Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Петренка Сергія Юрійовича*

академічної групи *125м-21-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методика впровадження СУІБ для охоронних підприємств*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	професор Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.	85	добре	

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Петренку Сергію Юрійовичу* **академічної групи** *125м-21-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Методика впровадження СУІБ для охоронних підприємств*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 31.10.2022 № 1200-с

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання, загальні теоретичні відомості, аналіз нормативно-правової бази, обґрунтування.	17.10.2022
Розділ 2	Обстеження охоронних підприємств та їх інформаційних активів, аналіз ризиків і загроз, політика безпеки, цілі заходів безпеки..	22.11.2022
Розділ 3	Поточні, капітальні витрати, економічна доцільність впровадження СУІБ.	15.12.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 14.09.2022р.

Дата подання до екзаменаційної комісії: 21.12.2022р.

Прийнято до виконання _____ Петренко С.Ю
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 121 с., 12 табл., 3 рис., 8 додатків, 12 джерел.

Об’єкт розробки: інформаційно-комунікаційна система охоронного підприємства

Предмет розробки: елементи пакету документів для впровадження СУІБ за стандартами ISO/IEC 27k.

Мета кваліфікаційної роботи: досягнення відповідності охоронних підприємств вимогам міжнародним стандартам.

У першому розділі розглянуто загальний стан питання, приведена причина впровадження СУІБ та розкрита її сутність, актуальність створення і проаналізована нормативна-правова база у сфері захисту інформації.

У другому розділі виконане загальне обстеження організації, обран процес (область діяльності), виконана ідентифікація ресурсів, що входять до обраної області діяльності, визначена цінність ресурсів. Виходячи з цих даних проведено розрахунок ризиків, підготовка політик, стандартів, положень, процедур для впровадження.

В економічній частині здійснені розрахунки капітальних витрат на внесення основних документів та визначена доцільність їх впровадження.

Практична значимість роботи полягає у підвищенні рівня конкурентоспроможності серед інших охоронних підприємств, можливість отримання підприємством після перевірки СУІБ сертифікату за стандартами ISO/IEC 27k.

ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, МОДЕЛЬ ЗАГРОЗ, ІНФОРМАЦІЙНІ ПОТОКИ, ЗАХИСТ ІНФОРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

ABSTRACT

Explanatory note: 121 p., 12 tables, 3 figures, 8 appendices, 12 sources.

Object of development: IST of security company

Subject of development: elements of the package of documents for the implementation of ISMS according to ISO/IEC 27k standards.

Purpose of qualification work: to achieve compliance of security companies with the requirements of international standards.

In the first section the general state of the issue is considered, the reason for the introduction of ISMS is given and its essence is revealed, the relevance of its creation and the regulatory framework in the field of information security is analyzed.

In the second section, a general survey of the organization was performed, the process (field of activity) was selected, the identification of resources included in the selected field of activity was performed, the value of resources was determined. Based on these data, the calculation of risks, preparation of policies, standards, regulations, procedures for implementation was carried out.

In the economic part, calculations of capital expenditures for the introduction of basic documents were carried out and the feasibility of their implementation was determined.

The practical significance of the work is to increase the level of competitiveness among other security companies, the possibility of obtaining a certificate according to ISO / IEC 27k standards after the ISMS inspection.

INFORMATION SECURITY POLICY, THREAT MODEL, INFORMATION FLOWS, INFORMATION PROTECTION, OBJECT OF INFORMATION ACTIVITY, INFORMATION SECURITY MANAGEMENT SYSTEM

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

БФП – багатофункціональний пристрій;

ЗКЗІ – засіб криптографічного засобу інформації;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІКС – інформаційно-комунікаційна система;

КС – комп'ютерна система;

КСЗІ – комплексна система захисту інформації;

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

СУІБ – система управління інформаційною безпекою.

ЗМІСТ

ВСТУП

У всьому комерційному, промисловому, охороні здоров'я, освіті та державному секторі, відсутність кібербезпеки стала головною проблемою для менеджерів і директорів. Через вразливості інформаційної безпеки багато компаній стали мішенями хакерів або зазнали витоку даних.

Кібербезпека підприємства – це захист цифрових активів та інформації організації. Вона може включати будь-що: від веб-сайту організації та онлайн-присутності до її внутрішніх мереж і даних. Щоб захистити ці активи, організації повинні мати комплексну стратегію кібербезпеки. Також стратегія повинна включати заходи для запобігання від кібератак, їх виявлення, коли вони відбуваються, та відповідного реагування на них. Кібербезпека – це не лише захист від хакерів; це також захист від випадкових зламів, крадіжки даних та інших типів атак.

Підприємства будь-якого розміру стурбовані виконанням замовлень, заснуванням майбутнього бізнесу, проблемами ланцюга постачання, а тепер і кіберзагрозам з усіх можливих джерел. Через внутрішні витоки та зовнішні атаки ІТ-фахівці ніколи не можуть відпочити, коли йдеться про ІБ підприємства. Захист інформації та ІТ-активів від несанкціонованого доступу може запобігти ризикам внутрішньої безпеки, спричиненим людською помилкою або незадоволеними працівниками.

