Режим доступу: https://er.knutd.edu.ua/bitstream/123456789/7279/1/V109_P062-069.pdf
60. Совершенствование системы информационной безопасности на предприятии [Електронний ресурс]. – Режим доступу: http://gm3d.ru/referaty_po_gosudarstvu_i_pravu/kursovaya_rabota_sovershenstvovanie_15.html