МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію
Завідувач кафедри УІКБ
Доктор економічних наук, доцент
_____С.В.Легомінова
«___»_____20__ р.

До захисту
Завідувач кафедри УІКБ
Доктор економічних наук, доцент
_____С.В.Легомінова
«___»_____20__ р.

**ДИПЛОМНА РОБОТА**

на тему:

# УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНІЗАЦІЇ

СТУДЕНТ: Озерінін Федір Олексійович _____

(підпис)

КЕРІВНИК: к.т.н., доц. Якименко Юрій Михайлович _____

(підпис)

НОРМОКОНТРОЛЕР: к.держ.упр. Мужанова Тетяна Михайлівна _____

(підпис)

Київ – 2021

**МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ**

**Навчально-науковий інститут захисту інформації**
**Кафедра Управління інформаційною та кібернетичною безпекою**
Освітньо-кваліфікаційних рівень – магістр
Спеціальність «Кібербезпека»
Спеціалізація «Управління інформаційною безпекою»

**Освітньо-кваліфікаційний рівень** – магістр
**Галузь знань** – «12 Інформаційні технології»
**Спеціальність** – «125 Кібербезпека»
**Спеціалізація** – «Управління інформаційною безпекою»

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
д.е.н. доцент_____ С.В.Легомінова
(підпис)
“___” _____20__ р.

**ЗАВДАННЯ**

**на дипломну роботу**

студенту Озерініну Федіру Олексійовичу

1. **Тема роботи** “ Управління забезпеченням політики інформаційної безпеки в організації ”, затверджена наказом по університету від “13” жовтня 2020 р. №.230

2. **Термін здачі** студентом закінченої дипломної роботи 25 грудня 2020 р.

3. **Об’єкт дослідження**: забезпечення інформаційної безпеки організації.

4. **Предмет дослідження**: політика інформаційної безпеки організації.

5. **Мета дослідження**: аналіз та складення рекомендацій щодо управління політикою інформаційної безпеки організації.

6. **Перелік обов’язкових демонстраційних креслень**:

6.1. Схема забезпечення політики інформаційної безпеки організації.

6.2. Структурно-логічна схема дій керівництва організації по управлінню забезпеченням політики інформаційної безпеки організації

6.3. Схема алгоритму розробки та впровадження політики інформаційної безпеки організації.

6.4. Рекомендації щодо управління забезпеченням політики інформаційної безпеки в організації (для вибраного прикладу).

6.5. Презентація доповіді, виконана в Microsoft PowerPoint.

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

7.1. Провести аналіз по основам управління забезпеченням політики інформаційної безпеки в організації, нормативно-правового забезпечення політики інформаційної безпеки організації.

7.2. Дослідити особливості роботи керівництва по управлінню забезпечення політики інформаційної безпеки організації, зокрема сформувати структурно-логічну схему роботи керівництва по забезпеченню політики інформаційної безпеки організації.

7.3. Провести дослідження процесів розробки та впровадження політики інформаційної безпеки організації.

8. **Дата видачі завдання** «26» жовтня 2020 р.

**Календарний план**

Дата видачі завдання 26.10.2020 року

| № з/п | Назва етапів магістерської атестаційної роботи | Термін виконання етапів | Відмітка про виконання |
|---|---|---|---|
| 1. | Підбір науково-технічної літератури. | 29.10.2020 р. | |
| 2. | Аналіз та систематизація матеріалу. Вступ | 05.11.2020 р. | |
| 3. | Аналіз основ по управлінню забезпеченням політики інформаційної безпеки організації. | 13.11.2020 р. | |
| 4. | Аналіз особливості роботи керівництва по управлінню забезпеченням політики інформаційної безпеки організації. | 01.12.2020 р. | |
| 5. | Дослідження процесів розробки та впровадження політики інформаційної безпеки організації. | 15.12.2020 р. | |
| 6. | Оформлення та друк пояснювальної записки | 25.12.2020 р. | |
| 7. | Отримання відгука та рецензії на роботу | 29.12.2020 р. | |
| 8. | Оформлення презентацій | 04.01.2021 р. | |
| 10. | Попередній захист на кафедрі | 08.01.2021 р. | |
| 11. | Захист в ДЕК | ___01.2021 р. | |

Керівник _____ Якименко Юрій Михайлович

(підпис) (прізвище, ім’я, по-батькові)

Завдання прийняв _____ Озерінін Федір Олексійович

для виконання (підпис) (прізвище, ім’я, по-батькові)

## РЕФЕРАТ

Дипломна робота написана за складеним планом, містить вступ, три розділи з підрозділами, що містять 10 рисунків, висновки, список використаних джерел. Загальний обсяг роботи – 105 сторінок, з яких 8 аркушів займають перелік скорочень та список використаних джерел.

**Об'єкт дослідження** – політика інформаційної безпеки організації.

**Предмет дослідження** – управління забезпеченням політики інформаційної безпеки організації.

**Метою роботи** є проведення аналізу процесів управління забезпеченням політики інформаційної безпеки і її впровадженням на прикладі вибраної моделі організаційно-функціональної структури організації та на основі отриманих результатів - розробка рекомендацій щодо поліпшення дій керівництва в процесах забезпечення і впровадження політики інформаційної безпеки в організації.

**Методи дослідження** – для вирішення означеного наукового завдання в роботі використані методи аналізу, синтезу, порівняння, проектування, методи системного аналізу та теорія інформаційної безпеки

У магістерській атестаційній роботі проаналізовано вимоги міжнародних та державних стандартів до формування політики інформаційної безпеки організації; досліджені нормативні вимоги до розробки політики, етапи та ресурси, що задіяні для забезпечення політики інформаційної безпеки організації; дії керівництва на етапах її розробки та впровадження. досліджені особливості роботи і ролі керівництва у цих процесах.

**Сфера застосування.** Розроблені підходи можуть бути використані при розробці, впровадженні та управлінні забезпеченням політики інформаційної безпеки організації.

**Ключові слова:** ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА ОРГАНІЗАЦІЇ, СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

**ЗМІСТ** Стор.

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

АС – автоматизована система

ДСТУ – Державні стандарти України

ЗІ – захист інформації

ІБ – інформаційна безпека

ІКТ – інформаційно-комунікаційні технології

ІС – інформаційна система

ІТ – інформаційні технології

ПЗ – програмне забезпечення

СЗІБ – система захисту інформаційної безпеки

СУІБ – система управління інформаційною безпекою

СМІБ – система менеджменту інформаційної безпеки

DoS – відмова в обслуговуванні

ISO – International Organization for Standardization

# ВСТУП

*Актуальність дослідження.* На сучасному етапі розвитку та широкого впровадження інформаційних технологій у всіх сферах життя та суспільної діяльності, жодне з організацій не може залишатися осторонь цих процесів. На відміну від минулого, коли конкурентоспроможність підприємства в більшості залежала від матеріальних чинників, сьогодні вона значною мірою залежить від здатності захищати свою ділову, технічну та комерційну інформацію.

Внаслідок цього, істотно посилюється значення інформаційної безпеки організації. Оскільки, втрати організацією своїх інформаційних ресурсів неминуче призводять до економічних та репутаційних втрат. Саме тому надійна система інформаційної безпеки відіграє ключову роль в забезпеченні економічного розвитку та стабільності організації.

Важливу роль в забезпеченні інформаційної безпеки будь-якої організації відіграє політика інформаційної безпеки, яка визначає цілі, методи та засоби забезпечення інформаційної безпеки. Інструментом забезпечення політики інформаційної безпеки є система управління інформаційною безпекою (СУІБ) організації.

Актуальність питання впровадження політики інформаційної безпеки організації пов’язано з швидким розвитком засобів і форм автоматизації процесів обробки інформації та високою залежністю від інформаційних ресурсів та мереж, що вимагає системного підходу до забезпечення політики інформаційної безпеки організації.

Об’єкт дослідження – політика інформаційної безпеки організації

Предмет дослідження – управління забезпеченням політики інформаційної безпеки організації.

*Завдання дослідження*:

1. Провести аналіз по основам управління забезпеченням політики інформаційної безпеки в організації, нормативно-правового забезпечення політики інформаційної безпеки організації

2. Дослідити особливості роботи керівництва по управлінню забезпечення політики інформаційної безпеки організації, зокрема сформувати структурно-логічну схему роботи керівництва по забезпеченню політики інформаційної безпеки

3. Дослідити процеси розробки та впровадження політики інформаційної безпеки організації (на прикладі)

*Наукова новизна одержаних результатів*

Проведені дослідження процесів забезпечення політики інформаційної безпеки організації на основі вибраної моделі організаційно-функціональної структури організації визначають роль та місце керівництва організації у цих процесах. Розроблена структурно-логічна схема дій керівництва у процесах забезпечення політики інформаційної безпеки організації. Розроблені підходи та рекомендації можуть бути використані при проектуванні, плануванні та реалізації забезпеченні політики інформаційної безпеки організації з іншою організаційно-функціональною структурою.

*Практичне значення одержаних результатів*

Результати досліджень можна використовувати на практиці для забезпечення політики інформаційної безпеки в цілому та управління окремими процесами розробки та впровадження політики інформаційної безпеки організації.

# РОЗДІЛ 1
# АНАЛІЗ ОСНОВ ПО УПРАВЛІННЮ ЗАБЕЗПЕЧЕННЯМ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Для дослідження процесів управління забезпеченням політики інформаційної безпеки організації необхідно визначити цілі, принципи та методи забезпечення інформаційної безпеки, вимоги нормативних документів до розроблення, впровадження та забезпечення політики інформаційної безпеки організації, структуру забезпечення політики інформаційної.

## 1.1. Нормативно-правові засади управління інформаційною безпекою організації

У цьому розділі будуть розглянуті нормативно-правові засади управління інформаційною безпекою. Вони базуються на Законах України, міжнародних та державних стандартах, внутрішніх документах організації, які визначають цілі, принципи та методи забезпечення інформаційної безпеки, вимоги до розроблення та впровадження політики інформаційної безпеки організації.

### 1.1.1 Цілі, принципи та методи забезпечення інформаційної безпеки

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління організації, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу інформаційної безпеки організації. В основі побудови система управління інформаційною безпекою лежить політика інформаційної безпеки організації.

Головною метою забезпечення політики інформаційної безпеки є забезпечення сталого функціонування організації і запобігання загрозам її інформаційній безпеці, розголошенню, втраті, витоку, перекручуванню та знищенню службової інформації, порушенню роботи технічних засобів, забезпечення виробничої діяльності, включаючи і засоби інформатизації.

В основі досягнення цієї мети лежить вирішення наступних завдань:

- прогнозування і своєчасне виявлення та усунення загроз безпеки інформації, причин і умов, що сприяють порушенню нормального функціонування організації;
- віднесення інформації до категорії обмеженого доступу (державної, службової та комерційної таємниць, іншої конфіденційної інформації, що підлягає захисту від неправомірного використання), та інших ресурсів - до різних рівнів уразливості (небезпеки) і підлягають збереженню;
- створення механізму і умов оперативного реагування на загрози інформаційній безпеці і прояв негативних тенденцій у функціонуванні ІС;
- ефективна протидія загрозам персоналу і зазіханням на ресурси на основі правових, організаційних та інженерно-технічних заходів і засобів забезпечення безпеки;
- створення умов для ослаблення негативного впливу наслідків порушення безпеки на досягнення стратегічних завдань організації.

Політика інформаційної безпеки організації розробляється за рішенням вищого керівництва комісією з інформаційної безпеки, яка призначається наказом вищого керівництва.

Згідно до стандарта ДСТУ ISO/IEC 27001 організація має визначити політику інформаційної безпеки на основі характеристик бізнесу, організації, її розміщення, активів та технологій. Тобто, політика – це загальні наміри та вказівки, офіційно виражені керівництвом. Зміст політики управляє діями та рішеннями, що стосуються предмету політики. Організація може мати декілька політик, по одній для кожної сфери діяльності, важливої для організації. Деякі політики незалежні одна від одної, в той час як інші політики знаходяться в ієрархічному співвідношенні. В галузі безпеки, політики, як правило, ієрархічно організовані. [1]

Зазвичай, політика безпеки організації являється політикою вищого рівня. Вона підкріплена більш конкретними політиками, включаючи політику інформаційної безпеки та політику системи менеджменту інформаційної безпеки. Політика інформаційної безпеки може бути підкріплена більш детальними

політиками з конкретних предметів, що відносяться до аспектів інформаційної безпеки. Більшість цих політик описані в стандарті ДСТУ ISO/IEC 27002, наприклад політика інформаційної безпеки підкріплена політиками, що стосуються контролю доступу, політики «чистого столу» та «чистого екрану», використання мережевих служб та криптографічного контролю. В деяких випадках можливе створення додаткових рівней політики.

Зміст політики має бути заснований на контексті організації. Проте, при розробці будь-якої політики в рамках основ треба взяти до уваги наступні фактори:

- Цілі та задачі організації: представляють собою цілі та задачі, визначені в корпоративній політиці організації. Політика інформаційної безпеки не повинна протирічити основним цілям бізнесу організації та повинна грати не ключову, а роль забезпечення розвитку бізнесу
- Стратегії, адаптовані для досягнення цих цілей: стратегія, що визначена в корпоративній політиці організації як комплекс стратегічних планів, засобів та методів для забезпечення виконання довгострокових бізнес-цілей організації
- Структура та процеси, адаптовані організацією: політика ІБ повинна бути побудована таким чином, щоб не порушувати основну діяльність організації. Для цього доцільно провести аналіз основних бізнес-процесів та адаптувати під них процеси ІБ. Політика ІБ в організації регламентує допоміжні та управлінські процеси підприємства
- Цілі та задачі, зв’язані з предметом політики: політика ІБ має чітко виражати цілі та задачі ІБ, основні аспекти забезпечення ІБ, методи та засоби, що використовуються для цього та вимоги до організації системи в цілому
- Вимоги політик більш високого рівня: політика ІБ організації має забезпечувати склад та напрям дій для забезпечення захисту інформації

Склад СУІБ – в політиці має бути визначений склад основних систем, що забезпечують безпеку підприємства, а також деталізація до підсистем СУІБ. Цей пункт необхідний для об’єднання в політиці регламенту як фізичного захисту, так і для СУІБ. Перелік окремих політик, рекомендованих для створення в організації

визначається стандартом ДСТУ ISO/IEC 27003:2018. В контексті діяльності досліджуваної організації, автор пропонує введення таких політик:

- Політика управління активами
- Політика контролю доступу
- Політика управління ризиками
- Політика управління документацією
- Політика резервного копіювання
- Політика використання корпоративної мережі
- Політика ведення записів

Принципи – опис правил, що стосуються дій та рішень для досягнення цілей, ключові процеси, пов’язані з виконанням політики та правила організації таких процесів

Сфери відповідальності – в цьому пункті розглядаються працівники, що відповідають за виконання даної політики в області її дії, роль менеджерів в забезпеченні виконання політики всіма співробітниками організації.

Політики в області безпеки – опис інших політик, що існують в організації для досягнення цілей даної політики.

Структура політики інформаційної безпеки організації повинна найбільш повно визначати вимоги до забезпечення захисту та у загальному випадку містити наступні положення:

- Загальні положення
- Призначення і правова основа документа
- Область дії політики
- Цілі і завдання забезпечення безпеки інформації
- Інтереси зацікавлених сторін інформаційних відносин
- Цілі менеджменту інформаційної безпеки
- Завдання системи забезпечення інформаційної безпеки
- Основні шляхи вирішення завдань системи захисту
- Напрями забезпечення інформаційної безпеки

- Принципи забезпечення інформаційної безпеки
- Область дії політики інформаційної безпеки
- Організація системи забезпечення інформаційної безпеки
- Об'єкти захисту
- Категорії інформаційних ресурсів, що підлягають захисту
- Політика класифікації ресурсів
- Основні загрози безпеки інформації
- Основні принципи побудови системи інформаційної безпеки
- Управління ризиками інформаційної безпеки
- Заходи забезпечення інформаційної безпеки
- Законодавчі (правові) заходи захисту
- Морально-етичні заходи захисту
- Технологічні заходи захисту
- Організаційні (адміністративні) заходи захисту
- Фізичні та технічні заходи
- Засоби забезпечення інформаційної безпеки
- Фізичні засоби захисту
- Технічні засоби захисту
- Засоби ідентифікації і аутентифікації користувачів
- Засоби розмежування доступу
- Засоби забезпечення та контролю цілісності
- Засоби оперативного контролю і реєстрації подій безпеки
- Криптографічні засоби захисту інформації
- Організація робіт із захисту інформації
- Розподіл відповідальності і порядок взаємодії
- Технічне забезпечення інформаційної безпеки
- Управління доступом до ресурсів ІС
- Регламентація доступу в приміщення

- Регламентація допуску співробітників до використання інформаційних ресурсів
- Регламентація процесів обслуговування і здійснення модифікації апаратних і програмних ресурсів
- Забезпечення і контроль фізичної цілісності (незмінності конфігурації) апаратних ресурсів
- Політика управління персоналом
- Підбір та підготовка персоналу, навчання користувачів
- Підрозділ забезпечення інформаційної безпеки
- Відповідальність за порушення встановленого порядку користування ресурсами інформаційної системи організації. Розслідування порушень
- Управління системою забезпечення безпеки інформації
- Принципи організації та функціонування системи безпеки
- Основні фактори, що впливають на інформаційну безпеку підприємства
- Основні принципи забезпечення інформаційної безпеки
- Контроль ефективності системи захисту
- Пропозиції по програмі створення системи безпеки

Реалізація вимог політики безпеки забезпечується шляхом побудови системи управління інформаційною безпекою, яка має базуватися на дотриманні наступних основних принципів забезпечення ІБ:

1. простота архітектури, мінімізація і спрощення зв'язків між компонентами, уніфікація і спрощення компонентів, використання мінімального числа протоколів мережевого взаємодії. Система повинна містити лише ті компоненти і зв'язки, які необхідні для її функціонування (з урахуванням вимог надійності та перспективного розвитку);
2. апробованість рішень, орієнтація на рішення, можливі ризики для яких і заходи протидії цим ризикам пройшли всебічну теоретичну і практичну перевірку;
3. побудова системи з компонентів, що володіють високою надійністю;

4. керованість, можливість збору реєстраційної інформації про всі компоненти і процесах, наявність засобів раннього виявлення порушень інформаційної безпеки, нештатної роботи апаратури, програм і користувачів;

5. простота експлуатації, автоматизація максимального числа дій адміністраторів;

6. ешелонування оборони - для кожної загрози безпеки повинно існувати кілька захисних рубежів;

7. безперервність захисту - системи повинні перебувати в захищеному стані протягом усього часу їх функціонування. Відповідно до цього принципу вживаються заходи щодо недопущення переходу систем в незахищене стан;

8. економічна доцільність витрат на забезпечення безпеки (критерій «ефективність - вартість»). У всіх випадках вартість системи безпеки повинна бути меншою за розмір можливого збитку від будь-яких видів ризику;

9. профілактика порушень безпеки - в більшості випадків для організації економічно виправданим є вжиття запобіжних заходів щодо недопущення порушень безпеки на відміну від заходів по реагуванню на інциденти, пов'язаних з прийняттям ризиків здійснення загроз інформаційній безпеці.;

10. мінімізація привілеїв - політика безпеки повинна будуватися на основі принципу «все, що не дозволено, заборонено». Права суб'єктів повинні бути мінімально достатніми для виконання ними своїх службових обов'язків;

11. спадкоємність і безперервність вдосконалення. Забезпечення постійного вдосконалення заходів і засобів захисту інформаційних ресурсів та інформаційної інфраструктури на основі наступності організаційних і технічних рішень, кадрового апарату, аналізу функціонування систем захисту з урахуванням змін в методах і засобах перехоплення інформації, нормативних вимог щодо її захисту, досягнутого передового вітчизняного та зарубіжного досвіду в цій галузі;

12. законність - передбачає розробку системи безпеки на основі національного законодавства в галузі інформатизації та захисту інформації та інших нормативних актів з безпеки, затверджених органами державного

управління в межах їх компетенції, із застосуванням всіх дозволених методів виявлення і припинення правопорушень;

13. централізація управління - передбачає самостійне функціонування системи безпеки за єдиними правовим, організаційним, функціональним і методологічним принципам і централізованим управлінням діяльністю системи безпеки;

14. контроль з боку керівництва - діяльність щодо забезпечення інформаційної безпеки ініційована і контролюється вищим керівництвом. Керівництво на регулярній основі розглядає звіти про стан інформаційної безпеки в структурних підрозділах, відділах, службах і фактах порушень встановлених вимог, а також загальні та приватні питання інформаційної безпеки, пов'язані з використанням технологій підвищеного ризику або істотно впливають на бізнес-процеси;

15. персональна відповідальність - всі співробітники організації несуть персональну відповідальність за дотримання вимог політики інформаційної безпеки. Обов'язки щодо забезпечення інформаційної безпеки включаються в трудові договори і посадові інструкції працівників, а так само угоди з контрагентами.