Кібербезпека підприємства – це практика блокування точок доступу та виходу для даних, щоб усунути якомога більше потенційних загроз. Це означає розширення безпеки бізнесу за межі традиційних кордонів організації, включаючи хмарні середовища, ідентифікації користувача, безпеку постачальника та будь-що інше, пов'язане з наскрізним використанням. Деякі називають це моделлю безпеки з нульовою довірою. Це також вимагає фундаментальної зміни значення захисту даних, поставивши безпеку на один рівень з найбільш цінними активами компанії.

Якщо діяти інакше, це спричинить катастрофу в сучасному взаємопов'язаному світі, який наповнюється все більш різноманітнішими атаками.

Актуальність інформаційної безпеки підприємств особливо тих, хто надає послуги з інтегрування в об'єкти клієнтів, як обладнання для «розумного дому» або систем охоронно-пожежної сигналізації та відеоспостереження є дуже важливим. Їх важливість полягає у тому, що інформаційна безпека цих інтегрованих систем так чи інакше напряму залежить вже від інформаційної безпеки того підприємства, які надала ці послуги. Для охоронних підприємств важлива постійна та безперервна доступність для моніторингу об'єктів клієнтів, і вона також може залежити від загальної інформаційної безпеки. І загальний рівень безпеки в таких підприємствах повинен бути вищим або як мінімум рівний тому, послуги які вона надає. Цей рівень, повинен гарантувати, що матеріальні та інформаційні цінності клієнтів будуть знаходитись під надійною охороною. В нашій державі на поточний момент, підвищення загальної інформаційної безпеки можливо здійснити за допомоги комплексної системи захисту інформації або Системою управлінням інформаційної безпеки.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальний стан питання

У сучасному світі інформація стає стратегічним ресурсом, одним із основних багатств економічно розвиненої держави. Швидке вдосконалення інформатизації, проникнення її у всі сфери життєво важливих інтересів особистості, суспільства та держави викликали, крім безперечних переваг і появу низки суттєвих проблем. Однією з них стала потреба захисту інформації. Враховуючи, що у наш час економічний потенціал дедалі більше визначається рівнем розвитку інформаційної структури, пропорційно зростає потенційна вразливість економіки від інформаційних впливів.

Поширення комп'ютерних систем, об'єднання в комунікаційні мережі посилює можливості електронного проникнення у них. Проблема комп'ютерної злочинності у всіх країнах світу, незалежно від їхнього географічного положення, викликає необхідність залучення дедалі більшої уваги та сил громадськості для організації боротьби даним видом злочинів. Особливо широкий розмах набули злочинів в автоматизованих банківських системах та в електронній комерції. За закордонними даними, втрати у банках внаслідок комп'ютерних злочинів щорічно становлять багато мільярдів доларів. Хоча рівень впровадження нових інформаційних технологій у практику настільки значний, комп'ютерному злочину з кожним днем дають себе знати дедалі більше, а захист держави й суспільства від них перетворилася на складне завдання для компетентних органів. Кожен збій роботи комп'ютерної мережі це не лише "моральний" збиток для працівників підприємства та мережевих адміністраторів. У міру розвитку технологій електронних платежів, "безпаперового" документообігу та інших, серйозний збій мереж може просто паралізувати роботу цілих корпорацій та банків, що призводить до відчутних матеріальних втрат. Не випадково, що захист даних у комп'ютерних

мережах стає однією з найгостріших проблем на сьогоднішній день. Однією з основних причин, пов'язаних з комп'ютерами, є недостатня освіченість у сфері безпеки. Тільки наявність деяких знань у сфері безпеки може припинити інциденти та помилки, забезпечити ефективне застосування заходів захисту, запобігти злочину або своєчасно виявити підозрюваного.

Управління інформаційною безпекою (ІБ) – невід'ємна частина управління будь-якою сучасною організацією в цілому, незалежно від її розміру та сфери діяльності. Управління ІБ – складний безперервний процес, перед яким стоїть безліч цілей і завдань, що забезпечують, допоміжними по відношенню до основних бізнес-цілей та завдань організації. Вони формулюються у різних документах організації: концепціях, стратегіях, політиках, стандартах, інструкціях тощо.

Процес управління ІБ розпадається на тісно взаємопов'язані підпроцеси, кожен з яких робить істотний внесок у досягнення загальних цілей управління ІБ. Об'єктами управління в рамках цих підпроцесів є активи, ризики ІБ, інциденти ІБ, безперервність бізнесу, зміни, удосконалення та багато іншого. Від ефективності та результативності кожного з цих підпроцесів залежать загальна ефективність та результативність усієї діяльності[1].

1.2 Визначення сутності СУІБ

Управління інформаційною безпекою – це циклічний процес, що включає усвідомлення ступеня необхідності захисту інформації та постановку завдань; збір та аналіз даних про стан інформаційної безпеки в організації; оцінку інформаційних ризиків; планування заходів щодо обробки ризиків; реалізацію та впровадження відповідних механізмів контролю, розподіл ролей та відповідальності, навчання та мотивацію персоналу, оперативну роботу щодо здійснення захисних заходів; моніторинг функціонування механізмів контролю, оцінку їх ефективності та відповідні коригувальні впливи.

Відповідно до ISO 27001, система управління інформаційною безпекою (СУІБ) – це «та частина загальної системи управління організації, яка ґрунтується на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід та вдосконалення інформаційної безпеки». Система управління включає організаційну структуру, політики, планування, посадові обов'язки, практики, процедури, процеси і ресурси.

Створення та експлуатація СУІБ вимагає застосування такого ж підходу, як будь-яка інша система управління. Процесна модель, що використовується в ISO 27001 для опису СУІБ, передбачає безперервний цикл заходів: планування, реалізація, перевірка, дія (ПРПД).

Процес безперервного вдосконалення зазвичай потребує початкового інвестування: документування діяльності, формалізація підходи до управління ризиками, визначення методів аналізу та виділення ресурсів. Ці заходи застосовуються для приведення циклу в дію. Вони не обов'язково мають бути завершені, перш ніж будуть активізовані стадії перегляду.

На стадії планування забезпечується правильне завдання контексту та масштабу СУІБ, оцінюються ризики інформаційної безпеки, пропонується відповідний план обробки цих ризиків. На стадії реалізації впроваджуються прийняті рішення, які були визначені на стадії планування. На стадіях перевірки та дії посилюють, виправляють та вдосконалюють рішення щодо безпеки, які вже були визначені та реалізовані.

Перевірки можуть проводитись у будь-який час та з будь-якою періодичністю залежно від конкретної ситуації. У деяких системах вони мають бути вбудовані в автоматизовані процеси з метою забезпечення негайного виконання та реагування. Для інших процесів реагування потрібне лише у випадку інцидентів безпеки, коли в інформаційні ресурси, що захищаються, були внесені зміни або доповнення, а також коли відбулися зміни загроз і вразливостей. Необхідні щорічні або інші періодичності перевірки або аудити, щоб гарантувати, що система управління в цілому досягає своїх цілей.

1.3 Обґрунтування необхідності впровадження СУІБ у підприємства

В Україні є власний стандарт з кібербезпеки, а саме атестат відповідності комплексного захисту інформації (КСЗІ). Але нажаль, деякі норми в КСЗІ застаріли, а необхідність відповідати цьому стандарту змушує компанії та підприємства будувати повноцінні системи безпеки.

У свою чергу, замість КСЗІ можуть запропонувати ISO/IEC 27001 – один із найвідоміших стандартів у сфері систем управління інформаційною безпекою. По суті, це лише набір політик і процедур, згідно з якими компанія захищатиме свої інформаційні активи від навмисного або випадкового неправильного використання, втрати чи пошкодження.

У підході ISO до стандартизації від самого початку закладений принцип, згідно з яким жодна система не може постійно перебувати в ідеальному стані. Тому там, де в КСЗІ вказані чіткі робочі схеми, ISO містить лише рекомендації. Для отримання ISO/IEC 27001 не обов'язково навіть на момент сертифікації дотримуватися всіх вимог зазначеного стандарту – достатньо взяти на себе зобов'язання протягом року доробити все необхідне.

Різниця між КСЗІ від СУІБ досить чітка. КСЗІ – сукупність організаційних та інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу. ISO/IEC 27001 – сертифікат відповідності бізнес-процесів підприємства міжнародному стандарту, який має високу гнучкість для впровадження його у майже будь-яке підприємство та може підвищити його імідж та інтерес до нього, як в так і поза межами держави. Хоча ці сутності не замінюють одна одну, вони можуть доповнюватись, і тим самим підвищити загальну ІБ організацій[2].

Отже актуальність впровадження СУІБ на даний момент:

1) Для прийняття зважених рішень з управління ризиками щодо стратегічних бізнес-завдань і забезпечувати певний рівень надійності.

2) Для фокусуванні уваги на критичній інформації в будь-якій формі: цифровій, паперовій, відео-, голосовій.

3) Для удосконалення показників інформаційної безпеки і звітності для обґрунтування поточних і зростаючих інвестицій в ефективні заходи контролю.

4) Для прийняття всебічного бачення ризиків, заснованого на впровадженні заходів контролю.

5) У майбутньому цілком вірогідний сценарій обов'язкового отримання сертифікату за стандартами ISO/IEC 27001 для підприємств.

1.4 Аналіз нормативно-правової бази

Так як СУІБ впроваджується у підприємства з надання охоронних послуг, то слід враховувати те, що воно вже повинно мати ліцензію на свою діяльність, а саме «ПОСТАНОВА від 18 листопада 2015 р. №960 Про затвердження Ліцензійних умов провадження охоронної діяльності».

Ліцензійні умови мають свої організаційні, кадрові та технологічні вимоги, які можуть частково поліпшити умови впровадження СУІБ за стандартами ISO/IEC 27k через вже сформовані правила безпеки на підприємстві і які не будуть суперечити одна одній.

Нормативно-правова база для інспекції та оцінки діяльності з управління інформаційною безпекою СУІБ – це набір міжнародних стандартів, що узагальнюють кращі практики, розроблені фахівцями з різних організацій та різних країн. Міжнародна організація зі стандартизації (ISO) і Міжнародна електротехнічна комісія (МЕК) утворюють спеціалізовану систему всесвітньої стандартизації. Всю цю необхідну для подальшої роботи можна зобразити у виді схеми зображеної на рисунку 1.1.