Діяльність із забезпечення політики інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у сукупності й складають методи. Метод передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування.

Що стосується сфери інформаційної безпеки, то у ній зазвичай виділяють наступні рівні реалізації політики безпеки:

1) фізичний;

2) програмно-технічний;

3) управлінський;

4) технологічний;

5) рівень користувача;

6) мережному;

7) процедурний.

На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються і управлінських технологіях.

На програмно-технічному рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки.

На технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища.

На мережному рівні дана політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою.

На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування відновлювальних робіт.

### 1.1.2. Вимоги нормативних документів по впровадженню політики інформаційної безпеки

Основними нормативними документами, які визначають вимоги та регламентують процедури впровадження політики інформаційної безпеки організації є стандарти ДСТУ ISO/IEC за номером 27001, 27002 та 27003.

ДСТУ ISO/IEC 27001 - цей стандарт описує загальну модель впровадження та функціонування СУІБ, а також дії з її розвитку та моніторингу. Мета цього стандарту полягає в узгодженості СУІБ з іншими механізмами управління компанії. ДСТУ ISO/IEC 27001 описує СУІБ як всеохоплюючу систему менеджменту, засновану на підході бізнес-ризиків, що призначена для створення, впровадження, експлуатації та підтримки СУІБ. Система має враховувати всі аспекти організаційної структури, політики, стратегію компанії, практики, процеси та процедури. [1]

ДСТУ ISO/IEC 27002 «Практичні правила менеджменту інформаційної безпеки» [2] є загальновизнаним міжнародним стандартом інформаційної безпеки, він дає детальний опис засобів управління безпекою, які забезпечують захист інформації та інформаційних технологій. ДСТУ ISO/IEC 27002 не визначає, як потрібно застосовувати ці засоби управління. Він дає напрямок для створення системи менеджменту, яке дозволяє вибрати засоби управління, організувати їх роботу з використанням кращих практик. Вибір процедур для реального впровадження засобів управління залишається за компанією, він буде залежати від її фізичного і технічного середовища.

ДСТУ ISO/IEC 27003 «Керівництво» містить керівні вказівки щодо вимог до системи управління інформаційною безпекою (СУІБ), як зазначено у стандарті ISO/IEC 27001, і надає рекомендації, можливості та дозволи щодо них. Цей документ не передбачає надання загальних рекомендацій з усіх аспектів інформаційної безпеки. Організації, що впроваджують СУІБ, не зобов'язані дотримуватися вказівок у цьому документі. СУІБ підкреслює важливість наступних етапів:

- розуміння потреб організації та необхідності встановлення політики інформаційної безпеки та цілей інформаційної безпеки;
- оцінка ризиків організації, пов'язаних з інформаційною безпекою;
- впровадження та керування процесами інформаційної безпеки, контролю та іншими заходами щодо ліквідації ризиків;
- моніторинг та перевірка продуктивності та ефективності СУІБ;

- впровадження постійного вдосконалення СУІБ.

Ці стандарти призначені для застосування до всіх організацій, незалежно від типу (державні чи комерційні) та розміру. Організація повинна визначити, яка частина цих стандартів поширюється на неї відповідно до її специфічного організаційного контексту. Деякі інструкції можуть бути придатними для великих організацій, але для дуже маленьких організацій (наприклад, з менш ніж 10 співробітниками) можуть бути непотрібними або неприйнятними

Стандарти управління інформаційною безпекою – це вимоги до системи менеджменту, яка визначає загальну організацію, класифікацію даних, системи доступу, напрямки планування, відповідальність співробітників, використання оцінки ризику і т. ін. в контексті інформаційної безпеки. У процесі впровадження стандарту створюється так звана система менеджменту інформаційної безпеки, мета якої скорочення матеріальних втрат, зв'язаних з порушенням інформаційної безпеки, забезпечення не тільки надійного захисту інформації, але також організація ефективного доступу до даних та нормальна робота з ними.

Згідно до вимог ДСТУ ISO/IEC 27001, побудова ефективної системи управління інформаційною безпекою можлива при реалізації напрямків наведених в табл. 1.1.

Таблиця 1.1

Напрямки побудови СУІБ згідно ДСТУ ISO/IEC 27000

<table>
<tr><td colspan="4">A.5 Політика в області безпеки</td></tr>
<tr><td colspan="4">A.6 Організація системи безпеки</td></tr>
<tr><td colspan="4">A.7 Класифікація активів та управління</td></tr>
<tr><td>A.8 Безпека та персонал</td><td>A.9 Фізична та зовнішня безпека</td><td>A.10 Менеджмент комп’ютерів та мереж</td><td rowspan="2">A.12 Придбання, розробка й обслуговування інформаційної системи</td></tr>
<tr><td colspan="3">A.11 Управління доступом до системи</td></tr>
<tr><td colspan="4">A.13 Менеджмент інцидентів інформаційної безпеки</td></tr>
<tr><td colspan="4">A.14 Забезпечення безперервності бізнесу</td></tr>
<tr><td colspan="4">A.15 Відповідність законодавства</td></tr>
</table>

Положення стандарту дозволяють вибрати для побудови системи управління інформаційною безпекою ті засоби управління, які мають відношення до конкретної організації або сфери відповідальності всередині організації. У зв'язку з цим, виділяється ряд ключових елементів управління, що подаються як фундаментальні. При цьому, поряд з елементами управління для комп'ютерів та комп'ютерних мереж, стандарт приділяє велику увагу питанням розробки політики безпеки, роботі з персоналом (прийом на роботу, навчання, звільнення з роботи), забезпечення безперервності виробничого процесу, юридичним вимогам. [5]

Стандарт дозволяє застосовувати підхід, при якому його використовують як набір рекомендацій, який необхідно застосовувати з урахуванням конкретних характеристик та умов функціонування організації. Застосування рекомендацій здійснюється на основі оцінки ризику та ретельно обґрунтовується. В залежності від рівня конфіденційності інформації, яка зберігається, обробляється та передається в організації, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні організації, а також інших чинників обґрунтовується пропозиція щодо доцільності застосування варіантів побудови СУІБ.

Можливі наступні варіанти побудови системи управління інформаційною безпекою організації:

1. досягнення необхідного рівня інформаційної безпеки за мінімальних затрат і допустимого рівня обмежень на технології зберігання, оброблення та передавання інформації у організації;

2. досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технології зберігання, оброблення та передавання інформації у організації;

3. досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технології зберігання, оброблення та передавання інформації у організації.

Рішення про вибір варіанту побудови СУІБ, джерел та обсягів фінансування робіт приймається вищим керівництвом організації. Досвід свідчить, що заходи і

засоби захисту виявляються більш ефективними та економічно доцільними, якщо вони інтегровані у технологічні процеси чи сервіси на стадіях вивчення вимог і проектування. Чим раніше організація впровадить заходи щодо захисту своїх інформаційних систем (продуктів), тим дешевшими та ефективнішими вони згодом будуть для неї.

Стандарт описує СУІБ як всеохоплюючу систему менеджменту, побудовану на принципах бізнес-ризиків, для впровадження, експлуатації, моніторингу та підтримки системи менеджменту безпеки.

Згідно до ДСТУ ISO/IEC 27001 [8], система управління інформаційною безпекою — це «та частина загальної системи управління організації, заснованої на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки».

Система управління інформаційною безпекою організації містить структуру організації, політики, планування, посадові обов’язки, практики, процедури, процеси і ресурси. Створення та експлуатація СУІБ вимагає застосування такого ж підходу, як і будь-яка інша система управління.

Рекомендована стандартом ДСТУ ISO/IEC 27001 для опису життєвого циклу СУІБ процесна модель передбачає безперервний цикл заходів PDCA (Plan-Do-Check-Act): планування, виконання, перевірка, вплив (управління, коригування), відомий як цикл Шухарта-Демінга - через наочну кругову графічну інтерпретацію стадій циклу (рис 1).

Цикл Демінга - це постійне коло регулювання удосконалення продукту і виробничих процесів, оптимізації окремих одиниць і об'єктів.

За допомогою постійних перевірок до, під час і після процесу виробництва, виховання відповідальності за якість і, перш за все, за допомогою постійного аудиту процесу виробництва можуть бути виявлені слабкі місця в різних процесах на підприємстві. PDCA служить саме для виявлення причин браку та підтримки всього процесу аж до усунення дефектів.

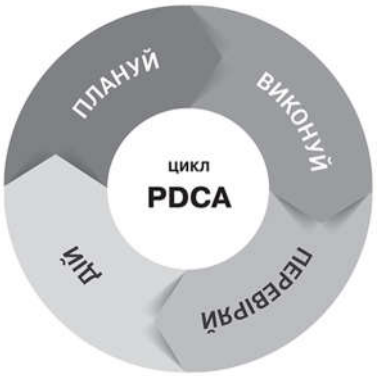


Рис. 1.1. Модель PDCA для впровадження СУІБ

Модель PDCA, з необхідними уточненнями, до теперішнього часу отримала широке застосування в міжнародних стандартах управління:

- Якістю продукції ISO 9001;
- Інформаційними сервісами ISO / IEC 20000;
- Інформаційною безпекою ISO / IEC 27000;
- Безпекою ISO 28000;
- Безперервністю бізнесу ISO 22300;
- Ризиками ISO 31000 та багато інших; [6]

Таблиця 1.2.

Опис циклу PDCA для впровадження СУІБ

| PDCA | Опис |
|---|---|
| Планування | Розроблення політики безпеки, визначення мети, процесів та процедур, пов'язаних з управлінням ризиками та підвищенням інформаційної безпеки для досягнення результатів відповідно до загальної політики та цілей організації |

Продовження табл. 1.2.

Опис циклу PDCA для впровадження СУІБ

| PDCA | Опис |
|---|---|
| Виконання | Впровадження та використання політики безпеки, елементів керування, процесів та процедур, механізмів контролю |
| Перевірка | Оцінювання та вимірювання ефективності роботи відповідно до політики безпеки, цілей та практичного досвіду, а також підготовка звіту про результати для керівництва з метою подальшого аналізу й аудиту |
| Дія (управління, коригування) | Застосування коригувальних та профілактичних заходів з метою досягнення постійного вдосконалення СУІБ на основі результатів аналізу; перегляд політики безпеки; підвищення інформованості персоналу |

Для побудови СУІБ організація має визначити ризики, пов’язані з її інформаційними активами. Досягнення інформаційної безпеки вимагає управління ризиком і охоплює ризики фізичні, людські та технологічні, що відносяться до погроз, що стосуються всіх форм інформації всередині організації або використовуваної організацією. Прийняття СУІБ є стратегічним рішенням для організації, і необхідно, щоб це рішення нерозривно інтегрувалося, оцінювалося і оновлювалося відповідно до потреб організації.

Одними із найважливіших процесів впровадження політики інформаційної безпеки організації є визначення області дії політики безпеки та розроблення плану впровадження політики інформаційної безпеки.

Детальне визначення області дії і меж по визначення політики інформаційної безпеки і, її прийняття і підтримка керівництвом, є ключовими первинними факторами для успішного впровадження СУІБ.

Щоб досягти мети «детального визначення області дії і меж СУІБ», необхідно виконати наступні дії:

a) визначити організаційну область дії і межі;

b) область дії і межі інформаційних і комунікаційних технологій (ІКТ);

c) фізичну область дії і межі;

d) конкретні характеристики і аспекти області дії і меж, пов'язані з підприємством, організацією, місцезнаходженням, активами і технологіями, і політика формуються в процесі визначення цієї області дії і меж.

Щоб побудувати ефективну систему управління для організації, необхідно детально визначити область дії СУІБ з урахуванням найважливіших інформаційних активів організації.

Важливо мати загальну термінологію і системний підхід для визначення інформаційних активів і оцінки життєздатних механізмів забезпечення безпеки. Це забезпечує простоту комунікації та сприяє сталому розумінню всіх фаз впровадження системи. Також важливо забезпечити включення в область дії системи найважливіших підрозділів організації.

Визначення організаційної області дії і меж, області дії і меж технології передачі інформації і фізичної області дії і меж не завжди має виконуватися послідовно.

Ступінь зусиль, необхідних для впровадження СУІБ, залежить від величини області дії, до якої ці зусилля докладаються. Цей фактор також може вплинути на всі дії, пов'язані з підтриманням інформаційної безпеки елементів, що входять в зону дії системи (наприклад, процесів, матеріальних об'єктів, інформаційних систем і людей), включаючи впровадження та супроводження засобів управління процесами та виконання таких завдань, як визначення інформаційних активів і оцінка ризику.

Якщо керівництво вирішує виключити деякі частини організації і області дії СУІБ, причини такого рішення також повинні бути задокументовані.

Коли визначена область дії СУІБ, важливо, щоб межі були досить ясними, щоб пояснити їх співробітникам, які беруть участь в їх визначенні.

Деякі заходи і засоби контролю і управління, що стосуються інформаційної безпеки, можуть вже існувати в організації в результаті введення в дію інших

систем управління. Їх слід враховувати при плануванні СУІБ, але вони не обов'язково визначають межі області дії існуючої СУІБ.

Сфери відповідальності, безпосередньо пов'язані з інформаційними активами або виробничими процесами, що включаються в область дії СУІБ, повинні вибиратися як частина організації, що знаходиться під контролем СУІБ. При визначенні організаційних меж слід враховувати наступні фактори:

1. Комісія по менеджменту СУІБ повинна складатися з керівних працівників, безпосередньо пов'язаних з областю дії СУІБ;

2. членом керівництва, відповідальним за СУІБ, повинен бути співробітник, який в кінцевому рахунку відповідає за всі порушені сфери відповідальності (тобто. його роль повинна диктуватися його сферою контролю та відповідальності в організації);

3. в разі, якщо співробітник, що відповідає за управління СУІБ, не є членом вищого керівництва, необхідний поручитель вищого керівництва, що представляє інтереси інформаційної безпеки і який діє у ролі захисника СУІБ на вищих рівнях організації;

4. область дії і межі необхідно визначити для того, щоб бути впевненим в тому, що всі пов'язані активи приймаються в розрахунок при оцінці ризику, і охопити ризики, які можуть вийти за межі цих меж.

На основі такого підходу аналізовані організаційні межі повинні визначати всіх співробітників, що потрапляють під дію СУІБ, і ці межі мають бути включені в область дії системи.

Визначення співробітників може бути пов'язано з процесами і (або) функціями в залежності від обраного підходу. Якщо деякі процеси в організації виконуються третіми сторонами, ці залежності повинні бути чітко задокументовані. Такі залежності підлягають додатковому аналізу в проекті впровадження СУІБ.

Результатом визначення організаційної області дії і меж має бути:

- опис організаційних меж СУІБ, включаючи обґрунтування виключення будь-яких частин організації з області дії СУІБ;

- функції і структура частин організації, що знаходяться в області дії СУІБ;
- визначення інформації, що підлягає обміну в рамках області дії системи, і інформації, обмін якою здійснюється через межі;
- процеси в організації і сфери відповідальності за інформаційні активи в області дії системи і за її межами;
- процес в ієрархії прийняття рішень, а також її структура в рамках СУІБ.

Визначення області дії і меж інформаційної та комунікаційної технологій може бути отримано на основі аналізу наявних інформаційних систем (замість підходу на основі інформаційних технологій). Коли приймається рішення керівництва про включення процесів інформаційної системи в область дії СУІБ, необхідно також розглянути всі пов'язані елементи інформаційно-телекомунікаційних технологій (ІКТ). Ці елементи включають всі частини організації, які зберігають, обробляють або передають важливу інформацію, активи або є важливими для інших частин організації, що входять в зону дії системи.

Якщо взяти до уваги вищесказане, межі ІКТ повинні включати опис наступних елементів:

a) інфраструктура зв'язку, в якій відповідальність за її управління входить в компетенцію організації, котра володіє різними технологіями (наприклад, бездротові і дротові мережі або мережі передачі даних і телефонного зв'язку);

b) програмне забезпечення в рамках організаційних меж, що використовується і контрольоване організацією;

c) апаратне забезпечення ІКТ, необхідну для мережі або мереж, додатків або виробничих систем;

d) ролі та сфери відповідальності, пов'язані з апаратним забезпеченням ІКТ, мережею і програмним забезпеченням.

Визначення фізичної області дії і меж полягає у визначенні приміщень, об'єктів і обладнання в організації, які повинні стати частиною СУІБ.

Фізичні межі, повинні включати опис наступних елементів:

- опис функцій або процесів з урахуванням їх фізичного місцезнаходження і ступеня контролю їх організацією;
- спеціального обладнання, яке використовується для зберігання (розміщення) апаратного забезпечення ІКТ або даних, що застосовуються в системі СУІБ (наприклад, на резервних плівках), на основі покриття меж ІКТ.

Результатом визначення фізичних меж СУІБ є:

- опис фізичних меж СУІБ з обґрунтуванням для виключення будь-яких фізичних меж, які перебувають під контролем організації, з області дії СУІБ;
- опис організації та її географічних характеристик, що відносяться до області дії СУІБ.

Область дії і межі СУІБ повинні бути отримані шляхом об'єднання всіх областей дії і меж: організаційної області дії і меж; області дії і меж інформаційних і комунікаційних технологій (ІКТ); фізичної області дії і меж.

Результат визначення області дії і межі СУІБ є документ «Положення про область дії СУІБ», що описує область дії і межі СУІБ і містить наступну інформацію:

- ключові характеристики організації (функція, структура, послуги, активи і область дії і межі відповідальності для кожного активу);
- процеси в організації, що знаходяться в області дії СУІБ;
- конфігурація обладнання та мереж, що знаходяться в області дії СУІБ;
- попередній перелік інформаційних активів, які перебувають в області дії СУІБ;
- перелік активів ІКТ, що знаходяться в області дії СУІБ (наприклад, серверів);
- схеми об'єктів, що знаходяться в області дії СУІБ, що визначають фізичні межі СУІБ;
- опис ролей та сфер відповідальності в рамках СУІБ і їх зв'язку зі структурою організації;
- докладний опис і обґрунтування виключень будь-яких елементів з області дії СУІБ.

Область застосування СУІБ повинна бути оформлена документально. Доцільно вказати область застосування СУІБ з використанням структурної та (або) логічної схеми інформаційної системи організації (частини інформаційної системи), на яке, буде поширювати свою дію СУІБ. У структурну схему, як правило, включають апаратні елементи, в тому числі і ті, які виконують функції захисту інформації, а також лінії електрозв'язку. У логічній схемі показують інформаційні системи і напрямки зовнішніх і внутрішніх потоків даних, а також специфікації використовуваних технологій і протоколів. [18]

Побудова системи управління інформаційною безпекою організації здіснюється відповідно до документу «План впровадження системи управління інформаційною безпекою», який розробляється комісією з інформаційної безпеки та затверджується вищим керівництвом організації. Розробка плану побудови СУІБ повинна визначити основні вимоги до складу робіт з впровадження системи менеджменту інформаційної безпеки, порядок, черговість і терміни виконання робіт, відповідальних виконавців і зацікавлені сторін по кожному процесу і роботі, передбаченими планом.