Рисунок 1.1 – Структура нормативно-правової бази

Для виконання роботи, слід враховувати такі закони, постанови та положення:

1) Конституція України – основний документ, який визначає державний устрій, систему та принципи, за якими функціонують державні органи, виборчу систему, права та обов'язки уряду, суспільства та громадян.

2) Закон України «Про інформацію» – визначає найважливіші методи доступу, використання, розповсюдження та зберігання інформації. Цей закон відображає право особам для отримання інформації щодо всіх аспектів суспільного та регіонального життя в інформаційній системі України, визначає статус учасників інформаційного спілкування, регулює доступ до інформації та забезпечує її захист, а також дає захист особистості та спільноту від неправдивої інформації.

3) Закон України «Про захист персональних даних» – закон регулює правовідносини, які відносяться до захисту та обробки персональних даних, і направлений на захист основних прав і свобод людей та громадян, включаючи права на приватне життя, пов'язане з обробкою їх персональних даних.

4) Закон України «Про захист інформації в інформаційно-комунікаційних системах» – закон, який здійснює нагляд за взаємовідносинами у галузі захисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, регулює об'єкти та суб'єкти захисту, які відносяться до системи, зі встановленням зв'язку між власниками системи, користувачами та власниками даних[7].

5) Закон України «Про електронний цифровий підпис» – закон визначає правовий статус електронних цифрових підписів та регулює порядок взаємодії в результаті використання електронних цифрових підписів. Він не застосовується до відносин, що виникають внаслідок використання інших типів електронних підписів, включаючи зображення, які переведені в електронний варіант з власноручно написаними підписами.

6) Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» від 29.03.2006 № 373;

7) Постанова Кабінету міністрів України « Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19.10.2016 №736.

З ціллю забезпечення безпеки інформації слід враховувати рекомендації, вимоги та стандарти які описані в таких документах як:

- ДСТУ ISO/IEC 27001:2015 – Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою – стандарт створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ) [3].

- ДСТУ ISO/IEC 27002:2015 – Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT) – міжнародний стандарт розроблено для організацій для використання як

довідкової інформації щодо вибору заходів безпеки під час впровадження СУІБ на базі ISO/IEC 27001 або як настанову для організацій, які впроваджують загальноприйняті заходи інформаційної безпеки. Цей стандарт також призначено для використання в розробленні настановних документів з управління інформаційною безпекою, специфічних для промисловості та організацій, з урахуванням специфічних ризиків інформаційної безпеки їх середовища [4].

- ДСТУ ISO/IEC 27005:2019 – Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT) – стандарт надає настанови для управління ризиками інформаційної безпеки. Підтримує основні концепції, визначені в ISO/IEC 27001, і розроблений для сприяння задовільному впровадженню інформаційної безпеки на основі підходу з управління ризиками [5].

Під час виконання роботи будуть використовуватись такі терміни та визначення:

Інформація з обмеженим доступом – інформація з правами доступу до якої обмежено встановленими певними правовими нормами і\або правилами [10].

Конфіденційна інформація – є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом [10].

Інформаційний ресурс – сукупність документів у інформаційних системах. Документом Закон України «Про інформацію» визначає формат отримання, зберігання, розповсюдження та використання інформації шляхом її запису на магнітні, кіно-, відео-, фото- чи інші носії інформації. Поняття "документи" має важливе значення, оскільки документи є частиною джерела інформації і мають юридичні наслідки. Інформація з обмеженим доступом (за умови захисту) може оброблятися, передаватися та зберігатися ресурсами ІКС, такими як сервери, робочі станції, пристрої зберігання даних, периферія (принтери, з'ємні носії),

мережеве обладнання, системи та програмне забезпечення, яке з'єднане з об'єктами ІКС для взаємодії з інформацією[10].

1.5 Постановка задачі

Після отримання знань щодо сутності СУІБ та її необхідності впровадження у підприємство, було проаналізовано нормативну правову базу. Занурюючись у стандарти ISO/IEC 27k і роблячи все так, як це рекомендовано в них, головне не забувати о другій частині процесу, а саме – про відповідність до державного законодавства. Одне іншому не повинно суперечити, і виконувати треба обидві вимоги одночасно. Також для охоронних підприємств важливо мати оптимальний рівень інформаційної безпеки, але використання КЗСІ для вирішення цієї проблеми може бути дуже складним та витратним для і них. Тому маючи саме міжнародні стандарти серії ISO/IEC 27k, охоронне підприємство зможе не тільки вирішити проблему з загальним підвищення інформаційної безпеки, а також і підвищити сам імідж та конкурентоспроможність, особливо коли таких підприємств на даний час є чимало. Також такі інвестиції можуть зіграти важливу роль у майбутньому, тому що все більше різних міжнародних підприємств можуть розташовуватись на території нашої держави, а для них такий сертифікат може стати гарантом для подальшого співробітництва.

Мета цього аналізу – надання повної інформаційної бази у можливості підвищення безпеки інформації на підприємствах та вирішення методу, яким вона може здійснитись з урахуванням всіх переваг.

1.6 Висновок

У цьому розділі було описано загальний стан питання щодо необхідності у підвищені захисту інформації для підприємств, які займаються охоронною діяльністю.

Також немало уваги приділено до самої сутності СУІБ за стандартами ISO/IEC 27k та доцільності в їх впроваджені. Усе це було закріплене нормативно-правовою базою задля дотримання державних законів, які так чи інакше стосуються захисту інформації, ліцензійних умов охоронної діяльності та безпеки інформації. Хоча вона оновлюється та актуалізується до поточних сучасних проблем, її дотримання займає першочергове місце.

Було обґрунтоване вирішення, щодо вибору, яким чином можна підвищити, як загальну інформаційну безпеку охоронних підприємств, так і їх конкурентоспроможність задля більш успішного ведення бізнесу у майбутньому.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Попередня підготовка да затвердження рішення створення СУІБ

Затвердження рішення про створення СУІБ. Рішення про створення СУІБ повинно прийматися керівниками компанії. Відділ захисту інформації (служба інформаційної безпеки) реалізовує початок даного процесу. У разі вирішення прийняття системи менеджменту інформаційної безпеки керівництво повинно усвідомлювати кінцеву ціль даного заходу та важливість сертифікації для бізнесу[10].

Попередня підготовка, а саме наступним етапом буде створення робочої групи та призначення керівника. До її складу мають увійти: представники керівництва організації, представники відділів, старші спеціалісти, що забезпечують інформаційну безпеку в компанії. Дані співробітники повинні усвідомленні про механізми систем менеджменту. До складу робочої групи можуть входити також консультанти, що спеціалізуються на питаннях СУІБ. Робоча група повинна мати всю необхідну нормативно-методичну базу для успішного створення, відповідно вимогам [10].

Також всі подальші етапи щодо реалізації СУІБ в підприємство можна зобразити у вигляді схеми процесів. Схема на рисунку 2.1 наглядно демонструє загальні етапи та документи стандартів які їх стосуються.