На етапі розробки (планування) комісії з інформаційної безпеки необхідно провести наступні заходи:

1. визначити (задокументувати) головні і допоміжні процеси основної діяльності організації;
2. визначити внутрішні і зовнішні аспекти, що впливають (обмеження) на досягнення результату впровадження СУІБ;
3. визначити зацікавлені сторони, а також їхні вимоги до основної діяльності організації (договірні зобов'язання; вимоги законодавства, локальних нормативних правових актів);
4. визначити сферу застосування СУІБ, враховуючи внутрішні і зовнішні аспекти, що впливають (обмеження) на досягнення результату впровадження СУІБ організації, вимоги зацікавлених сторін, а також існуючі зовнішні зв'язки і інтерфейси з іншими організаціями;
5. визначити фізичні і логічні межі області дії (застосування) СУІБ;

6. визначити цілі впровадження СУІБ, сумісні зі стратегією (концепцією) розвитку організації, і забезпечити інтеграцію вимог СУІБ з процесами діяльності організації;

7. розробити політику інформаційної безпеки;

8. провести інвентаризацію (виявлення і облік) активів організації:

9. апаратних засобів, фізичних пристроїв;

10. програмного забезпечення (прикладного та системного);

11. засобів обробки інформації, інформаційних систем та мереж;

12. інформації (відомостей), оброблюваної в системі;

13. потоків інформації і засобів комунікації;

14. посадових осіб та їх обов'язків в сфері інформаційної безпеки;

15. визначити засоби управління інформаційною безпекою, які застосовуються в організації;

16. визначити посадові особи, відповідальні за експлуатацію та встановлення правил використання активів (далі, якщо не визначено інше, - власники активів);

17. провести класифікацію (категорування) активів організації, з огляду на їхню соціальну значимість і критичність для основної діяльності організації;

18. визначити (розробити) методологію оцінки ризиків порушення інформаційної безпеки (методика управління ризиками, критерії оцінки ризиків);

19. оцінити ризики порушення інформаційної безпеки відповідно до обраної (розробленої) методологією;

20. розробити план обробки ризиків порушення інформаційної безпеки

21. розробити методику і процедури внутрішнього аудиту.

Етап впровадження полягає у виконанні всіх планів, пов'язаних з побудовою та вдосконаленням СУІБ, визначених на попередньому етапі, а також на етапі вдосконалення.

Зміст документу «План впровадження системи менеджменту інформаційної безпеки» має відповідати рекомендаціям міжнародного стандарту

Структура кожного пункту плану повинна включати:

- Фаза впровадження відповідно вимог ДСТУ ISO / IEC 27003
- Номер етапу
- Дії, посилання на ДСТУ ISO / IEC 27003
- Попередні умови для даного етапу
- Задокументовані вихідні дані
- Відповідальні виконавці та зацікавлені сторони
- Терміни виконання роботи.

На даному етапі вибираються засоби управління, відповідні ризикам порушення інформаційної безпеки, оціненим на попередньому етапі. Необхідно застосовувати захисні заходи, правильність роботи яких може бути перевірена. При цьому слід оцінювати ефективність реалізації і справну роботу пристроїв засобів управління.

Розробка положення про можливість застосування контролю, контрольного переліку, методики та плану внутрішнього аудиту системи інформаційної безпеки організації дозволяють на етапі впровадження та забезпечення політики інформаційної безпеки організації дозволяють керівництву організації здійснювати ефективний контроль повноти та відповідність вимогам стандартів процесів управління інформаційною безпекою організації.

## 1.2. Структура забезпечення політики інформаційної безпеки

Організація та проведення робіт по забезпеченню ІБ підприємства визначаються діючою концепцією, діючими державними та міжнародними стандартами та іншими нормативними й методичними документами. Структура забезпечення політики інформаційної безпеки організації наведена на рис. 1.2.


Рис. 1.2. Схема забезпечення політики інформаційної безпеки

Організаційні (адміністративні) засоби захисту – це засоби організаційного характеру, що регламентують процеси функціонування системи обробки даних, використання її ресурсів, діяльність обслуговуючого персоналу, а також порядок взаємодії користувачів з системою таким чином, щоб максимально ускладнити або виключити можливість реалізації загроз ІБ, або знизити шкоду у випадку їх реалізації.

Технічне забезпечення включає такі підсистеми ефективного захисту інформації у організації:

- Підсистема антивірусного захисту шлюзів входу в мережу Інтернет, файлових серверів, робочих місць користувачів, централізованого управління, періодичного оновлення антивірусних баз даних.

- Підсистема управління контролем доступу та ідентифікацією в інформаційній системі.
- Підсистема міжмережевого екранування, яка дозволяє реалізувати безпеку міжмережевої взаємодії через використання програмних і програмно-апаратних міжмережевих екранів.
- Підсистема криптографічного захисту, яка гарантує безпеку передачі інформації завдяки шифруванню даних.
- Підсистема забезпечення цілісності інформації та програмного середовища шляхом застосування відповідних засобів для фіксації та контролю стану програмного комплексу, управління зберіганням даних для резервного копіювання та архівування.
- Підсистема захисту від інсайдерів, яка контролює дії порушників, реалізує інформаційну безпеку при управлінні доступом і реєстрації.
- Підсистема захисту систем управління базами даних.
- Підсистема виявлення вторгнень і спроб несанкціонованого доступу до інформаційних ресурсів організації. Підсистема забезпечує реалізацію захисних заходів з протидії атакам хакерів і поширенню спаму.
- Підсистема захисту мобільних пристроїв.
- Підсистема моніторингу подій інформаційної безпеки, яка дозволяє своєчасно виявляти загрози інформаційній системі та оперативно реагувати на них. [43]

Технологічне забезпечення включає в себе захист інформації на нормативно-правовому рівні та складається з різних технологічних інструкцій, методик реалізацій процесів, документованих процедур та процесів діяльності щодо забезпечення ІБ.

Кадрове забезпечення включає в себе процес підбору персоналу, організація навчання працівників організації необхідним аспектам захисту інформації, донесення інструкцій до персонала та його атестація, а також контроль дотримання працівниками організації правил.

Методичне керівництво і контроль ефективності передбачених заходів захисту інформації – на директора з безпеки та керівника служби ІБ організації.

Організаційну структуру системи забезпечення ІБ організації можна представити у вигляді сукупності таких рівнів:


Рис. 1.3. Організаційна структура керівництва в системі забезпечення ІБ

- рівень 1 - керівництво організації;
- рівень 2 - підрозділ організації інформаційної безпеки;
- рівень 3 - адміністратори штатних і додаткових засобів захисту;
- рівень 4 - відповідальні за організацію інформаційної безпеки в підрозділах (на технологічних ділянках);
- рівень 5 - кінцеві користувачі і обслуговуючий персонал.

Крім того, на інформаційну безпеку організації можуть впливати сторонні особи і сторонні організації, як партнерські, так і такі, що мають за мету втручання в процес функціонування системи ІБ або несанкціонований доступ до інформації як локально, так і віддалено. [17]

Експлуатація ІС організації здійснюється у повній відповідності з затвердженою організаційно-розпорядною та експлуатаційною документацією, з урахуванням вимог та положень, викладених у відповідних розділах політики.

Комплекс засобів захисту інформації організації включає в себе наступні заходи:

- призначення ролей та розподіл відповідальності за використання інформаційних ресурсів корпоративної мережі
- розробка, реалізація, інтеграція та контроль виконання планів заходів, політик безпеки та інших документів щодо забезпечення ІБ
- підготовка користувачів та технічних спеціалістів до вирішення проблем, пов’язаних з забезпеченням ІБ
- проектування, введення та вдосконалення технічної інфраструктури СУІБ

Більшість фахівців у галузі захисту інформації вважають, що інформаційна безпека підтримується на належному рівні, якщо для всіх інформаційних ресурсів системи підтримується відповідний рівень конфіденційності (неможливості несанкціонованого отримання будь-якої інформації), цілісності (неможливості навмисної або випадкової її модифікації) і доступності (можливості оперативно отримати запитувану інформацію). [18]

## Висновки до першого розділу

В рамках першого розділу були досліджені основні питання нормативно-правових засад управління інформаційною безпекою шляхом аналізу вимог стандартів ДСТУ ISO/IEC серії 27к. Розглянуті цілі, принципи та методи забезпечення політики інформаційної безпеки організації.

Розроблена схема структури забезпечення політики інформаційної безпеки організації та схема організаційної структури дій керівництва у системі забезпечення управління інформаційною безпекою організації.

Проведено аналіз дій керівництва на різних фазах створення системи управління інформаційною безпекою організації. Отримані результати в подальшому будуть використані при дослідженні роботи керівництва організації по забезпеченню політики інформаційної безпеки організації.

# РОЗДІЛ 2
# АНАЛІЗ ОСОБЛИВОСТІ РОБОТИ КЕРІВНИЦТВА ПО УПРАВЛІННЮ ЗАБЕЗПЕЧЕННЯМ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Для аналізу особливості роботи керівництва по управлінню забезпеченням політики інформаційної безпеки організації необхідно дослідити вплив факторів повязаних з особливостями системи управління та функціонування організації, вимог та області дії політики безпеки. Для дослідження необхідно розробити організаційно-функціональну структуру організації та розробити структурно-логічну схему роботи керівництва.

## 2.1. Ресурси, які задіяні до розробки політики інформаційної безпеки

Виходячи з вимог нормативно-правового забезпечення, створення системи управління інформаційною безпекою, на першому етапі вищому керівництву організації потрібно визначити ресурси, необхідні для розробки політики інформаційної безпеки організації. Для дослідження ресурсів, необхідних для розробки політики інформаційної безпеки буде використано організаційно-функціональну структуру організації, наведену у розділі 2.2.

Вимоги до політики визначаються ДСТУ ISO/IEC 27001:

Найвище керівництво повинне встановити політику інформаційної безпеки, яка:

1. відповідає призначенню організації;
2. включає цільові показники в сфері інформаційної безпеки або служить основою для завдання таких показників;
3. включає зобов'язання щодо задоволення поставленим вимогам, пов'язані з інформаційною безпекою;
4. включає зобов'язання безперервного поліпшення системи менеджменту інформаційної безпеки.

Політика інформаційної безпеки повинна:

- бути оформлена як документована інформація;
- бути поширена в організації;
- бути доступною в установленому порядку для зацікавлених сторін.

Політика безпеки визначає стратегію підприємства в області ІБ, а також ту міру уваги і кількість ресурсів, яку керівництво вважає за доцільне виділити.

Для аналізу ресурсів, які задіяні до розробки політики інформаційної безпеки організації, пропонується застосувати процесний підхід, взявши за основу процеси розробки політики інформаційної безпеки визначені ДСТУ ISO/IEC 27003.

Кожен із процесів розробки політики інформаційної безпеки організації вимагає певного складу ресурсів, обумовленого специфікою змісту процесу.

Разом з тим, можна виділити ресурси, які використовуються для розробки політики інформаційної безпеки організації усіма процесами.

Це, насамперед:

- кадрові ресурси
- організаційні ресурси
- нормативно-правові ресурси
- Технічні та інженерні ресурси.

Кадрові ресурси. Відповідно до організаційно-функціональної структури та статуту організації функції вищого керівництва організації виконують генеральний директор та рада директорів. Для формування політики інформаційної безпеки організації необхідно провести великий обсяг робіт, які потребують значних витрат людських ресурсів відповідної кваліфікації, а також матеріальних ресурсів. З цією метою вищим керівництвом створюється комісія з інформаційної безпеки, до якої входять:

- Директор з питань безпеки;
- Керівник служби безпеки бізнесу;
- Керівник служби інформаційної безпеки;
- Керівник юридичної служби;
- Технічний директор;

- Керівник аналітичного відділу;
- Керівник технологічного відділу;
- Керівник відділу кадрів.

До кадрових ресурсів також слід віднести провідних фахівців виробничих підрозділів, служби інформаційної безпеки, а також експертів, які залучаються до розробки політики безпеки організації.

Організаційні ресурси. До організаційних ресурсів відносяться внутрішні організаційно-розпорядчі документи:

- Контекст організації
- Статут організації
- Документи системи управління організацією
- Схема організаційно-штатної структури організації
- Положення про виробничі підрозділи та служби
- Положення про службу безпеки організації
- Посадові інструкції керівників та співробітників організації
- Положення про внутрішньо об'єктовий режим
- Положення про конфіденційність
- Та інші внутрішні документи організації.

До нормативно-правових ресурсів відносяться:

- Закони України
- Постанови Кабінету міністрів України
- Міжнародні стандарти
- Державні стандарти України
- Галузеві стандарти

Технічні та інженерні ресурси:

- Плани приміщень та території організації
- Схеми інженерних комунікацій

- Система управління доступом до об'єктів організації
- Схеми інформаційно комунікаційних мереж
- Технічні засоби інформаційно комунікаційних технологій
- Засоби управління інформаційно комунікаційних технологій
- Середовище розробки та тестування
- Програмні засоби та утиліти
- Системи управління базами даних
- Експлуатаційна документація ІКТ
- Засоби антивірусного захисту
- Засоби захисту мережі

## 2.2. Структурно-логічна схема роботи керівництва по забезпеченню політики інформаційної безпеки

Для дослідження особливостей роботи керівництва по управлінню забезпеченням політики інформаційної безпеки організації буде викладатися на прикладі організації, схема організаційно-функціональної структури якої, наведена на рис. 2.1.

Організаційно-функціональна структура становить сукупність вертикальних і горизонтальних зв'язків, що забезпечують упорядкованість, координацію та регулювання діяльності організації з досягнення її цілей. Основою такої структури є відносини ієрархічної співпідпорядкованості.

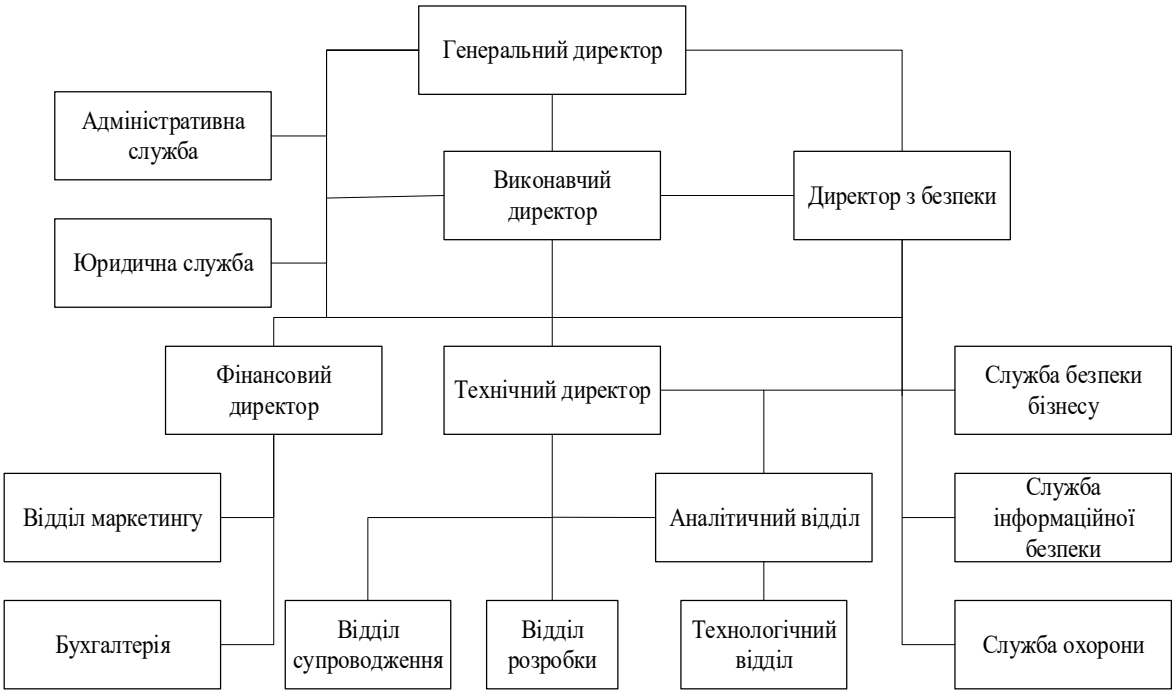


Рис. 2.1. Схема організаційно-функціональної структури організації

Одним із основних видів діяльності обраної структури організації є розробка, впровадження та супроводження програмного забезпечення в сфері автоматизації процесів управлінської та фінансово-економічної діяльності підприємств, що використовується у різних галузях виробництва.

Організаційна структура підприємства виглядає наступним чином:

Генеральний директор.

Директор з безпеки

- Служба безпеки бізнесу
- Служба інформаційної безпеки
- Служба охорони

Виконавчий директор

- Адміністративна служба
- Юридична служба
- Відділ кадрів

Технічний директор

- Аналітичний відділ
- Відділ розробки продуктів

- Технологічний відділ
- Відділ впровадження та супроводження

Фінансовий директор

- Відділ маркетингу
- Бухгалтерія

Особливості роботи керівництва по управлінню забезпеченням політики інформаційної безпеки кожної окремої організації великою мірою залежать від наступних факторів:

- контексту організації;
- вимоги зацікавлених сторін;
- вимоги міжнародних, державних галузевих чи корпоративних стандартів;
- функціонуючої системи управління організацією;
- організаційно-функціональної структури організації;
- категорії інформації, яка обробляється в організації;
- області дії політики безпеки організації;
- фази життєвого циклу Системи управління інформаційною безпекою організації;
- функціональних обов'язків персоналу.

Вище керівництво повинно продемонструвати дії з управління та зобов'язання по відношенню до системи управління інформаційною безпекою:

- гарантуванням, що політика інформаційної безпеки та цілі інформаційної безпеки розроблені та сумісні зі стратегічними планами організації;
- гарантуванням інтеграції вимог системи інформаційної безпеки в процеси організації;
- гарантуванням, що ресурси, потрібні для системи управління інформаційною безпекою, доступні;
- доведенням до відома організації важливості ефективного управління інформаційною безпекою та відповідності вимогам системи управління інформаційною безпекою;

- гарантуванням, що система управління інформаційною безпекою досягне своїх запланованих результатів;
- призначенням та підтримкою осіб для досягнення ефективності системи управління інформаційною безпекою;
- сприянням постійному вдосконаленню; та підтримкою інших пов’язаних ролей вищого керівництва, щоб продемонструвати їх керівну роль, яку вони застосовують у сферах їх відповідальності. [22]

Функції керівництва по управлінню забезпеченням політики інформаційної безпеки організації випливають із загальних вимог міжнародних стандартів та державних нормативних документів Системи технічного захисту інформації .

Зміст і набір функцій, здійснюваних в процесі управління, залежать від типу організації , від розмірів організації, від сфери її діяльності , від рівня в управлінській ієрархії від функціональної сфери.

Проте можна згрупувати всі види управлінської діяльності в п´ять основних функції:

1. ***Планування*** включає встановлення цілей, виділення ресурсів і розробку шляхів їх досягнення.
2. ***Організація*** включає визначення особливих дій, забезпечення ресурсами, а також ухвалення рішень про розподіл повноважень, обов'язків і відповідальності між підрозділами і посадовими особами.
3. ***Координація*** (керування і регулювання) включає повідомлення працівникам, в чому полягають їх обов'язки по виконанню плану компанії, з метою координації їх дій.
4. ***Мотивація*** включає забезпечення такого організаційного оточення, в якому працівники спонукаються виконувати свої обов'язки найкращим чином.
5. ***Контроль*** включає наглядову і регулюючу діяльність, націлену на забезпечення виконання завдань організації згідно з планами. [26]

Загальна структура управління інформаційною безпекою наведена на рис.2.2.

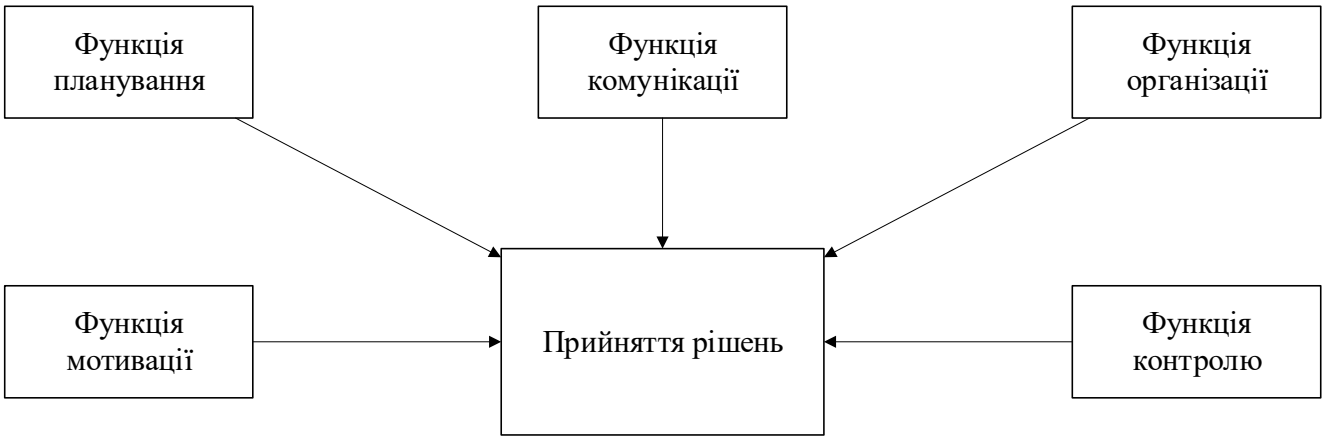


Рис. 2.2. Структура функцій в організації управління інформаційною безпекою при прийнятті рішень

Згідно до вимог ДСТУ ISO/IEC 27003 та, враховуючи структурно-функціональну схему організації, структурно-логічну схему роботи керівництва можна представити у вигляді, зображеному на рис. 2.3.