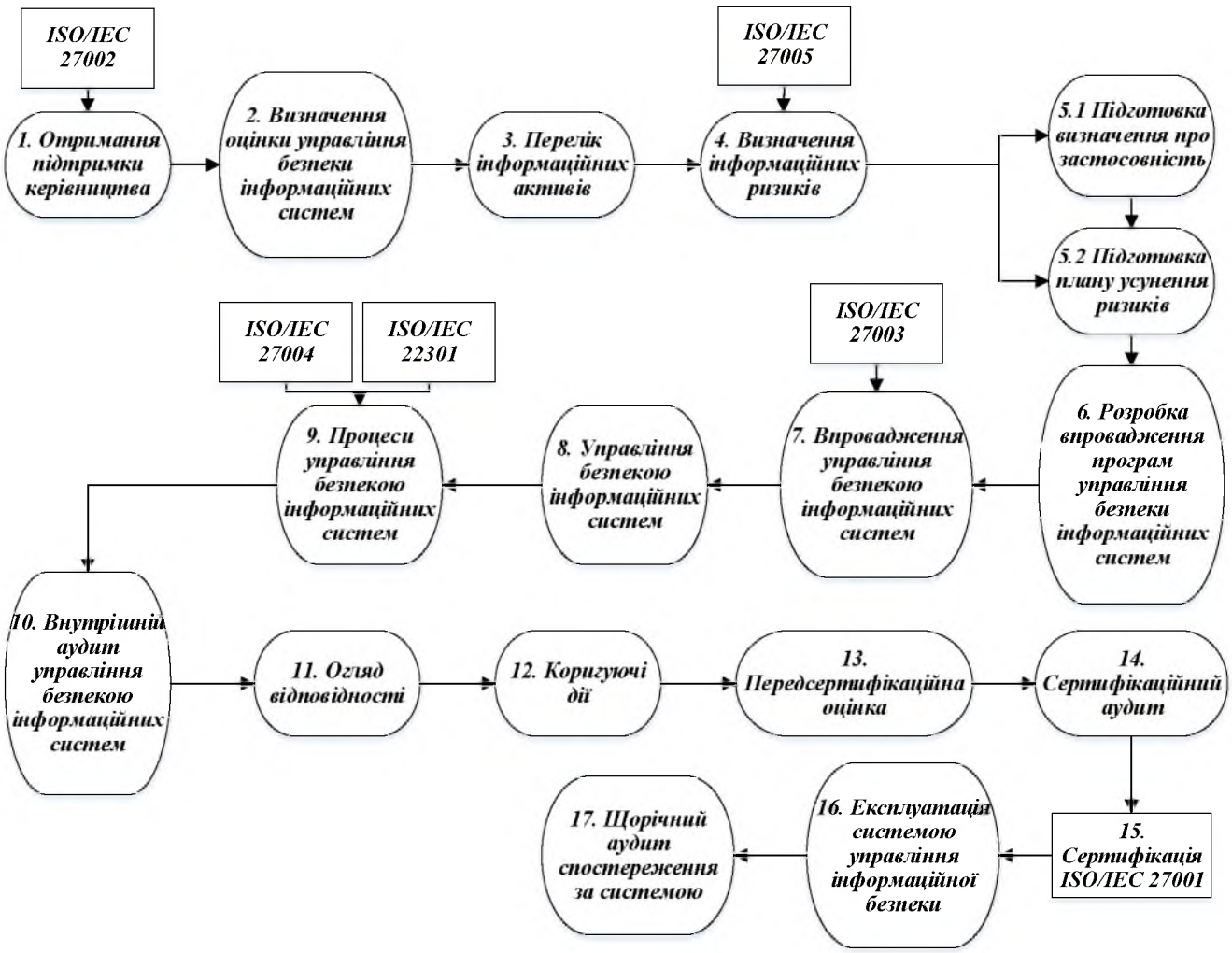


Рисунок 2.1 – Схема процесу реалізації СУІБ

2.2 Визначення цінності інформації на охоронних підприємствах

Цінність інформації безпосередньо залежить від ступеню захисту конфіденційності, цілісності та доступності в залежності від її типу, цілей, для яких вона вказується, та ризиків, яким вона наражається. Збереження конфіденційності, доступності та цілісності (інформації є головною метою захисту інформації. У охоронній діяльності конфіденційність об'єктів та надання охоронних послуг залежить від збереження конфіденційності персональної інформації клієнтів та їх

об’єктів. Щоб зберегти конфіденційність, також повинні бути вжиті заходи щодо збереження цілісності даних, якщо це може бути єдиною причиною, через яку може бути порушена цілісність даних управління доступом, журналів аудиту та інших системних даних способами, що дозволяють порушенням конфіденційності відбуватися чи залишатися непоміченими. Дотримання цілісності інформації, допомагає правильно зреагувати пульту охорони на підозрілі випадки, або надавати повну інформацію правоохоронним органам при необхідності. Так само високий рівень доступності є особливо важливим атрибутом системи охорони, через те що потрібен постійний моніторинг за об’єктами, які знаходяться під охороною цього підприємства.

Існують додаткові чинники, які формують мету захисту інформації для підприємств з надання охоронних послуг. Вони включають:

1) Дотримання законодавчих зобов'язань, закріплених у чинних законах та положеннях про захист даних, що захищають права об'єктів з надання ним охоронних послуг.

2) підтримка встановлених у сфері ІКС рекомендованих методів забезпечення захисту інформації;

3) підтримання підзвітності на рівні окремої людини та організації;

4) підтримка здійснення систематичного управління ризиками у таких організаціях;

5) задоволення вимог захисту, виявлених у загальних ситуаціях;

6) зниження експлуатаційних витрат за рахунок сприяння ширшому використанню технології в безпечній, надійній і добре керованій манері, яка підтримує, але не обмежує, поточну діяльність;

7) управління електронними інформаційними системами у середовищі, належним чином захищеною від загроз.

Також існує кілька типів інформації, конфіденційність, цілісність і доступність до якої повинні бути захищені:

- персональна інформація як клієнтів так і співробітників;

- плани будівель або приміщень об’єктів замовників;

- інформація розміщення сповіщувачів та ППКОП(Прилад приймально-контрольний охоронно-пожежний) та їх спосіб підключення на об’єктах замовників;

- інформація розміщення систем відеоспостереження та їх технічних засобів обробки та зберігання записів на об’єктах замовників;

- данні для входу з правами адміністратора через клавіатуру, підключену до ППКОП;

- дані журналів та систем моніторингу щодо загального стану роботи пристроїв охорони на об’єктах;

- інформація щодо розташування груп швидкого реагування.

2.3 Легенда та структура організації

Задля подальшої роботи, буде розглядатися типове приватне охоронне підприємство, яке здійснює фізичну охорону об’єктів усіх форм власності. Воно виконує роботи з проектування та монтажу систем охоронної та пожежної сигналізації, систем пожежогасіння, відеоспостереження, систем контролю доступу та їх обслуговування, тобто матиме повний обсяг послуг, яке може надавати таке підприємство

Діяльність такої організації пов’язана з взаємодією як з юридичними, так і фізичними особами, надаючи їм відомості щодо наявних видів послуг.

На підприємстві циркулює інформація, що містить конфіденційну інформацію клієнтів і персональні дані працівників.

Основний робочий склад працівників охоронного підприємства функціонує 5 днів на тиждень, з 8.30 до 17.30.

Офіс охронних підприємств знаходиться у частині нежилої багатоповерхової будівлі або займає окрему будівлю. Навколо будівлі встановлений паркан, на

території підприємства паркувальна зона, в'їзд то якої через шлакбаум, сама територія охороняється силами самого підприємства.

Офіс оснащений системою контролю та управління доступом на кожний вхід. Кожний працівник компанії має магнітний ключ, за допомогою якого здатний пройти до офісного приміщення свого відділу. Пропуск до інших приміщень здійснюється за попереднім узгодженням, або через впізнання особи через камеру відеоспостереження або домофоном за якими веде моніторинг один з диспетчерів.

Пропуск сторонніх осіб на територію здійснюється лише із узгодженням з керівництвом.