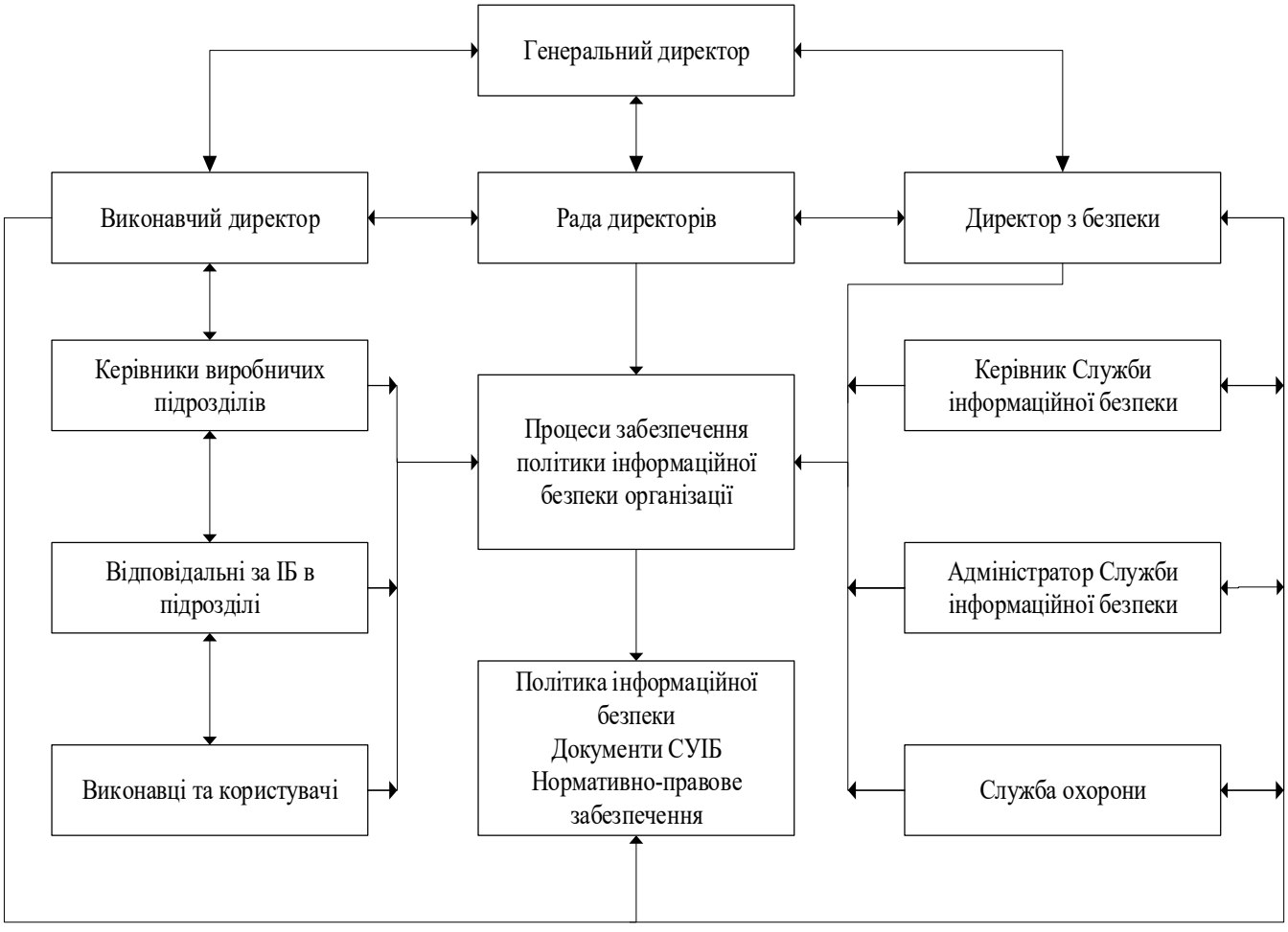


Рис. 2.3. Структурно-логічна схема роботи керівництва по забезпеченню політики інформаційної безпеки

Згідно до вимог ДСТУ ISO/IEC 27003 та, враховуючи контекст організації, дії керівництва по забезпеченню ІБ можна представити у вигляді, зображеному на табл. 2.2.

Таблиця 2.2

Дії керівництва по забезпеченню інформаційної безпеки

| Номер етапу | Завдання/Зміст робіт згідно ДСТУ ISO/IEC 27003 | Документування результатів | Дії керівництва |
|---|---|---|---|
| 1 | Підготувати наказ | Наказ про створення Комісії з інформаційної безпеки | Організація |
| 2 | Підготувати наказ про створення Служби інформаційної безпеки та призначення керівництва Служби | Наказ<br>Ознайомлення та прийняття повноважень | Організація, координація |
| 3 | Визначити цілі, потреби інформаційної безпеки та вимоги організації до СУІБ | Опис цілей, потреб ІБ та вимог організації СУІБ | Планування |
| 4 | Зібрати відповідні регулятивні стандарти, стандарти відповідності та галузеві стандарти, що застосовуються в організації | Опис стандартів<br>Перелік законодавчих, нормативних, організаційних, контрактних та інших вимог | Планування |
| 5 | Визначити попередню область дії СУІБ | Опис попередньої дії СУІБ<br>Визначення ролей та сфер відповідальності в області СУІБ | Планування, координація, затвердження документу |

Продовження табл. 2.2

Дії керівництва по забезпеченню інформаційної безпеки

| Номер етапу | Завдання/Зміст робіт згідно ДСТУ ISO/IEC 27003 | Документування результатів | Дії керівництва |
|---|---|---|---|
| 6 | Скласти план проекту для затвердження керівництвом | План проекту | Планування, затвердження документу |
| 7 | Отримати схвалення керівництва та доручення на запуск проекту створення СУІБ | Схвалення керівництвом запуску проекту створення СУІБ<br>Наказ про створення СУІБ | Організація, координація |
| 8 | Визначити межі організації | Опис меж організації<br>Функції та структура організації<br>Опис меж ІКТ<br>Опис фізичних меж СУІБ | Планування |
| 9 | Визначити межі та область дії СУІБ | Документ, що описує область дії та межі СУІБ<br>Положення про область дії СУІБ | Планування, організація, затвердження документу |
| 10 | Розробка Політики безпеки організації | Політика інформаційної безпеки<br>Політика управління інформаційною безпекою | Організація, координація, затвердження документу |

Продовження табл. 2.2

Дії керівництва по забезпеченню інформаційної безпеки

| Номер етапу | Завдання/Зміст робіт згідно ДСТУ ISO/IEC 27003 | Документування результатів | Дії керівництва |
|---|---|---|---|
| 11 | Визначення вимог до інформаційної безпеки | Список основних процесів, функцій, об’єктів інформаційних систем та комунікаційних мереж<br>Політика класифікації інформації<br>Положення про конфіденційність<br>Перелік відомих вразливостей в організації | Планування, затвердження документу |
| 12 | Визначення активів в рамках області дії СУІБ | Опис процесів управління активами<br>Політика управління активами<br>Реєстр інформаційних активів | Планування, затвердження документу |
| 13 | Запуск оцінки інформаційної безпеки | Документ з фактичного стану та оцінки інформаційної безпеки в організації, що включає також існуючі заходи та засоби контролю та управління інформаційною безпекою | Організація, затвердження документу |

Продовження табл. 2.2

Дії керівництва по забезпеченню інформаційної безпеки

| Номер етапу | Завдання/Зміст робіт згідно ДСТУ ISO/IEC 27003 | Документування результатів | Дії керівництва |
|---|---|---|---|
| 14 | Проведення оцінку ризиків | Затверджена методологія оцінки ризиків, поєднана з контекстом стратегічного менеджменту ризиками в організації | Планування, організація, затвердження документу |
| 15 | Отримання схвалення керівництва для впровадження СУІБ | Ризики та визначені для них варіанти оцінки<br>Обрані цілі, засоби та заходи контролю та управління зниженням ризиків | Мотивація, організація |
| 16 | Санкція керівництва на впровадження та використання СУІБ | Документована санкція керівництва на впровадження та використання СУІБ | Організація, координація, затвердження документу |
| 17 | Розробка документації СУІБ | Визначення документації, пов’язаною зі СУІБ<br>Структура організації, пов’язана з ролями та сферами відповідальності у сфері інформаційної безпеки<br>Методика управління документацією<br>Реєстр документів СУІБ | Організація, затвердження документу |

Продовження табл. 2.2

Дії керівництва по забезпеченню інформаційної безпеки

| Номер етапу | Завдання/Зміст робіт згідно ДСТУ ISO/IEC 27003 | Документування результатів | Дії керівництва |
|---|---|---|---|
| 18 | Розробка процесів впровадження СУІБ | Плани проектів впровадження для процесів обраних засобів управління ІБ, пов’язаних з інформаційною безпекою ІКТ та фізичних об’єктів | Планування, організація |
| 19 | Розробка процедур управління ІБ | Процедури, що описують процеси звітності та перевірки, що проводиться керівництвом<br>Положення про застосовність контролю<br>Методика внутрішнього аудиту | Планування, організація, затвердження документу |
| 20 | Кінцевий план проекту СУІБ | План проекту впровадження СУІБ організацією, що охоплює заплановане виконання дій з її ІБ, ІКТ та фізичних об’єктів, а також пов’язані з СУІБ вимоги з її впровадження, згідно до ДСТУ ISO/IEC 27003 | Планування, координація, мотивація |
| 21 | Впровадження системи управління інформаційною безпекою | Наказ про впровадження СУІБ | Організація, координація, контроль |

## 2.3. Міжнародний досвід впровадження політики інформаційної безпеки

На сьогоднішній день сформувалась краща практика політик інформаційної безпеки. Це, насамперед, практика розробки політик, процедур, стандартів та інструкцій з безпеки визнаних технологічних лідерів. В цьому підрозділі будуть досліджені практики таких компаній як IBM, Sun Microsystems, Cisco Systems, Microsoft.

Підхід компанії IBM. На думку фахівців компанії IBM, розробка корпоративних керівних документів в області інформаційної безпеки повинна починатись з створення політики інформаційної безпеки. Політика безпеки має вважатись складовою частини процесу управління інформаційними ризиками. Вважається, що розробка політики безпеки відноситься до стратегічних задач менеджменту компанії, що здатен адекватно оцінити вартість інформаційних активів компанії та прийняти обґрунтоване рішення щодо захисту інформації, приймаючи в увагу цілі та задачі бізнесу. [26]

Компанія IBM виділяє наступні етапи розробки політики безпеки:

- визначення інформаційних ризиків компанії, здатних завдати максимальної шкоди, для розробки в подальшому процедур і заходів щодо попередження їх виникнення;
- розробка політики безпеки, яка описує заходи захисту інформаційних активів, адекватні цілям і задачам бізнесу;
- прийняття планів дій в надзвичайних ситуаціях для зменшення шкоди у випадках, коли обрані заходи захисту не змогли запобігти інциденти в області безпеки;
- оцінка залишкових інформаційних ризиків і прийняття рішення про додаткові інвестиції в засоби і заходи безпеки. Рішення приймає керівництво на основі аналізу залишкових ризиків.

Політика безпеки компанії, з точки зору IBM, повинна містити явну відповідь на питання «Що потрібно захистити?». Дійсно, якщо керівництво компанії розуміє, що необхідно захистити, які інформаційні ризики і загрози інформаційних активів

компанії існують, тоді можна переходити до створення ефективної політики інформаційної безпеки.

Після створення корпоративної політики створюється серія стандартів. Під стандартами IBM розуміє документи, що описують порядок застосування корпоративної політики безпеки в термінах аутентифікації, авторизації, ідентифікації, контролю доступу і т. Д. Стандарти можуть вимагати частих змін, так як на них впливають поточні загрози і вразливості інформаційних технологій.

В компанії IBM політики і стандарти безпеки створюються для:

• розробки правил і норм безпеки рівня компанії;

• аналізу інформаційних ризиків і способів їх зменшення;

• формалізації способів захисту, які повинні бути реалізовані;

• визначення очікувань з боку компанії і співробітників;

• чіткого визначення процедур безпеки, яких потрібно дотримуватися;

• забезпечення юридичної підтримки в разі виникнення проблем в області безпеки.

Стандарти реалізуються за допомогою практик і / або процедур. Практики являються реалізацією стандартів в операційних системах, додатках та інформаційних системах. В них деталізуються сервіси, що встановлюються на операційних системах, порядок створення облікових записів і т. д. Процедури документують процеси запиту і підтвердження доступу до певних сервісів, наприклад VPN.

Підхід компанії Sun Microsystems. Sun вважає, що політика безпеки є необхідною для ефективної організації режиму інформаційної безпеки організації. Для них під політикою безпеки мається на увазі стратегічний документ, в якому очікування та вимоги керівництва компанії до організації ІБ виражаються у певних вимірних та контрольованих цілях і завданнях. При цьому, Sun рекомендує реалізовувати підхід «зверху-вниз», а тобто спочатку розробити політику безпеки, а вже потім приступати до побудови відповідної архітектури корпоративної системи захисту інформації. [26]

Рекомендована структура документів політики безпеки:

• опис основних цілей і завдань захисту інформації,

• визначення ставлення керівництва компанії до політики безпеки,

• обгрунтування шляхів реалізації політики безпеки,

• визначення ролей і обов'язків відповідальних за організацію режиму інформаційної безпеки в компанії,

• визначення необхідних правил і норм безпеки,

• визначення відповідальності за порушення політики,

• визначення порядку перегляду і контролю положень політики безпеки.

Компанія Sun рекомендує використовувати наступний шаблон політики безпеки:

• розділи: робиться короткий огляд основних розділів політики безпеки;

• заяву про призначення: чому потрібна політика безпеки;

• область дії: яка область дії політики безпеки;

• заяву політики: які специфічні особливості політики безпеки;

• обов'язки: хто і що повинен робити;

• аудиторія: на кого орієнтована політика безпеки;

• впровадження: хто відповідає за впровадження політики безпеки; хто відповідає за порушення політики безпеки;

• виключення: опис можливих винятків;

• інші угоди: опис додаткових угод;

• доведення: хто відповідає за доведення політики безпеки до співробітників; який процес доведення;

• процес перегляду та поновлення: хто відповідає за перегляд і оновлення політики безпеки; що являє собою процес перегляду; з яких причин це відбувається; періодичність перегляду політики безпеки (наприклад, щорічно або при виникненні проблеми);

• здійснення політики: хто відповідає за здійснення політики безпеки; як це виконується;

• моніторинг відповідності: як виконується моніторинг відповідності політики безпеки вимогам бізнесу.

Підхід компанії Cisco. З точки зору фахівців Cisco, відсутність мережевої політики безпеки може призвести до серйозних інцидентів в області безпеки. Розробку політики безпеки компанії рекомендується починати з оцінки ризиків мережі і створення робочої групи з реагування на інциденти.

Компанія Cisco рекомендує створити політики використання, які описують ролі і обов'язки співробітників компанії для належного захисту конфіденційної інформації. При цьому можна почати з розробки головною політики безпеки, в якій чітко прописати спільні цілі і завдання організації режиму інформаційної безпеки компанії.

Наступний крок - створення політики допустимого використання для партнерів, щоб проінформувати партнерів компанії про те, яка інформація їм доступна. Слід чітко описати будь-які дії, які будуть сприйматися як ворожі, а також можливі способи реагування при виявленні таких дій.

З урахуваннях попередніх політик необхідно створити політику допустимого використання для адміністраторів, щоб описати процедури адміністрування облікових записів співробітників і перевірки привілеїв. При цьому якщо компанія має певну політику щодо використання паролів або категорирования інформації, то потрібно її тут згадати. Далі необхідно перевірити названі політики на несуперечливість і повноту, а також переконатися в тому, що сформульовані вимоги до адміністраторів знайшли своє відображення в планах з навчання. [26]

Проведення аналізу ризиків. Призначення аналізу ризиків полягає в катеригозації інформаційних активів компанії, визначити найбільш значущі загрози і вразливості активів і обґрунтовано вибрати відповідні контрзаходи безпеки. Мається на увазі, що це дозволить знайти і підтримувати прийнятний баланс між безпекою та необхідним рівнем доступу до мережі. Розрізняють такі рівні інформаційних ризиків:

• низький рівень - інформаційні системи і дані, які, будучи скомпрометовані (доступні для вивчення неавторизованими особами, пошкоджені або загублені), не приведуть до серйозного збитку, фінансовим проблемам або до проблем з правоохоронними органами;

• середній рівень - інформаційні системи і дані, які, будучи скомпрометовані (доступні для вивчення неавторизованими особами, пошкоджені або загублені), приведуть до помірного збитку або до невеликих проблем з правоохоронними органами, або до помірних фінансових проблем, а також до отримання подальшого доступу до інших систем. Порушені системи і інформація вимагають помірних зусиль по відновленню;

• високий рівень - інформаційні системи і дані, які, будучи скомпрометовані (доступні для вивчення неавторизованими особами, пошкоджені або загублені), приведуть до значного збитку або до серйозних проблем з правоохоронними органами, або до фінансових проблем, нанесення шкоди здоров'ю та безпеці співробітників. Системи і інформація вимагають істотних зусиль по відновленню.

Після визначення рівнів ризику необхідно визначити ролі користувачів в цих системах. Рекомендується виділяти наступні п'ять найбільш загальних типів користувачів:

• адміністратори - внутрішні користувачі, що відповідають за мережеві ресурси;

• привілейовані користувачі - внутрішні користувачі з необхідністю більшого рівня доступу;

• рядові користувачі - внутрішні користувачі зі звичайним рівнем доступу;

• партнери - зовнішні користувачі з необхідністю доступу до деяких ресурсів;

• інші - зовнішні користувачі або клієнти.

Cisco рекомендує створити групу мережевої безпеки під керівництвом менеджеру з безпеки, що буде включати представників кожної з значимої бізнес-одиниці компанії. Члени групи повинні добре знати політики безпеки організації та технічні аспекти мереж та систем, що підлягають захисту. Часто це потребує додаткового навчання працівників вищеназваної групи. Група безпеки повинна брати участь у розробці політики безпеки, організації режиму інформаційної безпеки, а також своєчасно реагувати на інциденти інформаційної безпеки компанії.

Процес супроводу політики безпеки заключається в контролі, та, при необхідності, перегляді політик безпеки організації. Необхідно як мінімум щорічний перегляд політик безпеки та проведення аналізу ризиків. [26]

Підхід компанії Microsoft. Компанія Microsoft розробила стратегію безпеки, яка складається з чотирьох основних компонентів:

- Цілі корпоративної безпеки
- Принципи операційної безпеки
- Модель прийняття рішень, заснована на аналізі ризиків
- Визначення пріоритетності дій по зменшенню ризиків

Фундаментом для дизайну, розробки та нормального функціонування захищених систем є принципи безпеки, розділені на кілька категорій (див. табл. 2.3).

Таблиця 2.3

Принципи безпеки захищених систем

| Категорія | Принцип безпеки |
|---|---|
| Організаційна: направлена на отримання підтримки керівництва з управління ризиками та ознайомлення з питаннями інформаційної безпеки | Управління ризиками згідно до задач бізнесу<br>Визначення ролей та обов'язків<br>Інвестиції у дизайн захищеності<br>Забезпечення безпеки операцій |
| Користувачі та дані: включає в себе аутентифікацію, захист даних користувачів та авторизацію | Управління принципом найменших привілеїв<br>Класифікація даних та їх використання<br>Впровадження захисту даних та ідентичності користувача<br>Захист інформації<br>Гарантія цілісності даних<br>Моніторинг гарантії ідентичності<br>Доступність |

Продовження табл. 2.3

Принципи безпеки захищених систем

| Категорія | Принцип безпеки |
|---|---|
| Розробка додатків та систем: включає в себе дизайн та розробку захищених систем | Інтеграція захисту інформації в життєвий цикл<br>Дизайн багаторівневого захисту<br>Зменшення поверхні атаки<br>Збереження простоти використання |
| Операції та супровід: об’єднання людей, процесів та технологій для побудови, підтримки та використання захищених систем | План підтримки системи<br>Інтеграція захищених конфігурацій<br>Моніторинг та реєстрація подій<br>Практика реагування на інциденти ІБ<br>Перевірка процедур відновлення у випадку аварії |

Для забезпечення інформаційної безпеки Microsoft використовує підхід з управління інформаційними ризиками. Під управлінням ризиками тут розуміється процес визначення, оцінки та зменшення ризиків на постійній основі. Управління ризиками безпеки дозволяє знайти розумний баланс між вартістю засобів і заходів захисту і вимогами бізнесу. Модель управління ризиками Microsoft представляє собою комбінацію різних підходів, таких, як кількісний аналіз ризиків, аналіз повернення інвестицій в безпеку, якісний аналіз ризиків, а також підходи кращих практик.

Інвестування в процес управління ризиками - з цільної структурою і визначеними ролями і обов'язками - готує організацію до визначення пріоритетів, планування зменшення загрози і переходу до парирування або нейтралізації наступної загрози або уразливості. Для найкращого управління ризиками Microsoft слідує традиційному підходу до управлінням ризиками, що складається з чотирьох етапів:

• оцінка інформаційних ризиків - виконання методології оцінки ризику для визначення його величини;

• розробка політики безпеки - розробка політики безпеки по зменшенню, ухиленню і попередженню ризиків;

• впровадження засобів захисту - об'єднання співробітників, процесів і технологій для зменшення ризиків, пов'язаних з аналізом співвідношення «ціна - якість»;

• аудит безпеки і вимір поточної захищеності - моніторинг, аудит безпеки і вимір захищеності інформаційних систем компанії.

Для розробки цілей безпеки створюється комітет з інформаційної безпеки. Комітет складається із співробітників з досвідом роботи в галузі безпеки, технічних співробітників і представників інших підрозділів під керівництвом офіцера з безпеки. Комітет вирішує наступні завдання:

• Розробка та управління життєвим циклом політики безпеки;

• створення процесів, що забезпечують досягнення цілей безпеки;

• створення процесів і планів по реалізації стандартів, описаних в політиці;

• допомога в організації програм ознайомлення з питаннями безпеки;

• консультування персоналу з питань безпеки;

• визначення бюджету і необхідних ресурсів для забезпечення безпеки.

## 2.4. Використання програмного забезпечення для перевірки політики інформаційної безпеки на відповідність вимогам нормативних документів

Для дослідження програмного забезпечення, в цьому розділі будуть розглянуті такі інструменти, як: Microsoft Security Assesment Tool, McAfee ePolicy Orchestrator, Jupiter One та IBM Tivoli.

Таблиця 2.4

Програмне забезпечення для перевірки політики інформаційної безпеки

| Найменування ПЗ | Призначення |
|---|---|
| Microsoft Security Assessment Tool | Засіб оцінки ризиків, що надає інформацію про систему безпеки IT-інфраструктури та рекомендації щодо її поліпшення, засновані на передовому досвіді. |
| McAfee ePolicy Orchestrator | Забезпечує централізоване управління політиками і їх примусове застосування для кінцевих точок і корпоративних продуктів безпеки. |
| Jupiter One | Конструкція та перевірка політик безпеки організації. Детальне налаштування політики безпеки, процедур та засобів контролю. |
| IBM Tivoli | Централізоване управління та застосування політики безпеки для ресурсів веб-служб, посилення контролю доступу для програм та служб. |

Microsoft Security Assesment Tool. Інструмент оцінки безпеки Microsoft Security Assessment Tool (MSAT) призначений для допомоги організаціям в оцінки вразливостей IT-середовища. Він дозволяє надати список розставлених по пріоритетам проблем і список рекомендацій щодо мінімізації цих загроз, а потім регулярно перевіряти здатність інфраструктури відповідати на ці загрози.

MSAT застосовує цілісний підхід до вимірювання рівня безпеки і охоплює такі теми, як персонал, процеси і технології. Основні можливості MSAT.

1. Надає зрозумілу, вичерпну і постійну поінформованість про рівень безпеки.

2. Описує інфраструктуру ешелонованого захисту, відповідну галузевим стандартам.

3. Надає докладні, постійні звіти, які порівнюють базові показники з досягнутими успіхами.

4. Описує перевірені рекомендації і розставлені по пріоритетах дії щодо поліпшення безпеки.

5. Надає структуровані рекомендації від компанії Microsoft в залежності від галузевої приналежності.

Опитувальник MSAT складається з понад 200 питань, що охоплюють інфраструктуру, додатки, операції і персонал. Питання, пов'язані з ними відповіді і рекомендації виводяться із загальноприйнятих практичних рекомендацій, стандартів, таких як ISO 27000 та NIST-800.x, а також рекомендацій та приписів від групи надійних обчислень Microsoft та інших зовнішніх джерел з безпеки.

MSAT вимірює рівень безпеки організації. Під рівнем безпеки на увазі мається розвиток високоефективних і стабільних методик забезпечення безпеки. При низькому значенні використовується обмежене число методів захисту, а заходи приймаються постфактум. При високому значенні практикуються усталені і перевірені процеси, які дозволяють компанії робити попереджувальні заходи і, при необхідності, реагувати ще ефективніше і більш злагоджено.

MSAT призначена для широкого охоплення областей потенційного ризику в середовищі, а не для надання глибокого аналізу конкретних технологій або процесів. Тому, засіб не може оцінювати ефективність застосованих заходів безпеки. Його слід використовувати як попереднє керівництво, що допомагає в розробці базових показників для концентрації на конкретних областях, що вимагають більш пильної уваги. MSAT можна запускати регулярно.

Його слід використовувати як попереднє керівництво, що допомагає в розробці базових показників для концентрації на конкретних областях, що вимагають більш пильної уваги. MSAT можна запускати регулярно.

MSAT пропонує перевірку політики безпеки відповідно нормативним документам організації як критерій оцінки загроз безпеці. Політика безпеки визначається як колекція окремих політик і рекомендацій, існуючих для управління безпечним і правильним використанням технології і процесів всередині організації. Ця область охоплює політики, що стосуються всіх типів безпеки, таких як безпека користувача, системи і даних. [28]

McAfee ePolicy Orchestrator**.** McAfee ePO дозволяє збирати критично важливу інформацію про те, що відбувається, встановлювати політики і автоматизувати процес примусового застосування політик для забезпечення належного рівня безпеки в масштабі всієї організації. ПЗ полегшує для адміністраторів ІБ організації роботу по підтримці політик ІБ. Крім того, воно дозволяє задіяти сторонні дані про погрози, використовуючи для цього рівень обміну даними Data Exchange Layer (DXL).

Крім зазначених функцій, консоль забезпечує двосторонню інтеграцію політик з різними іншими продуктами. McAfee ePO впорядковує політики по продуктам, а потім за категоріями для кожного продукту. Така оптимізація операцій дозволяє скоротити непродуктивні витрати, пов'язані з обробкою інформації і обміном даними, і підвищити швидкість і точність реагування. [29]

Jupiter One. Jupiter One – ПЗ, призначене для конструкції та перевірки політик безпеки організації. За його допомогою можна детально налаштовувати політики безпеки, процедури та засоби контролю. ПЗ працює таким чином: він ставить питання, що стосуються організації та, після відповіді на них, створює шаблон, який можна коригувати відповідно до нормативних документів організації. Це означає, що найновіша версія політики може розміщуватись в одному централізованому місці, на яке організація може посилатися.

Jupiter One довзволяє візуалізувати та оновлювати взаємозв’язки створених політик безпеки з іншими елементами інформаційної системи. Модель взаємозв'язку, яка пов'язує активи у інтерфейсі програми з політиками та процедурами, необхідними для дотримання вимог системи безпеки, дозволяє

здійснити оцінку політик, що включає автоматично згенерований звіт, що висвітлює статус прийняття політик та процедур. [30]

IBM Tivoli. Менеджер політики безпеки IBM Tivoli покращує відповідність і керує оперативним управлінням у всієї організації, дозволяючи архітекторам та командам операційних служб централізовано керувати та застосовувати політики безпеки для ресурсів веб-служб у багатьох точках забезпечення політики.

Tivoli Security Policy Manager - це засноване на стандартах ПЗ з інформаційної безпеки, що забезпечує централізоване управління правами додатків, управління політикою безпеки та безпеку служб виконання для посилення контролю доступу до програм та служб. Tivoli Security Policy Manager дозволяє корпоративним архітекторам та командам операційних служб централізовано керувати та застосовувати політики безпеки для ресурсів веб-служб у кількох точках забезпечення політики.

Адміністрування політики стосується управління життєвим циклом політики, створення, зміна, підтримка та видалення політик. В рамках цього життєвого циклу політика вдосконалюється до специфічних для сервісів послуг, таких як показники ефективності, політика довіри тощо. Ці політики, в свою чергу, забезпечуються інфраструктурою, коли вони налаштовані як вимоги, яким повинна відповідати інфраструктура.

Ключовим є відстеження політик від бізнес-вимог високого рівня до примусових конфігурацій та політики виконання, перш за все для відстеження мети політики та основи поведінки під час виконання. Ця здатність може допомогти відстежувати відповідальність за зміни політики та керувати нею. Tivoli дозволяє відстежувати застосовану та минули політики, а також оцінювати відповідність політики нижчого рівня корпоративній політиці.

Ця відстежуваність, контроль версій та перевірка відповідності є ключовими частинами загального рішення щодо управління інформаційною безпекою. Розгортаючи програму, ви адмініструєте політику, пов’язану з програмою, щоб відображати будь-які зміни, які можуть відбутися протягом усього терміну дії програми.

Зміни в політиках безпеки включають зміни політики авторизації (наприклад, додавання нових ролей, які можуть отримати доступ до ресурсів, або призначення ролей новим групам або користувачам), зміни управління користувачами (наприклад, користувачі, призначені додатковим групам користувачів), або інші зміни, включаючи аудит вимоги та обмеження, такі як цілісність або конфіденційність.

В основі інфраструктури управління політикою лежить здатність формально формулювати політику.

Політика може бути сформульована з точки зору метаданих про послуги, особисті дані чи іншу контекстну інформацію, таку як надійність аутентифікації, час доби тощо. Тому формулювання та управління метаданими є дуже важливим.

Метадані можуть стосуватися вмісту цільової інформації, конфігурації та топології цих систем або додатків, що дозволяють отримати доступ до даних. Наприклад, метадані можуть містити рівні класифікації даних, чутливість даних, значення в разі втрати, конфігурацію системи та топології тощо. Метадані також можуть бути доступними через реєстри служб та сховища.

Політику безпеки, яку створюють, потрібно розподілити між виконуючими підрозділами та керівництвом в межах інфраструктури. Політика визначається централізовано і поширюється до місця виконання в форматі, передбаченому організацією. Також розповсюджується обов’язкова інформація щодо дотримання політики відповідним чином. [31]

## Висновки до другого розділу

В другому розділі були проаналізовані основні дії керівництва по управлінню забезпеченням політики інформаційної безпеки організації. Визначені основі функції, на яких мають базуватися дії керівництва по забезпеченню політики інформаційної безпеки.

Визначені та описані ресурси, що задіяні до розробки політики інформаційної безпеки

Розроблена організаційно-функціональна схема організації, яка в подальшому буде використовуватись для дослідження процесів розробки та впровадження політики інформаційної безпеки організації.

На основі аналізу розроблена структурно-логічна схема алгоритму дій керівництва по забезпеченню інформаційної безпеки організації.

Проведено аналіз дій керівництва згідно до ДСТУ ISO/IEC 27003.

Досліджені та проаналізовані практики розробки та впровадження політики інформаційної безпеки провідних міжнародних організацій, таких як: Sun Microsystems, Microsoft, Cisco, IBM.

Проведений аналіз сучасного програмного забезпечення для розробки, формування, впровадження та перевірки політики інформаційної безпеки згідно до нормативних документів.

# РОЗДІЛ 3
# ДОСЛІДЖЕННЯ ПРОЦЕСІВ РОЗРОБКИ ТА ВПРОВАДЖЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Дослідження процесів розробки та впровадження політики інформаційної безпеки в організації буде проведено для організації, організаційно-функціональна структура якої, була визначена в розділі 2.2.

Контекст організації полягає у її діяльності - розробка, впровадження та супроводження програмного забезпечення в сфері автоматизації процесів управлінської та фінансово-економічної діяльності підприємств, що використовується у різних галузях виробництва; взаємодії з користувачами продуктів компанії; наявності власної інформаційно-комунікаційної системи.

Аналіз дій керівництва організації в процесах розробки політики інформаційної безпеки організації, визначення області дії політики безпеки та меж системи управління інформаційною безпекою були проведені в розділі 2.

Дослідження дій керівництва в процесах впровадження політики інформаційної безпеки організації буде проведений шляхом аналізу документації системи управління інформаційною безпекою, склад якої наведено у документі «Реєстр документів СУІБ» у табл. 3.1.

Таблиця 3.1

Реєстр документів СУІБ

| № п/п | Шифр розділу/ документу | Найменування документу | Відповідальний за документ | Місце зберігання |
|---|---|---|---|---|
| | **ДСУІБ 01.** | **Політики інформаційної безпеки** | | |
| | ДСУІБ 01.01. | Політика інформаційної безпеки | | |
| | ДСУІБ 01.02. | Політика менеджменту інформаційної безпеки | | |
| | ДСУІБ 01.03. | Положення про область дії СУІБ | | |

Продовження табл. 3.1

Реєстр документів СУІБ

| | | | | |
|---|---|---|---|---|
| | **ДСУІБ 02.** | **Організація системи інформаційної безпеки** | | |
| | ДСУІБ 02.01. | Наказ про створення СУІБ | | |
| | ДСУІБ 02.02. | Наказ про призначення вповноваженого з інформаційної безпеки | | |
| | ДСУІБ 02.03. | Положення про службу інформаційної безпеки | | |
| | ДСУІБ 02.04. | Наказ про введення СУІБ | | |
| | ДСУІБ 02.05. | План введення СУІБ | | |
| | ДСУІБ 02.06. | Розподіл відповідальності з інформаційної безпеки | | |
| | ДСУІБ 02.07. | Наказ про призначення відповідальних за устаткування | | |
| | ДСУІБ 02.08. | Положення про конфіденційність | | |
| | ДСУІБ 02.09. | Інструкція з інформаційної безпеки | | |
| | ДСУІБ 02.10. | Процедура ідентифікації вимог | | |
| | **ДСУІБ 03.** | **Управління документацією СУІБ** | | |
| | ДСУІБ 03.01. | Методика управління документацією | | |
| | ДСУІБ 03.02. | Реєстр документів СУІБ | | |
| | **ДСУІБ 04.** | **Управління персоналом** | | |
| | ДСУІБ 04.01. | Процес управління персоналом | | |
| | ДСУІБ 04.02. | Організаційно-функціональна структура організації | | |

Продовження табл. 3.1

Реєстр документів СУІБ

| | | | | |
|---|---|---|---|---|
| | ДСУІБ 04.03. | План навчання та підвищення освіченості | | |
| | ДСУІБ 04.04. | Інструкція користувачу з інформаційної безпеки | | |
| | ДСУІБ 04.05. | Процедура прийому на роботу | | |
| | **ДСУІБ 05.** | **Управління активами** | | |
| | ДСУІБ 05.01. | Методика управління активами | | |
| | ДСУІБ 05.02. | Реєстр інформаційних активів | | |
| | ДСУІБ 05.03. | Реєстр програмно згенерованих записів (логів) | | |
| | ДСУІБ 05.04. | Схема мережі | | |
| | **ДСУІБ 06.** | **Менеджмент ризиків інформаційної безпеки** | | |
| | ДСУІБ 06.01. | Методика управління ризиками інформаційної безпеки | | |
| | ДСУІБ 06.02. | План обробки ризиків | | |
| | ДСУІБ 06.03. | Управління вразливостями | | |
| | **ДСУІБ 07.** | **Фізична безпека** | | |
| | ДСУІБ 07.01. | Політика фізичної безпеки | | |
| | ДСУІБ 07.02. | Робочі інструкції з фізичної безпеки | | |
| | **ДСУІБ 08.** | **Операційний менеджмент** | | |
| | ДСУІБ 08.01. | Положення про використання ПЗ | | |
| | ДСУІБ 08.02. | Процедура управління змінами | | |

Продовження табл. 3.1

Реєстр документів СУІБ

| | | | | |
|---|---|---|---|---|
| | ДСУІБ 08.03. | Процедура тестування та розробки операцій | | |
| | ДСУІБ 08.05. | Положення про систему резервного копіювання | | |
| | ДСУІБ 08.06. | Інструкція з антивірусного захисту | | |
| | ДСУІБ 08.07 | Інструкція адміністратора безпеки з антивірусного захисту | | |
| | **ДСУІБ 09.** | **Управління доступом** | | |
| | ДСУІБ 09.01. | Політика управління доступом | | |
| | ДСУІБ 09.02. | Процедура надання та зміни прав доступу | | |
| | ДСУІБ 09.03. | Процедури контролю доступу (моніторинг) | | |
| | **ДСУІБ 10.** | **Управління інцидентами** | | |
| | ДСУІБ 10.01. | Процедура управління інцидентами | | |
| | ДСУІБ 10.02. | Інструкція реагування на інциденти | | |
| | ДСУІБ 10.03. | Записи по інцидентам | | |
| | ДСУІБ 10.04. | Звіти по інцидентам ІБ | | |
| | **ДСУІБ 11.** | **Управління аудитом** | | |
| | ДСУІБ 11.01. | Методика внутрішнього аудиту | | |
| | ДСУІБ 11.02. | Програма внутрішнього аудиту | | |
| | ДСУІБ 11.03. | Звіт (протокол) про проведення внутрішнього аудиту | | |

Продовження табл. 3.1

Реєстр документів СУІБ

| | | | | |
|---|---|---|---|---|
| | ДСУІБ 11.04. | Розклад внутрішніх аудитів | | |
| | **ДСУІБ 12.** | **Відповідність вимогам** | | |
| | ДСУІБ 12.01. | План підготовки до сертифікації СУІБ | | |

Для аналізу алгоритму дій керівництва в процесах розробки та впровадження політики інформаційної безпеки організації в даному розділі обрано групу процесів, реалізація яких значною мірою пов'язана з безпосередньою та опосередкованою участю керівництва організації: процеси управління активами організації та процеси управління документацією СУІБ.

## 3.1. Аналіз алгоритму дій керівництва в процесах розробки та впровадження політики інформаційної безпеки в організації (на прикладі)

Управління інформаційною безпекою в організації реалізується шляхом поєднання заходів організаційного та програмно-технічного рівнів. Організаційні заходи складаються із заходів адміністративного рівня і процедурних заходів захисту інформації. Основою заходів адміністративного рівня, тобто заходів, що вживаються керівництвом підприємства, є політика інформаційної безпеки.

Аналіз загальних дій керівництва в процесах розробки та впровадження політики інформаційної безпеки будуть досліджені на основі вимог і положень політики безпеки вищого рівня, прийнятими в організації. Політика інформаційної безпеки визначається взаємопов'язаними документами: «Політика інформаційної безпеки», «Політика управління інформаційною безпекою» та доповнюється «Положенням про область дії СУІБ».

Структура та зміст «Політики інформаційної безпеки» наведені у таблиці 3.2.