Типове охоронне підприємство складається з наступних структурних підрозділів:

- генеральний директор
- секретар генерального директора;
- фінансовий директор(бухгалтерія, юридичний відділ, відділ кадрів);
- завідуючий автопарком(водії);
- завідуючий відділом фізичної охорони(групи швидкого реагування, фізична охорона);
- завідуючий відділом пожежної сигналізації;
- завідуючий відділом охоронної сигналізації;
- завідуючий технічний відділом(системний адміністратор);
- завідуючий відділом позавідомчої охорони(оператори та диспетчери пульту, охоронці).

Організаційна структура класифікується, як лінійно-функціональна. Відповідно з такою структурою кожен співробітник організації підпорядковується керівництву свого функціонального блоку, а керівники відділів і команд – генеральному директору.

Схема організаційної структури підприємства знаходиться у додатку В

2.4 Обґрунтування вибору бізнес-процесу організації

Перед впровадженням СУІБ повинно визначитись, чи потрібно підприємству впроваджувати її на все підприємство, та чи достатньо ресурсів для цієї реалізації. Стандарт має гнучкість, тому при необхідності СУІБ можна впровадити у конкретні бізнес-процес/и підприємства, а у майбутньому при необхідності розширювати саму її область.

Тому до моменту затвердження області дії, що буде сертифікуватися, необхідно проаналізувати всі існуючі бізнес-процеси у компанії і вибрати з нього найбільш критичні процеси з точки зору інформаційної безпеки. Це може бути обробка та зберігання даних клієнтів, фінансові операції, робота з чутливими даними чи щось інше.

У процесі вибору важливо врахувати такий зовнішній фактор, як опитування клієнтів, а саме у якій галузі діяльності вашої компанії клієнти все більше цікавляться наявністю сертифікатів на відповідність національним та/або міжнародним стандартам у сфері інформаційної безпеки[10].

Отже насамперед область дії СУІБ повинен охоплювати саме той відділ або відділи, у яких підприємство використовує найбільші інформаційні ресурси, або найбільш цінну інформацію для бізнес-процесів, як для себе, так і для клієнтів, яким вона надає послуги.

В охоронних підприємствах, ті бізнес-процеси, які беруть на себе фізичну охорону, або завідуванням автопарку брати в охоплення СУІБ має низький рівень необхідності, через те що там обробляється мінімальна інформація про клієнтів або її взагалі немає. Дані працівники використовують тільки лінії зв'язку(через рації, телефони тощо), для швидкого реагування при надані послуг, а інших процесів з використанням різних технічних засобів для обробки, зберігання інформації, окрім звітів немає.

Технічний відділ потрібен підприємству задля постійного обслуговування усієї обчислювальної системи та неперервної її роботи. Тому інформація цього відділу стосується тільки самого підприємства і зацікавленість або будь-яка взаємодія з клієнтами мінімальна або взагалі відсутня.

Відділ фінансів, яка охоплює бухгалтерію, відділ кадрів та юридичний відділ вже може бути охоплений, тому що оброблювальна інформація у ньому, а саме бухгалтерські звіти, персональні дані як працівників підприємства та клієнтів, контрактні угоди та інше має цінність як для підприємства так і для клієнтів. Для майбутніх документів, які стосуються СУІБ можна виділити записи навчання, навичок та кваліфікації всіх працівників підприємства. Це все зберігається та обробляється як у паперовому, так і електронному вигляді, вона має загрози конфіденційності, але втрата її більш вагома буде саме для підприємства ніж для її клієнтів.

Відділ пожежної сигналізації надає послуги з проектування, монтажу та обслуговування систем пожежної сигналізації. Інформація яка обробляється під час надання цих послуг, також обробляється у паперовому та електронному вигляді. Основна її унікальна цінність це плани об’єктів замовників. Порушення конфіденційності такої інформації, порушує саме її, але як правило на такі плани мають низьку цінність для зловмисників, через її малу інформативність. Тому важливість її захисту для клієнтів теж має достатньо низьку зацікавленість у більшості випадків.

Відділ охоронної сигналізації надає послуги з проектування, монтажу та обслуговування систем охоронної сигналізації, систем відеоспостереження. Даний відділ обробляє та зберігає паперову та електронну інформацію, яка безпосередньо стосується захисту та безпеки як майна так і інших цінностей клієнтів. Плани об’єктів, конфігурації встановлених технічних засобів та їх стан повинен бути відомий тільки працівникам та клієнту. Втрата, зкомпроментованість та розголошення цієї інформації, може привести як до значних втрат з боку клієнта, так і втрати довіри до підприємства та фінансових значних витрат з обох сторін.

Відділ позавідомчої охорони являє собою інформаційний центр, який корегує та надає інформацію підрозділам фізичної охорони та обслуговуючих охоронно-пожежної сигналізації щодо стану та випадків, які можуть випливати при виконанні обов'язків. Він повинен працювати 24 години на тиждень задля постійного моніторингу за об'єктами клієнтів підприємства. Інформація у більшості випадків являє собою електронну інформацію, доступність до якої не повинно бути під загрозою. У більшості випадків, доступ постороннім особам до приміщень даного підрозділу відсутній, також як і будь-яка взаємодія з клієнтами.