Таблиця 3.2

Структура та зміст документу «Політика інформаційної безпеки»

| Номер | Розділ |
|---|---|
| 1 | **Мета** |
| 2 | **Сфера застосування** |
| 3 | **Визначення та умовні позначення** |
| 4 | **Загальні положення** |
| 5 | **Стратегія, цілі та способи забезпечення інформаційної безпеки** |
| 5.1 | Основні фактори, що впливають на інформаційну безпеку |
| 5.2 | Функціональні показники захищеності інформації |
| 5.3 | Область дії політики інформаційної безпеки |
| 6 | **Загальна характеристика інформаційної системи** |
| 6.1 | Опис об’єктів захисту |
| 6.2 | Призначення та основні функції інформаційної системи |
| 6.3 | Функціональні підсистеми інформаційної системи |
| 6.4 | Класифікація користувачів системи |
| 6.5 | Організаційна структура |
| 7 | **Види інформаційних ресурсів системи** |
| 8 | **Структура інформаційних потоків** |
| 8.1 | Внутрішні інформаційні потоки |
| 8.2 | Зовнішні інформаційні потоки |
| 8.3 | Взаємодії з іншими системами |
| 9 | **Модель загроз інформаційної безпеки** |
| 9.1 | Об’єкти захисту |

Продовження табл. 3.2

Структура та зміст документу «Політика інформаційної безпеки»

| Номер | Розділ |
|---|---|
| 9.2 | Основні види загроз |
| 9.3 | Джерела загроз |
| 9.4 | Шляхи реалізації загроз |
| 9.5 | Вразливості та методи для оцінки вразливостей |
| 9.6 | Неформальна модель порушників |
| 9.7 | Типи порушників інформаційної безпеки |
| 10 | **Засоби забезпечення інформаційної безпеки** |
| 10.1 | Засоби забезпечення інформаційної безпеки організаційного рівня |
| 10.2 | Засоби забезпечення інформаційної безпеки процедурного рівня |
| 10.3 | Програмно-технічні засоби забезпечення інформаційної безпеки |
| 10.4 | Безпечне використання технічних засобів інформатизації |
| 10.5 | Аудит та реагування на загрози безпеці |
| 10.6 | Оцінка ефективності системи забезпечення інформаційної безпеки |
| 11 | **Порядок затвердження та внесення змін** |

В результаті аналізу процесів розробки політики безпеки організації була сформована схема алгоритму розробки політики інформаційної безпеки, зображена на рис. 3.1.

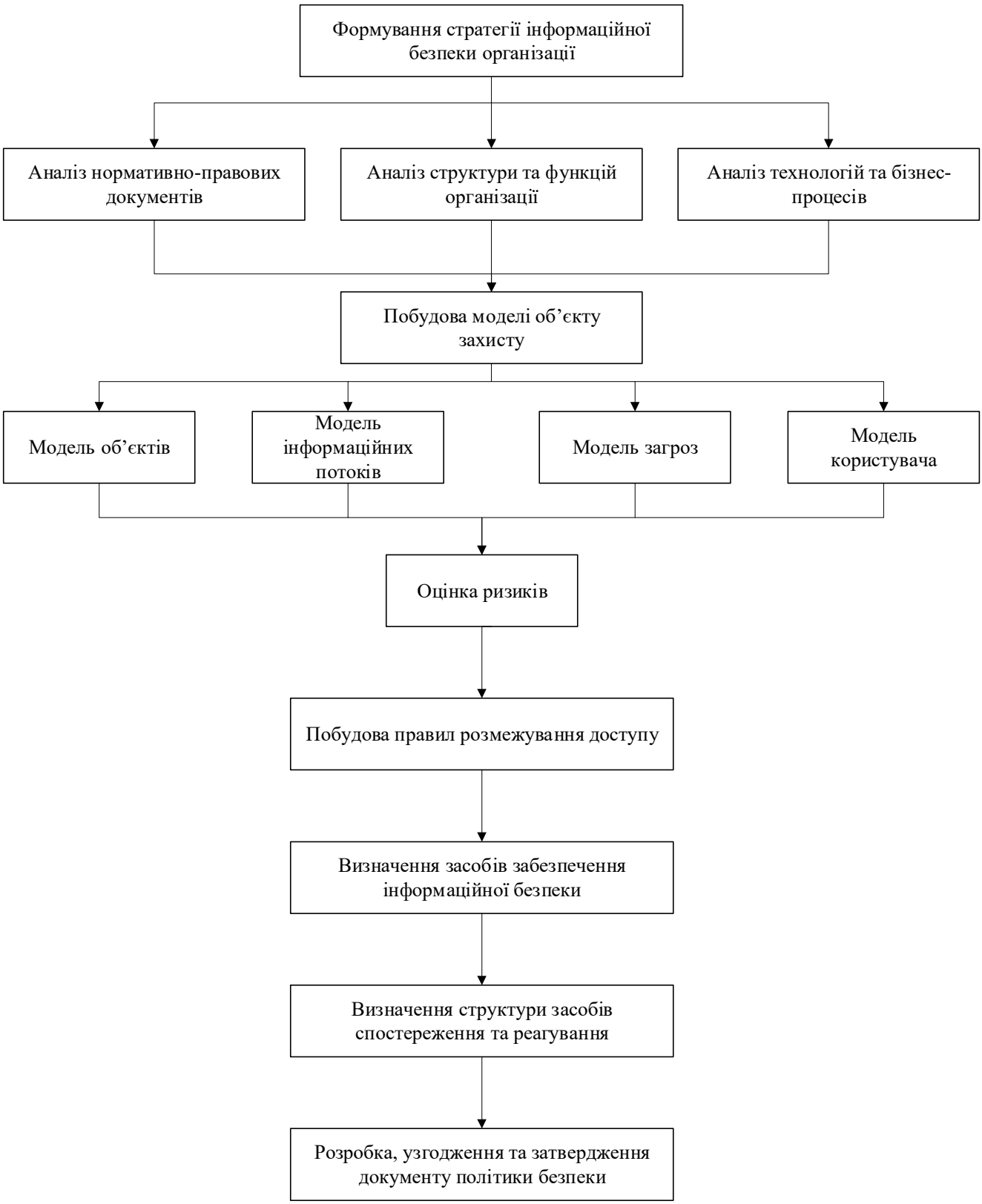


Рис. 3.1. Схема алгоритму розробки політики інформаційної безпеки

Структура та зміст «Політика управління інформаційною безпекою» наведена у таблиці 3.3.

Таблиця 3.3

Структура та зміст документу «Політика управління інформаційною безпекою»

| Номер | Зміст розділу |
|---|---|
| 1 | **Мета** |
| 2 | **Сфера застосування** |
| 3 | **Визначення та умовні позначення** |
| 4 | **Загальні положення** |
| 4.1 | Призначення та правова основа документу |
| 4.2 | Область дії політики |
| 5 | **Задачі управління інформаційною безпекою** |
| 5.1 | Інтереси суб’єктів інформаційних відносин |
| 5.2 | Цілі управління інформаційною безпекою |
| 5.3 | Напрямок забезпечення інформаційної безпеки |
| 5.4 | Задачі управління інформаційною безпекою |
| 5.5 | Основні шляхи вирішення задач системи захисту |
| 5.6 | Принципи забезпечення інформаційної безпеки |
| 5.7 | Організація системи забезпечення інформаційної безпеки |
| 6 | **Об’єкти захисту** |
| 6.1 | Категорії інформаційних ресурсів, що підлягають захисту |
| 6.2 | Політика класифікації ресурсів |
| 7 | **Основні загрози безпеки інформації** |
| 8 | **Управління ризиками інформаційної безпеки** |
| 9 | **Засоби забезпечення інформаційної безпеки** |
| 9.1 | Законодавчі (правові) засоби захисту |
| 9.2 | Морально-етичні засоби захисту |

Продовження табл. 3.3

Структура та зміст документу «Політика управління інформаційною безпекою»

| | |
|---|---|
| 9.3 | Технологічні засоби захисту |
| 9.4 | Організаційні (адміністративні) засоби захисту |
| 9.5 | Фізичні та технічні засоби |
| 10 | **Управління засобами забезпечення інформаційної безпеки** |
| 10.1 | Фізичні засоби захисту |
| 10.2 | Технічні засоби захисту |
| 10.3 | Засоби ідентифікації та аутентифікації користувачів |
| 10.4 | Засоби розмежування доступу |
| 10.5 | Засоби забезпечення та контролю цілісності |
| 10.6 | Засоби оперативного контролю та реєстрації подій безпеки |
| 10.7 | Криптографічні засоби захисту інформації |
| 11 | **Організація робіт щодо захисту інформації** |
| 12 | **Розподілення відповідальності та порядок взаємодії** |
| 13 | **Управління доступом до ресурсів організації** |
| 13.1 | Регламентація доступу до приміщення |
| 13.2 | Регламентація допуску працівників до використання інформаційних ресурсів |
| 13.3 | Регламентація процесів обслуговування та здійснення модифікації апаратних та програмних ресурсів |
| 13.4 | Забезпечення та контроль фізичної цілісності (незмінності конфігурації) апаратних та програмних ресурсів |
| 14 | **Політика управління персоналом** |
| 14.1 | Підбір та підготовка персоналу, навчання користувачів |
| 14.2 | Служба інформаційної безпеки організації |

Продовження табл. 3.3

Структура та зміст документу «Політика управління інформаційною безпекою»

| | |
|---|---|
| 14.3 | Відповідальність за порушення установленого порядку використання інформаційними ресурсами. Розслідування порушень |
| 15 | **Управління системою забезпечення інформаційної безпеки** |
| 16 | **Контроль ефективності системи захисту** |
| 16.1 | Контроль з боку керівництва |
| 16.2 | Оперативний контроль захищеності інформаційних ресурсів |
| 16.3 | Управління внутрішнім аудитом |
| 17 | **Порядок затвердження та внесення змін до документу** |

В результаті аналізу процесів забезпечення політики безпеки організації була сформована схема алгоритму впровадження політики інформаційної безпеки, зображена на рис. 3.2.

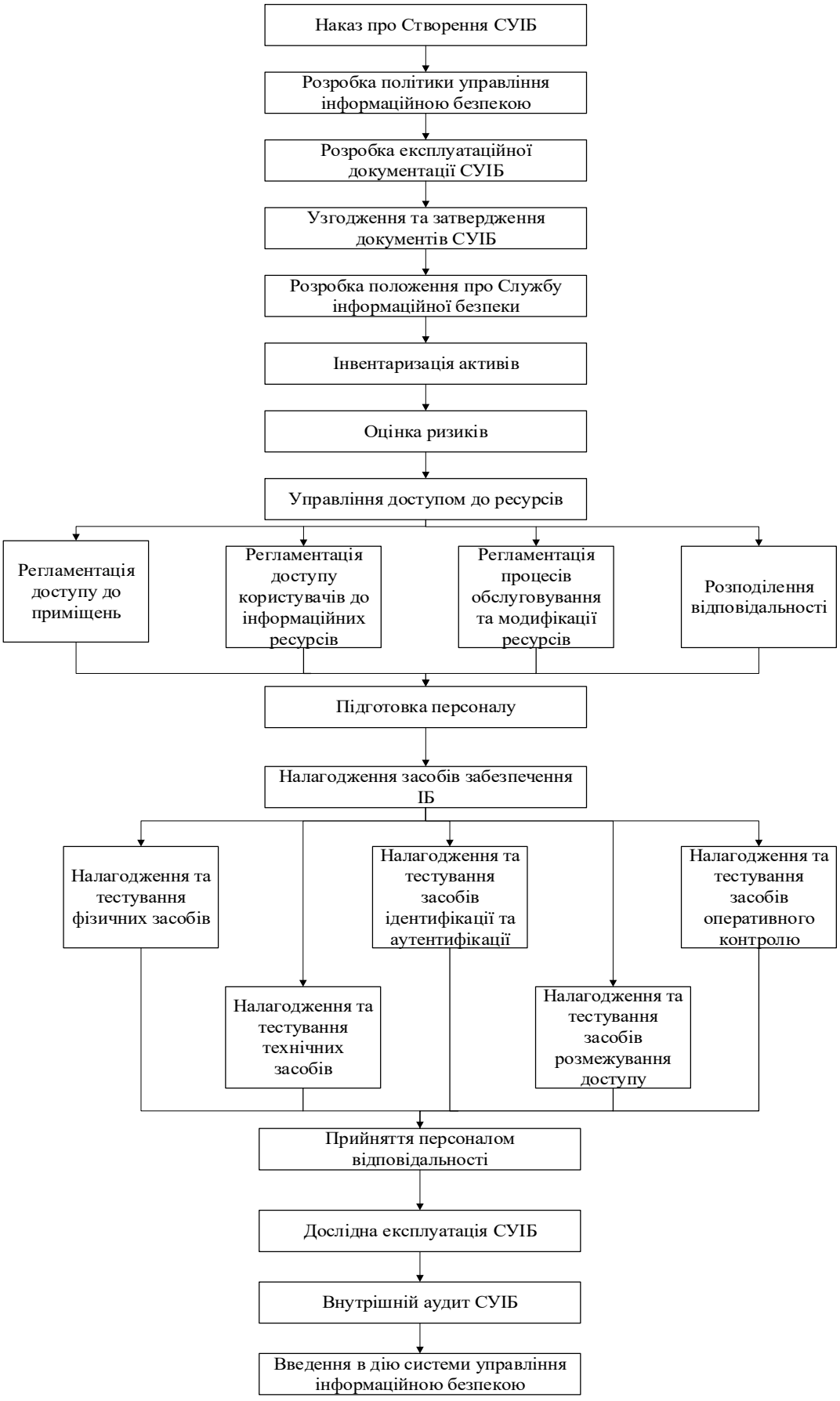


Рис. 3.2. Схема алгоритму впровадження політики інформаційної безпеки

Аналіз алгоритму дій керівництва в процесах розробки та впровадження політики інформаційної безпеки організації проводиться на прикладі процесів управління активами та процесів управління документацією СУІБ шляхом аналізу методик управління цими процесами.

### 3.1.1. Процеси управління активами організації

Процес управління інформаційними активами — це процес планування, створення, організації впровадження і контролю за якістю інформаційних активів закладу, установи, організації. Український стандарт ДСТУ ISO/IEC 27002 рекомендує такі дії керівництва для забезпечення цих процесів.

Виходячи з контексту організації та її бізнес-цілей, керівництво організації повинне класифікувати інформацію, якою володіє та використовує організація. Інформація повинна бути класифікована з точки зору юридичних вимог, змісту, критичності і уразливості для несанкціонованого розкриття і зміни; точки зору її цінності, правових вимог, секретності та критичності для організації. Класифікація та пов'язані з нею методи захисту інформації повинні враховувати потреби бізнесу в обміні інформацією або обмеження доступу до неї, так само як і законодавчі вимоги. [14]

Ступінь конфіденційності або значимості інформації може змінюватися після закінчення певного періоду часу, наприклад, після її опублікування. Подібні фактори повинні прийматися до уваги, тому що віднесення до більш високої категорії може вести до застосування методів реалізації, в яких немає необхідності, що веде до додаткових витрат, або навпаки, віднесення до нижчої категорії може ставити під загрозу досягнення бізнес-цілей організації.

Схема класифікації повинна включати в себе угоду про класифікацію та критерії для перегляду класифікації через якийсь час. Рівень захисту в схемі повинен бути оцінений на основі аналізу конфіденційності, цілісності і можливості застосування, а також будь-яких інших вимог, пов'язаних з інформацією. Схема повинна бути узгоджена з політикою контролю доступу. Кожному рівню має бути

присвоєно найменування, яке має сенс в контексті застосування цієї класифікаційної схеми.

Схема повинна бути єдиною для всієї організації, щоб всі, хто будуть класифікувати інформацію і пов'язані з нею активи, робили це однаково, мали загальне розуміння вимог захисту і застосовували відповідні заходи захисту.

Класифікація повинна бути включена в процеси організації, бути єдиною і логічно несуперечливою в рамках організації. Результати класифікації повинні відображати цінність активів, що залежить від їх ступеня закритості і значущості для організації, наприклад, з точки зору конфіденційності, цілісності і можливості застосування. Результати класифікації повинні оновлюватися відповідно до вимірами цієї цінності, ступеня конфіденційності і значущості протягом всього їх життєвого циклу.

Основні принципи класифікації повинні включати умови для початкової класифікації і повторної класифікації після закінчення деякого часу відповідно до якоїсь визначеної політикою контролю доступу.

Інформація часто перестає бути чутливою або критичною після закінчення деякого періоду часу, наприклад, коли інформація зроблена загальнодоступною. Ці аспекти слід брати до уваги, оскільки привласнення підвищеної категорії може привести до задіяння зайвих заходів захисту, таким чином, збільшуючи витрати.

Активом є все, що має цінність для організації і, отже, потребує захисту. При ідентифікації активів слід мати на увазі, що інформаційна система складається не тільки з апаратних і програмних засобів.

Ідентифікацію активів слід здійснювати на відповідному рівні деталізації, що забезпечує достатню інформацію для оцінки ризику. Рівень деталізації, який використовується при ідентифікації активів, впливає на загальний обсяг інформації, зібраної під час оцінки ризику. Цей рівень може бути більш деталізований при подальших ітераціях оцінки ризику.

Для кожного активу повинен бути визначений власник, щоб забезпечити компетентність і відповідальність за кожен актив. Власник активу може не мати права власності на актив, але він несе повну відповідальність за його отримання,

розробку, підтримку, використання і безпеку. Найчастіше власник активу є найбільш підходящою особою, яка спроможна визначити реальну цінність активу для організації. Призначений власник може бути або окремою особою, або підрозділом, який має затверджену відповідальність за актив протягом усього його життєвого циклу. [33]

У складних інформаційних системах може бути корисним позначати групи активів, які діють спільно для забезпечення такої певної функції, як «послуги». У цьому випадку власник послуг відповідає за поставку послуги, включаючи функціонування активів, які її забезпечили.

Організація повинна ідентифікувати всі активи і документувати важливість цих активів. Інвентаризація активів повинна включати всю інформацію, необхідну для відновлення активів після будь-якого лиха, включаючи тип активу, формат, місце розташування, дублюючу інформацію, інформацію про ліцензії та цінність бізнесу. Інвентаризація не повинна без необхідності дублювати інші інвентаризації, а повинна забезпечувати коригування свого змісту.

Після класифікації інформації, на її основі формується опис активів, до яких відносяться:

- інформацію: бази даних і файли даних, контракти і угоди, системна документація, інформація про дослідження, керівництва користувача, навчальні матеріали, процедури експлуатації або підтримки, плани щодо забезпечення безперервності ділової діяльності, процедури відкоту при збоях, контрольні журнали і архівована інформація;
- активи програмного забезпечення: прикладне програмне забезпечення, системне програмне забезпечення, інструментальні засоби розробки і утиліти;
- фізичні активи: комп'ютерне обладнання, апаратура зв'язку, знімні носії інформації та інше обладнання;
- послуги: обчислювальні послуги і послуги зв'язку, основні комунальні послуги, наприклад, опалення, освітлення, подача електроенергії, кондиціонування;
- працівники і їх кваліфікація, виробничі досвід і навички;

- нематеріальні фактори, такі як: репутація і престиж організації. [14]

Опис активів надає впевненість в тому, що забезпечується ефективний захист активів, і можуть також знадобитися для цілей забезпечення безпеки праці, страхування або вирішення фінансових питань (управління персоналом). Процес складання опису активів - важливий аспект управління ризиками інформаційної безпеки. Правила для належного використання інформації і активів, пов'язаних з інформацією та пристроями обробки інформації, повинні бути визначені, задокументовані та впроваджені в залежності від оброблюємої інформації.

Для визначення активів в рамках області дії СУІБ необхідно визначити і вказати наступну інформацію:

- унікальне найменування процесу;
- опис процесу і пов'язані з ним дії (створення, зберігання, передача, видалення);
- важливість процесу для організації (критичний, важливий, допоміжний);
- власник процесу (підрозділ організації);
- процеси, що забезпечують вихідні і вихідні дані цього процесу;
- додатки IT, що підтримують процес;
- д) класифікація інформації (конфіденційність, збереження, доступність, контроль доступу, неспростовності і (або) інші важливі для організації властивості, наприклад, як довго може зберігатися інформація).

Співробітники і зовнішні користувачі, які використовують або мають доступ до активів організації, повинні бути ознайомлені з вимогами інформаційної безпеки, що відносяться до інформації та інших активів організації, які пов'язані з інформацією, пристроями і ресурсами для обробки інформації. Вони повинні нести відповідальність за застосування ними будь-яких ресурсів обробки інформації і будь-яка подібна використання, здійснюване в зоні їх відповідальності. Термін «власник» не означає, що особа фактично має будь-які права на власність. [35]

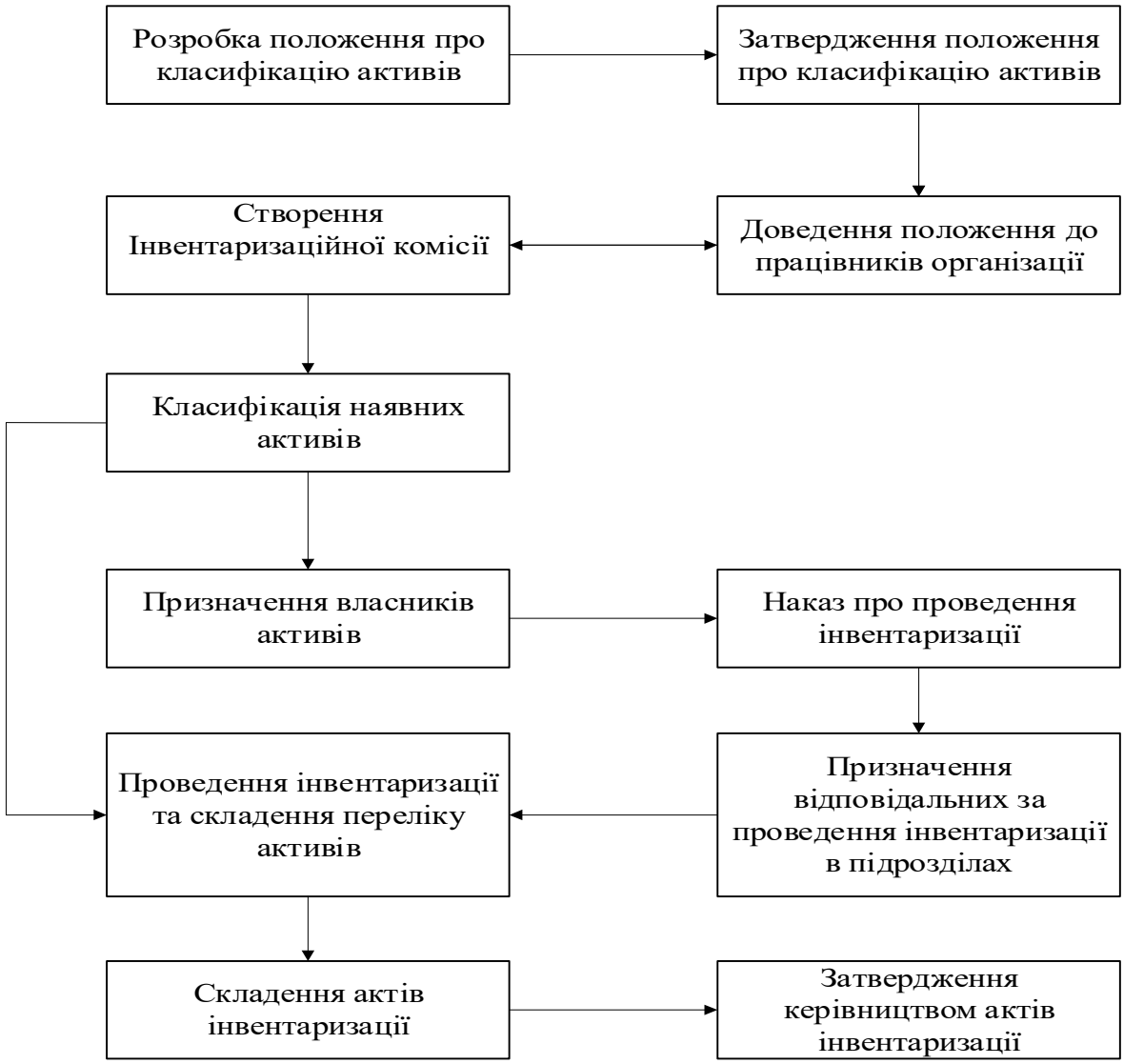


Рис. 3.3. Схема алгоритму дії керівництва в процесі управління активами

1. Комісія з інформаційної безпеки розробляє Положення про класифікацію активів організації.

2. Генеральний директор затверджує Положення про класифікацію активів організації.

3. Положення про класифікацію активів організації доводиться до керівників усіх підрозділів.

4. Керівництво підрозділів проводить класифікацію наявних у підрозділі активів.

5. Рішення про проведення інвентаризації активів організації у процесі створення системи управління інформаційною безпекою приймає Генеральний директор за поданням Комісії з інформаційної безпеки.

6. Наказом Генерального директора створюється Інвентаризаційна комісія та встановлюється термін завершення інвентаризації.

7. Керівниками підрозділів призначаються відповідальні за проведення інвентаризації в підрозділі.

8. Членами інвентаризаційної комісії разом з відповідальними від підрозділу проводиться інвентаризація та складаються переліки активів, які підписуються членами комісії та представником підрозділу.

9. Перевірка фактичної наявності ресурсів ІКС виробляється за участю посадових осіб, відповідальних за інформаційну безпеку в підрозділі.

10. Інвентаризаційна комісія складає акти інвентаризації з переліками активів та подає на розгляд Комісії з інформаційної безпеки.

11. Комісія з інформаційної безпеки розглядає, погоджує та подає на затвердження Генеральному директору акти інвентаризації з переліками активів

12. Генеральний директор затверджує документи інвентеризації активів.

Після введення в дію системи управління інформаційною безпекою, управління активами організації забезпечується Службою інформаційної безпеки під керівництвом директора з безпеки.

### 3.1.2. Процеси управління документацією СУІБ

Аналіз алгоритму дій керівництва у процесі управління документацією СУІБ здійснюється шляхом аналізу методики управління документацією СУІБ.

Документація Системи управління інформаційною безпекою є складовою документації Системи управління організацією.

Управління документацією СУІБ грунтується на вимогах та рекомендаціях ДСТУ ISO/IEC 27001 та ДСТУ ISO/IEC 9001 і будується на таких основних принципах:

1) керівництво організації в рамках затвердженої політики безпеки визначило документацію (в тому числі протоколи), яка необхідна для створення, впровадження та забезпечення ефективного функціонування системи управління інформаційною безпекою і забезпечення діяльності процесів, що застосовуються в організації;

2) характер і обсяг документації відповідає вимогам ДСТУ, адаптований до профілю виробництва таким чином, що задовольняє контрактні, правові та регламентовані вимоги до документування процесів забезпечення інформаційної безпеки. Документація може мати будь-яку форму і розміщуватися на будь-якому носії, відповідно до умов і потреб виробництва;

3) на основі прийнятої в організації політики обізнаності персоналу з питань інформаційної безпеки забезпечений доступ працівникам до інформації, необхідної для виконання функціональних обов'язків.

Завданням управління документами і даними є організація чіткої ідентифікації (позначення), шляхи пошуку і використання їх в роботі. Таке ж управління має поширюватися і на всі зміни, що вносяться в документи.

Щодо системи управління інформаційною безпекою всі документи, що розробляються і знаходяться в обігу в організації діляться на наступні групи:

1) зовнішні, міжнародні стандарти, державні та відомчі нормативні документи, регламенти, документи;

2) внутрішні документи системи управління інформаційною безпекою (положення, політики, методики, робочі інструкції, звіти про аудити, протоколи).

Вхідна, вихідна кореспонденція та документи зовнішніх організацій обробляються відповідно до загальних правил та порядку поводження, обробки і зберігання документів в організації.

Документація системи менеджменту інформаційної безпеки структурована згідно до основних концептуальних напрямків забезпечення інформаційної безпеки, вимог міжнародних і національних стандартів і спеціальних нормативних документів і об'єднує в блоки:

- Політики інформаційної безпеки

- Організація системи інформаційної безпеки
- Управління документацією СУІБ
- Управління персоналом
- Управління активами
- Менеджмент ризиків інформаційної безопасноти
- Фізична безпека
- Операційний менеджмент
- Управління доступом
- Управління інцидентами
- Управління аудитом
- Відповідність вимогам

А також містить перелік зовнішніх документів, структурований за наступними напрямками:

- Міжнародні стандарти та нормативні документи;
- Державні стандарти та нормативні документи;
- Корпоративні стандарти і нормативні документи;
- Експлуатаційні документи ІС.

Документація системи управління інформаційною безпекою містить:

1) документально оформлену політику інформаційної безпеки;

2) керівництво з інформаційної безпеки;

3) опис процесів СУІБ;

4) задокументовані методики СУІБ (далі - методики) відповідно до вимог:

5) документи для забезпечення ефективного планування, функціонування та контролю процесів, зокрема:

- програми та методики забезпечення інформаційної безпеки виконання проектів;
- стандарти організації, положення та інші документи, що визначають організацію, структуру і відповідальність підрозділів і посадових осіб за виконання вимог системи менеджменту інформаційної безпеки в процесі виконання

організацією своїх зобов'язань перед замовником та іншими зацікавленими сторонами;

- методики (опису) процесів.

6) протокольні записи (протоколи та інші облікові і звітні документи) для надання доказів відповідності вимогам та результативності системи управління інформаційною безпекою. Протоколи повинні бути чіткими, зручними для читання та ідентифікації.

Облік всіх зовнішніх і внутрішніх документів СУІБ ведеться методом їх реєстрації в електронних базах документів

Документовані методики СУІБ. Документовані методики системи управління інформаційною безпекою (далі - методики) складають основну частину документації системи менеджменту інформаційної безпеки, та використовується для загального планування і управління видами діяльності, які впливають на інформаційну безпеку. Відповідно до стандарту ДСТУ ISO/IEC 27001 ці методики охоплюють всі відповідні процеси і елементи системи управління інформаційною безпекою. Вони встановлюють функціональні обов'язки, повноваження, відповідальність і взаємозв'язок персоналу, виконують, перевіряють і аналізують роботу, яка впливає на інформаційну безпеку, керують цією роботою, а також встановлюють порядок здійснення різних видів діяльності, використання документації та застосування засобів контролю.

Кожна методика охоплює процес, елемент системи, логічно відокремлену частину процесу (подпроцесс) або елемента системи і відображає складність, характер і спосіб виконання відповідного виду діяльності.

Кількість методик, обсяг кожної з них, спосіб їх побудови та подання стандартам ДСТУ ISO/IEC 27001 не визначаються і можуть змінюватися в процесі вдосконалення системи управління інформаційною безпекою і перегляду її документації.

З метою полегшення розробки та подальшої роботи з методиками, вони побудовані і оформлені за уніфікованими правилами.

Робочі інструкції СУІБ. Положення методик розширюються робочими інструкціями СУІБ, які визначають порядок і відповідальність при виконанні описаних в методиках процесів і процедур системи управління інформаційною безпекою.

Робочі інструкції з інформаційної безпеки на відміну від робочих інструкцій виробничого призначення (вирішення технічних питань) не містять технічних даних і включають:

1. докладний опис етапів діяльності по методиці;
2. відповідальність за виконання;
3. порядок документального оформлення роботи згідно з інструкцією;
4. структурну побудову і порядок оформлення документів СУІБ, що розробляються;
5. порядок розподілу документів.

Протокольні записи СУІБ. Результати роботи з управління та контролю системи менеджменту інформаційної безпеки організації підлягають документальному оформленню у вигляді протокольних записів (протоколів, актів та інших документів), що містять відомості про:

- ступеня виконання завдань в області інформаційної безпеки;
- результати функціонування системи з проведення аналізу та підвищення інформаційної безпеки розробки проектів інформатизації та програмних продуктів;
- коригувальні та запобіжні дії, їх ефективність;
- рівень кваліфікації і підготовки персоналу.

Ідентифікація (позначення), контроль і зберігання цих документів здійснюється відповідно до цієї методики.

Правила розробки внутрішніх документів СУІБ. Жорстких вимог до структури і оформлення керівництва з інформаційної безпеки не існує, але воно точно, повно і послідовно визначає політику, цілі і основні документовані методики товариства в області інформаційної безпеки.

Методики виконання процесів обов'язково повинні мати такі розділи:

- зміст;
- терміни, визначення понять і умовні позначення;
- цілі процесу;
- галузь застосування;
- загальні положення;
- схема процесу;
- оцінка результативності процесу;
- посилання;
- сторінка реєстрації змін;
- список виконавців.

Форми протоколів СУІБ обов'язково повинні мати такі поля:

- номер протоколу;
- дата заповнення протоколу;
- посаду, прізвище, підпис особи, що заповнює протокол;
- інші поля для реєстрації даних.

Допускається оформлення протоколів без затвердженої форми, при цьому у верхній частині необхідно вказувати також назва протоколу.

Правила внесення змін до документів. Внесення змін до документів СУІБ здійснюється за допомогою:

а) введення нової редакції всього документа зі скасуванням попередньої редакції і реєстрацією в відомості документів;

б) заміною однієї або декількох сторінок документа з виданням повідомлення про зміну та інформації на титульному аркуші по номеру зміни, дати зміни і номерів змінених сторінок.

Узгодження зміни, яке впливає на виробничий процес, проводиться з усіма особами, які погодили основний документ і беруть участь у впровадженні цієї зміни. Затверджує зміни відповідальна особа, яка затвердила основний документ.

Всі дії по розробці нових документів, внесення змін до існуючих документів, зміни статусу документа проводить особа, відповідальна за розробку цього

документа. Вище перераховані дії розробник документа здійснює автономно (на своєму комп'ютері). Після проведення вищевказаних дій документи подаються на перевірку, погодження та затвердження.

Перевірка та затвердження. Впровадження в дію документів СУІБ регламентується наказом організації.

З метою забезпечення правильності структури, чіткості, точності, прийнятності викладу всі документи системи менеджменту інформаційної безпеки перед випуском повинні проходити перевірку та затверджуватися Директором з безпеки.

Документи СУІБ за конкретним проектом затверджуються одночасно з іншими планувальними документами по проекту.

Окремі документи СУІБ за конкретним проектом, які розробляються в структурних підрозділах або з їх ініціативи, можуть затверджуватися заступниками генерального директора, якому підпорядковані ці підрозділи, з обов'язковим погодженням директором з безпеки та керівником служби інформаційної безпеки.

Затвердження документа дає дозвіл на його випуск на електронних носіях і іншими способами.

Відповідальність за своєчасне поширення документів СУІБ несуть керівник групи інформаційної безпеки і керівник проекту.

Поширення затверджених документів СУІБ забезпечує впевненість в тому, що всі користувачі мають необхідний доступ до них.

Керівництво організації та структурних підрозділів забезпечують, щоб всім працівникам було відомо, які частини установки та інші документи СУІБ стосуються кожного користувача в межах його функціональних вовноважень.

Внутрішні документи розробляються і коректуються за допомогою комп'ютерних засобів. Документи СУІБ оформляються відповідно до вимог

Керівник служби інформаційної безпеки реєструє документ в Реєстрі документів.

Уповноважений співробітник служби інформаційної безпеки готує необхідну кількість копій, позначає їх і розсилає (заміну попередньої редакції документа на

нову) згідно з переліком розсилки що додається до оригіналу. Перелік розсилки визначає службова особа, котра затвердила документ. При отриманні нового документа (нової редакції) відповідальні особи розписуються в отриманні.

Відповідний контроль за поширенням затверджених документів здійснюється шляхом нанесення облікових номерів на паперових примірниках для конкретних одержувачів.

Примірники документів СУІБ, переданих в виробничі підрозділи, є контрольованими.

Доступ до документів СУІБ. Доступ до документації СУІБ повинні мати тільки вище керівництво, відповідальні за інформаційну безпеку, керівник проекту і керівники структурних підрозділів, які розробляють даний проект, а також персонал служби інформаційної безпеки. Інші працівники організації мають допуск до документів системи управління інформаційною безпекою в межах їх функціональних повноважень.

Правила зберігання і використання документів СУІБ. Всі документи СУІБ повинні зберігатися в умовах, що виключають їх пошкодження, бути розбірливі, не повинні мати помарок,.

Електронні документи СУІБ зберігаються в базі документів, доступ до якої суворо регламентований.

Скасування документів СУІБ. Заміна та скасування документів СУІБ регламентується наказом організації за поданням служби інформаційної безпеки та директора з безпеки.

Знищення скасованих оригіналів і документів, що знаходяться на електронних носіях здійснюється за вказівкою представника керівництва з питань інформаційної безпеки.

Відібрані для знищення скасовані документи оформляються актом про знищення за встановленою формою.

Відповідальність за організацію планування і розробку нових і перегляд чинних документів СУІБ, за забезпечення організації зовнішньою нормативною і

законодавчою документацією несе директор з безпеки та керівник служби інформаційної безпеки.

Розробники документів несуть відповідальність за зміст документів, правильність оформлення, дотримання порядку розробки, відповідно до вимог цієї методики.

Служба інформаційної безпеки складає плани і розробляє документи СУІБ. Плани розробки документів СУІБ складаються на підставі результатів аналізу та конкретних вказівок з боку керівництва організації, пропозицій керівників структурних підрозділів, вимог нормативних документів і стандартів, повсякденного аналізу документації.

За планування і розробку документів СУІБ, які відносяться до конкретного проекту, несе відповідальність Керівник проекту.

Порядок затвердження і внесення змін. Відповідальний за розробку документа СУІБ представляє редакцію документа на розгляд Служби інформаційної безпеки для оцінки його повноти і соответсвия вимогам нормативної і законодавчої документації. Після розгляду і внесення необхідних поправок документ проходить процедуру узгодження зацікавленими сторонами і затвердження керівництвом.

Зміни в документ вносяться, узгоджуються і затверджуються в тому ж порядку що і основний текст документа.

Рішення про внесення змін до документа СУІБ приймається Службою інформаційної безпеки в разі зміни вимог нормативних документів, зміни вимог політики інформаційної безпеки, зміні архітектури, складу і платформи функціонування АС, а також:

- на вимогу вищого керівництва;
- за пропозиціями керівників структурних підрозділів;
- за пропозиціями керівників проектів підрозділів-розробників системи.

Інформація про внесення змін до документа СУІБ здійснюється Службою інформаційної безпеки шляхом розсилки зацікавленим сторонам і виконавцям повідомлень про внесення змін до документа.

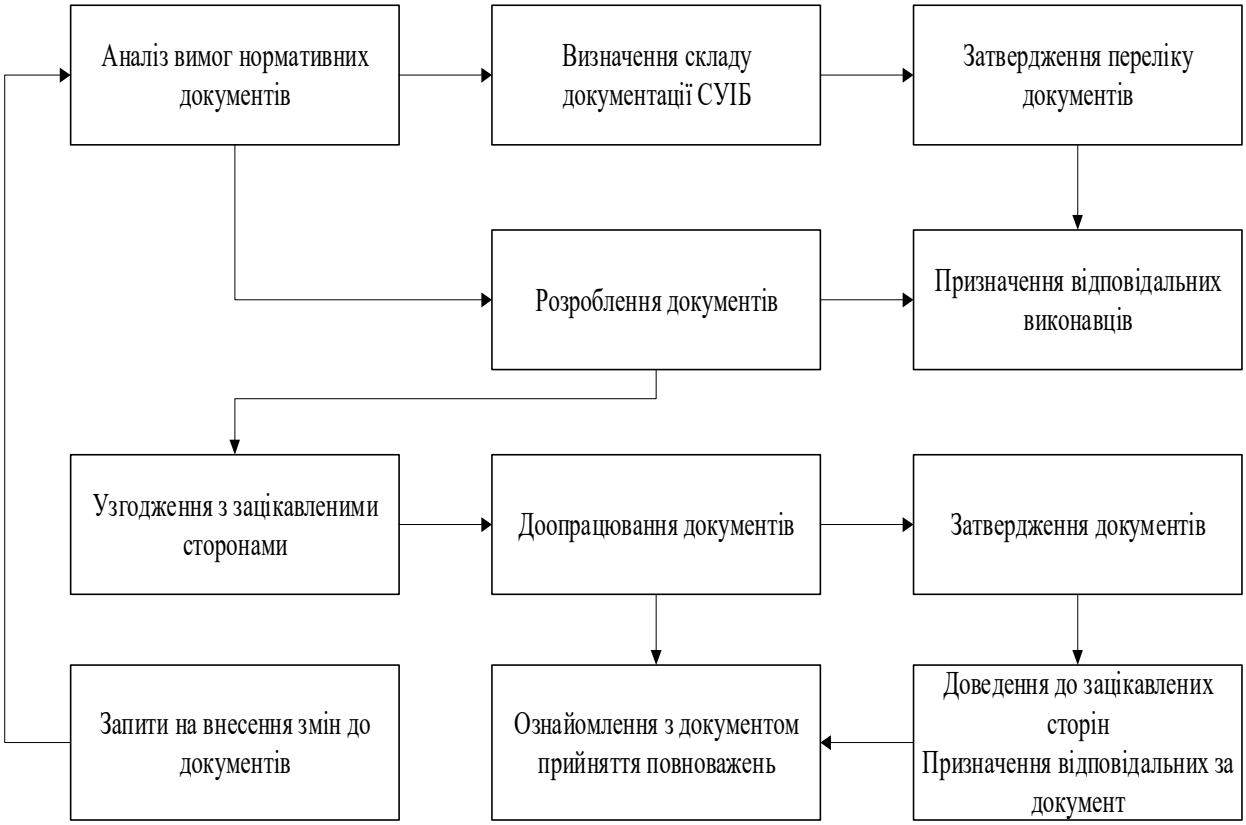


Рис. 3.4. Схема алгоритму дій керівництва в процесі управління документацією

1. Комісія з інформаційної безпеки розробляє перелік документів СУІБ організації та визначає відповідальних за розробку документів.

2. Генеральний директор затверджує перелік документів СУІБ організації та призначає відповідальних за розробку документів.

3. Комісія з інформаційної безпеки розробляє Методику управління документацією СУІБ.

4. Генеральний директор затверджує Методику управління документацією СУІБ.

5. Методику управління документацією СУІБ організації доводиться до усіх зацікавлених сторін та підрозділів.

6. Керівництво підрозділів призначає відповідальних за управління документацією СУІБ у підрозділі.

7. Координацію робіт з розробки документів СУІБ забезпечує Комісія з інформаційної безпеки.

8. Комісія з інформаційної безпеки розглядає, погоджує та подає документи СУІБ на затвердження Генеральному директору.

9. Документи СУІБ затверджуються та вводяться в дію наказом Генерального директора.

10. Директор з безпеки призначає відповідальну особу за ведення Реєстру документів СУІБ.

11. Внесення змін у документи СУІБ здійснюється розпорядженням директора з безпеки організації.

12. Скасування документів СУІБ здійснюється наказом Генерального директора.

### 3.2. Рекомендації щодо поліпшення дій керівництва в процесах забезпечення політики інформаційної безпеки в організації

Після прийняття керівництвом рішення щодо створення СУІБ організації необхідно провести ряд заходів, які дозволять підготувати організацію до вирішення задач побудови системи управління інформаційною безпекою.

Роботи по створенню СУІБ вимагають відповідної освіти, досвіду роботи у галузі інформаційної безпеки та високого кваліфікаційного рівня співробітників. У зв’язку з чим, необхідно на етапі підготовки до створення СУІБ створити в структурі організації спеціалізований підрозділ - Службу інформаційної безпеки.

Директору з безпеки та начальнику відділу кадрів необхідно укомплектувати Службу інформаційної безпеки підготовленими спеціалістами з відповідним досвідом роботи, з відповідною базовою освітою та досвідом роботи у сфері інформаційної безпеки. Забезпечити навчання співробітників служби, які потребують підвищення кваліфікації. Після укомплектування та навчання, персонал Служби інформаційної безпеки повинен детально ознайомлення з організаційно-функціональною структурою організації та інформаційними технологіями та засобами захисту інформації, які використовуються в організації.

На стадії розробки концепції інформаційної безпеки організації доцільно залучати до виконання робіт сторонніх експертів, які мають відповідний досвід роботи. Для забезпечення ефективної роботи вищому керівництву слід активніше застосовувати мотивацію.

Вищому керівництву організації необхідно більше уваги приділяти контролю забезпечення політики інформаційної безпеки організації, для чого керівництву потрібно розробити «Положення про застосування контролів», «Положення про внутрішній аудит», «Методику внутрішнього аудиту».

На етапі впровадження регулярно проводити наради про стан виконання планів та аналізу виконання контролів.

## Висновки до третього розділу

В рамках третього розділу були проаналізовані процеси розробки та впровадження політики інформаційної безпеки в організації для організації, організаційно-функціональна структура якої була визначена в розділі 2.2.

Структура та зміст політики інформаційної безпеки організації відповідає вимогам стандартів та, в основному, корелює з передовими практиками, які були досліджені у розділі 2.3.

Досліджені процеси розробки та впровадження політики інформаційної безпеки організації, на основі яких розроблено схему алгоритму розробки політики інформаційної безпеки організації та схему алгоритму впровадження політики інформаційної безпеки організації.

На основі аналізу методики класифікації інформації організації та методики управління активами, досліджено процеси управління активами. Розроблено структуру переліків інвентаризації активів (див. Додаток А.). Розроблений та схематично зображений алгоритм дій керівництва при управлінні інформаційними активами.

На основі аналізу методики управління документацією, досліджені процеси та дії керівництва по управлінню документацією СУІБ організації, визначені

вимоги до структури окремих документів СУІБ. Розроблений та схематично зображений алгоритм дій керівництва по управлінню документацією СУІБ.

Розроблені документи придатні до практичного використання у якості шаблонів документів.

Розроблені рекомендації щодо поліпшення дій керівництва в процесах забезпечення політики інформаційної безпеки організації.

## ВИСНОВКИ

У результаті роботи було:

1. Досліджено основні питання нормативно-правових засад управління інформаційною безпекою шляхом аналізу вимог стандартів ДСТУ ISO/IEC серії 27к. Розглянуті цілі, принципи та методи забезпечення політики інформаційної безпеки організації.

2. Розроблено схема структури забезпечення політики інформаційної безпеки організації та схема організаційної структури дій керівництва у системі забезпечення управління інформаційною безпекою організації.

3. Проведено аналіз дій керівництва на різних фазах створення системи управління інформаційною безпекою організації. Отримані результати використані при дослідженні роботи керівництва організації по забезпеченню політики інформаційної безпеки організації.

4. Проаналізовано основні дії керівництва по управлінню забезпеченням політики інформаційної безпеки організації. Визначені основі функції, на яких мають базуватися дії керівництва по забезпеченню політики інформаційної безпеки. Визначені та описані ресурси, що задіяні до розробки політики інформаційної безпеки

5. Розроблено організаційно-функціональну схему організації, яка використовувалась в роботі для дослідження процесів розробки та впровадження політики інформаційної безпеки організації.

6. На основі аналізу розроблено структурно-логічну схему алгоритму дій керівництва по забезпеченню інформаційної безпеки організації. Проведено аналіз дій керівництва згідно до ДСТУ ISO/IEC 27003.

7. Досліджено та проаналізовано практики розробки та впровадження політики інформаційної безпеки провідних міжнародних організацій, таких як: Sun Microsystems, Microsoft, Cisco, IBM.

8. Досліджено та проаналізовано використання сучасного програмного забезпечення для розробки, формування, впровадження та перевірки політики інформаційної безпеки згідно до нормативних документів.

9. Досліджено процеси розробки та впровадження політики інформаційної безпеки організації, на основі яких розроблено схему алгоритму розробки політики інформаційної безпеки організації та схему алгоритму впровадження політики інформаційної безпеки організації.

10. На основі аналізу методики класифікації інформації організації та методики управління активами, досліджено процеси управління активами. Розроблено структуру переліків інвентаризації активів (див. Додаток А.). Розроблений та схематично зображений алгоритм дій керівництва при управлінні інформаційними активами.

11. На основі аналізу методики управління документацією, досліджено процеси та дії керівництва по управлінню документацією СУІБ організації, визначені вимоги до структури окремих документів СУІБ. Розроблений та схематично зображений алгоритм дій керівництва по управлінню документацією СУІБ.

12. Розроблено рекомендації щодо поліпшення забезпечення управління політикою інформаційної безпеки організації. Розроблені документи придатні до практичного використання у якості шаблонів документів.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013/Cor 2:2015, IDT). Поправка № 2:2019 [Чинний від 01.11.2019] Вид. офіц: ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» [Електронний ресурс]. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85804
2. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013/Cor 2:2015, IDT). Поправка № 2:2019 [Чинний від 16.10.2019] Вид. офіц: ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» [Електронний ресурс]. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85805
3. ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT) [Чинний від 01.10.2018] Вид. офіц: ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» [Електронний ресурс]. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=78517
4. О. К. Юдін, В.М. Богуш Інформаційна безпеки держави, Київ: МК-Прес, 2005 с. 35 [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/5376129/
5. Овсянніков В.В Аналіз нормативно-правових та організаційно-технічних аспектів забезпечення інформаційної безпеки, *Сучасні інформаційні технології у сфері безпеки та оборони*, № 3 2015, с.187-192 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/sitsbo_2015_3_35
6. Щебланін Ю.М. «Правове забезпечення інформаційної безпеки»: конспект лекцій [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/5367198/page:4/

7. Якименко Ю.М. Особливості реалізації системного методу стосовно до побудови систем управління інформаційною безпекою організації, *Збірник тез наукових доповідей* (Київ, 4 квітня 2019 року), с. 144-147 [Електронний ресурс]. – Режим доступу: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf
8. М.Ю. Комаров, Є.Ф. Гончар, А.В. Ониськова Нормативний аспект побудови та впровадження системи управління інформаційною безпекою на об'єктах критичної інфраструктури, *Моделювання та інформаційні технології*. - 2018. - Вип. 82., С. 40-48. [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/j-pdf/Mtit_2018_82_8.pdf
9. В. Г. Кононович, С.В. Стайкуца, Т. М. Тардаскіна, Т. М. Шинкарчук. «Забезпечення інформаційної безпеки цифрових програмно керованих АТС: навчальний посібник для курсового та дипломного проектування.». - 2011., с. 6-11 [Електронний ресурс]. – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/1115/view/493
10. Л.Я Страхарчук, В.П. Страхарчук Інформаційні системи і технології в банках: навчальний посібник, К.: УБС НБУ: Знання, 2010. с.186-188 [Електронний ресурс]. – Режим доступу: https://pidru4niki.com/1584072022211/bankivska_sprava/informatsiyni_sistemi_i_tehnologiyi_v_bankah
11. М. О. Мельник, Г. Д. Нікітин, К. О. Мезенцева Аналіз побудови моделі політики інформаційної безпеки підприємства, *Системи обробки інформації*. - 2017. - Вип. 2. - С. 126-128. [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/soi_2017_2_26
12. Медведев М.В. Стандарты и политика информационной безопасности автоматизированных систем, «*Приборостроение*», 2010, №1 с.103-111 [Електронний ресурс]. – Режим доступу: https://cyberleninka.ru/article/n/standarty-i-politika-informatsionnoy-bezopasnosti-avtomatizirovannyh-sistem

13. ISO/IEC 27001 Information technology - Security techniques - Information security management systems, – Requirements [Електронний ресурс]. – Режим доступу: https://trofisecurity.com/assets/img/iso27001-2013.pdf
14. ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls [Електронний ресурс]. – Режим доступу: https://trofisecurity.com/assets/img/ISO-IEC_27002-.pdf
15. Матиев Д. Средства защиты информации: проблема выбора и соответствия / Джабраил Матиев. [Електронний ресурс]. – Режим доступу: https://bankir.ru/publikacii/20100621/sredstva-zaschiti-informacii-problema-vibora-i-sootvetstviya-5386161/
16. Н.В. Медведев, П.М. Квасов, В.Л. Цирлов Стандарты и политика информационной безопасности автоматизированных систем, «*Приборостроение*», 2010, №1 с.103-111 [Електронний ресурс]. – Режим доступу: https://cyberleninka.ru/article/n/standarty-i-politika-informatsionnoy-bezopasnosti-avtomatizirovannyh-sistem/viewer
17. Т.М. Мужанова Організаційне забезпечення інформаційної безпеки підприємства: основні засади, *Сучасний захист інформації* №2, 2016, с.78-82 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/szi_2016_2_13
18. В.М. Ахрамович Адміністративний рівень інформаційної безпеки, *Сучасний захист інформації* №1, 2017, с.10-14 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/szi_2017_1_4
19. Чистоклетов Л.Г., Хитра О.Л. Адміністративно-правові засоби у забезпеченні інформаційної безпеки України [Електронний ресурс]. – Режим доступу: http://aphd.ua/publication-349/
20. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №2163-VIII [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text
21. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президент України

від 26.05.2015 № 287/2015. – [Електронний ресурс]. Режим доступу : http: //zakon2.rada.gov.ua/laws/show/287/2015/ paran14#n14.

22. Постанова «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» від 28.09.2017 № 95 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text

23. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 №80/94 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

24. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу від 22 квітня 1999р. №22 [Електронний ресурс]. – Режим доступу: https://tzi.com.ua/downloads/1.1-003-99.pdf

25. Хорошко В.О., Артемов В.Ю. Окремі аспекти впровадження міжнародних стандартів забезпечення інформаційної безпеки в спеціальних службах України, *Науково-технічний журнал «Захист інформації»* №3, 2009, с. 85-90 [Електронний ресурс]. – Режим доступу: http://jrnl.nau.edu.ua/index.php/ZI/article/download/4035/4183

26. Петренко С.О., Курбатов В.А Политики безопасности компании при работе в Интернет, ДМК Пресс, 2011, с. 85-123 [Електронний ресурс]. – Режим доступу: https://proklondike.net/books/defence/petrenko_polit_bez_komp_2011.html

27. В. С. Шевченко Менеджмент і адміністрування (менеджмент): конспект лекцій, 2016, с. 26 [Електронний ресурс]. – Режим доступу: https://core.ac.uk/download/pdf/78066418.pdf

28. Microsoft Security Assesment Tool User Guide, 2005 [Електронний ресурс]. – Режим доступу: https://nanopdf.com/download/user-guide-5aea9e3ff00da_pdf

29. McAfee ePolicy Orchestrator [Електронний ресурс]. – Режим доступу: https://www.mcafee.com/enterprise/ru-ru/assets/data-sheets/ds-epolicy-orchestrator.pdf

30. Jupiter One Security Policy Builder [Електронний ресурс]. – Режим доступу: https://jupiterone.com/features/policy-builder/

31. Tivoli Security Policy Manager User Guide [Електронний ресурс]. – Режим доступу:https://www.ibm.com/support/knowledgecenter/ru/SS9H2Y_10.0/com.ibm.dp.doc/tspm_introduction.html

32. Білокомірова Я. М Інформаційне забезпечення економічної безпеки підприємницької діяльності, *Вісник економіки транспорту і промисловості* №29, 2010, с. 308-312 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/Vetp_2010_29_77

33. О. В. Олійник Адміністративно-правові засоби забезпечення інформаційної безпеки, *Юридичний вісник 1 (34),* 2015, с. 65-67 [Електронний ресурс]. – Режим доступу: http://jrnl.nau.edu.ua/index.php/UV/article/view/8180

34. Домарєв В.В. Герасименко А.В. Системний підхід у вирішенні завдань по організації роботи підрозділу технічного захисту інформації на підприємстві, *Сучасний захист інформації* №2, 2013, с.13-15 [Електронний ресурс]. – Режим доступу: http://journals.dut.edu.ua/index.php/dataprotect/article/view/898/840

35. Марков А. С., Цирлов В. Л. Руководящие указания по кибербезопасности в контексте ISO 27032, *Вопросы кибербезопасности №1(2),* 2014, с.28-31 [Електронний ресурс]. – Режим доступу: https://s3r.ru/wp-content/uploads/2014/03/iso27032.pdf

36.А. М. Чорна Структура ресурсного забезпечення економічної безпеки підприємства, *Вісник Хмельницького національного університету*, № 4, 2009 Т. 1, с. 92 [Електронний ресурс]. – Режим доступу: http://journals.khnu.km.ua/vestnik/pdf/ekon/2009_4_1/pdf/092-095.pdf

37. Горбашко Е.А. Управління конкурентоспроможністю: навч. посібник, СПБ. Университет экономики и финансов, 1991. [Електронний ресурс]. Режим доступу: https://stud.com.ua/43080/ekonomika/sistema_upravlinnya_informatsiynoyu_bezpekoyu_pidpriyemstva

38. Захаров О.І. Інформаційне забезпечення управління системою економічної безпеки підприємства, с.5-6 [Електронний ресурс]. – Режим доступу: https://library.krok.edu.ua/media/library/category/statti/zakharov_0010.pdf

39. Зайцев С.Є. Политики информационной безопасности в системах информационной безопасности, *Научный вестник МГТУ ГА серия Студенческая наука*, 2008, №137, с.2-5 [Електронний ресурс]. – Режим доступу: https://cyberleninka.ru/article/n/politiki-informatsionnoy-bezopasnosti-v-sistemah-informatsionnoy-bezopasnosti

40. Игнатьев В.А. Информационная безопасность современного коммерческого предприятия: монографія. — Старый Оскол: ООО «ТНТ», 2005. с.10 [Електронний ресурс]. – Режим доступу: https://www.studmed.ru/view/ignatev-va-informacionnaya-bezopasnost-sovremennogo-kommercheskogo-predpriyatiya_f7b0bde3c2d.html?page=10

41. Кібальник Л.О. Впровадження політики інформаційної безпеки банківських установ, Причорноморські економічні студії., *Гроші, фінанси та кредит*, Вип. 12(2)., 2016., с.119-120 [Електронний ресурс]. – Режим доступу: http://bses.in.ua/journals/2016/12-2_2016/23.pdf

42. Інформаційна безпека. Чи працює Політика ІБ у Вашій компанії? [Електронний ресурс]. – Режим доступу: https://legalitgroup.com/informaciyna-bezpeka-v-kompanii/

43. Легомінова С.В Теоретичні засади інформаційної безпеки підприємства, *Економіка. Менеджмент. Бізнес.* № 3. , 2015., с. 87-92. [Електронний ресурс]. – Режим доступу: http://journals.dut.edu.ua/index.php/emb/article/view/477/443

# ДОДАТКИ

**Додаток А.**

## Шаблони документів з інвентаризації активів

Таблиця А.1.

Перелік приміщень, що захищаються:

| № п\п | Фізичне розташування | Опис, характеристики | Власник | Підстава права використання | Основне функціональне призначення | Встановлені технічні активи (з переліку технічних активів) | Методи захисту інформації, що використовуються | Цінність активу | Відповідальний |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | |
| | | | | | | | | | |

Таблиця А.2.

Перелік технічних активів:

| п\п | Виробник, модель | Серійний/інвентарний номер | Номер сертифікату з інформаційної безпеки (при наявності) | Фізичне розташування | Тип (згідно до технічної документації) | Основне функціональне призначення | Методи захисту інформації, що використовуються | Розробник, назва, версія (вбудованого програмного забезпечення) | Цінність активу | Відповідальний |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| | | | | | | | | | | |
| | | | | | | | | | | |

Таблиця А.3.

Перелік дистрибутивів програмних засобів:

| № п\п | Розробник | Назва | Версія | Місце встановлення (з переліку технічних активів) | Тип (згідно до програмної документації) | Основне функціональне призначення (згідно до програмної документації) | Методи захисту інформації, що використовуються | Цінність активу | Відповідальний |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | |
| | | | | | | | | | |

Таблиця А.4.

Перелік системних утиліт та засобів адміністрування:

| №п\п | Розробник | Назва | Версія | Місце встановлення (з переліку технічних активів) | Тип (згідно до програмної документації) | Основне функціональне призначення (згідно до програмної документації) | Методи захисту інформації, що використовуються | Цінність активу | Відповідальний |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | |
| | | | | | | | | | |

Таблиця А.5.

Перелік дозволеного програмного забезпечення:

| № п\п | Розробник | Назва | Версія | Місце встановлення (з переліку технічних активів) | Тип (згідно до програмної документації) | Основне функціональне призначення (згідно до програмної документації) | Методи захисту інформації, що використовуютьс я | Цінність активу | Відповідальний |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | |
| | | | | | | | | | |

Таблиця А.6.

Перелік засобів розробки, тестування:

| №п\п | Розробник | Назва | Версія | Місце встановлення (з переліку технічних активів) | Тип (згідно до програмної документації) | Основне функціональне призначення (згідно до програмної документації) | Методи захисту інформації, що використовуються | Цінність активу | Відповідальний |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | |
| | | | | | | | | | |

Таблиця А.7.

Перелік інформаційних активів:

| № п\п | Найменування активу | Місце розташування (з переліку інформаційних активів) | Чутливість до порушення конфіденційності | Чутливість до порушення цілісності | Чутливість до порушення доступності | Клас по типу можливого носія | Клас по доступу | Клас по можливості передачі | Відповідальний |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | |
| | | | | | | | | | |