Після аналізу роботи кожного з підрозділів підприємства та їх бізнес-процесів, які потенційно можуть бути розглянуті для сертифікування, його можна зобразити у виді таблиці 2.1 та проранжувати їх за рівнем значимості як для підприємства так і для клієнта(де 1 – низький, 4 – максимальний), щоб остаточно обрати область дії СУІБ[10].

Таблиця 2.1 – для визначення області діяльності СУІБ підприємства

№	Назва відділу	Критичність з точки зору підприємства, від 1 до 4	Важливість процесу з точки зору клієнта від 1 до 4
1	Відділ позавідомчої охорони	3	2
2	Відділ охоронної сигналізації	3	3
3	Відділ пожежної сигналізації	2	2
4	Відділ фінансів(Юридичний, Бухгалтерія, Відділ кадрів)	3	2
5	Відділ фізичної охорони	1	1
6	Технічний відділ	2	1

Отже за даними с таблиці може бути вирішено у якій області або областях впроваджувати СУІБ. Підприємство може обрати ту кількість відділів, на яку трата ресурсів та фінансів буде для неї оптимальна. В подальших етапах при переліку інформаційних активів буде розглянутий відділ охоронної сигналізації.

2.5 Необхідні складові документаційного забезпечення СУІБ

Список, що містить мінімальний набір документів та облік записів, необхідні для ISO/IEC 27001 версії 2015 року наведений у таблиці 2.2–2.3. Також ті документи, які виходять з додатку А в цьому стандарті(номер пункту починається з неї) є необов'язкові, якщо підприємство вирішує, що не буде ніяких ризиків або інших вимог для використання СУІБ.

Цей список не є остаточним і може доповнюватись або змінюватись, тому що сам стандарт має гнучкість для використання альтернативних документів. Згодом при необхідності підприємство може додавати до списку інші документи, які так чи інакше будуть підвищувати рівень ІБ та основуватися на вимогах СУІБ та досвіду.

Таблиця 2.2 – мінімальний набір документів

№	Документи	Задовольняє номер пункту стандарту
1	Визначення сфери застосування системи управління інформаційною безпекою	4.3
2	Політика інформаційної безпеки	5.2, 6.2
3	Оцінка ризиків інформаційної безпеки	6.1.2
4	Положення щодо застосовності	6.1.3 d)
5	План оброблення ризиків	6.1.3 e), 6.2
6	Оцінювання ризиків	8.2
7	Процедура управлінням документами	7.5
8	Процедура управлінням записами	7.5
9	Внутрішній аудит	9.2
10	Невідповідності й корегувальні дії	10.1
11	Визначення ролей та обов'язків	A.7.1.2, A. 13.2.4
12	Інвентаризація ресурсів СУІБ	A.8.1.1
13	Припустиме використання ресурсів СУІБ	A.8.1.3
14	Політика контролю доступу	A.9.1.1

Таблиця 2.3 – мінімальний набір записів

№	Записи	Номер пункту стандарту
1	Записи про рівень підготовки, навички, досвід та кваліфікації	7.2
2	Моніторинг та вимірювання результатів	9.1
3	Програма внутрішнього аудиту	9.2
4	Результати внутрішніх аудитів	9.2
5	Результати аналізу з боку керівництва	9.3
6	Результати коригуючих дій	10.1

2.6 Процедури управління документообігом

Документообіг є в кожному підприємстві і як правило для нього використовується загальноприйнятий стандарт по його оформленню та змісту. Створення цих стандартів в більшості випадків не зв'язано з побудовою СУІБ, але це значно йому допоможе. Після ухвалення та підписання генеральним директором наказу, щодо побудови та впровадження СУІБ, майбутнім розподіленням обов'язків і ролей у цих процесах, саме стандарт який вже може існувати на підприємстві, дія якого полягає встановлювати правила написання та оформлення дозволить поліпшити роботу над послідуючими документами. Для тих же підприємств, які не мають прийнятий внутрішнього стандарту щодо оформлення документацій, слід у першу чергу почати з нього. Тому що у майбутньому це заощадить багато часу та фінансів, при переоформленні вже готових документів, в особливості у тому випадку, коли на ними працювало декілька людей. Для підприємств, які надають охоронні послуги, зазвичай мають свої загальноприйняті правила щодо створення документів.

Як правило в цей стандарт може складатися з 2-3 сторінок, з правилами, яким шрифтом слід користуватися та його розміром. Більшість цих загальних питань щодо форматування та оформлення документів повинно також відповідати ДСТУ 4163:2020 «Уніфікована система організаційно-розпорядчої документації. Вимоги оформлення документів» та може доповнюватись. А доповнюватись має саме

цілями процедури при роботі з внутрішніми документами як вхідними так і вихідними. Правилами документообігу та інформування співробітників. Також одним із важливіших, це те що кожен документ повинен мати свій ідентифікаційний номер, який дозволяє забезпечити класифікацію при їх зберіганні, спрощує процес відсилки до них і поліпшує пошук.

2.7 Аналіз інформаційних активів середовища

Охоронне підприємство так чи інакше має свою обчислювальну систему, яка буде складатися з основних да допоміжних технічних засобів. Основні засоби обробки та збереження інформації будуть являти собою мережу з комп'ютерів, найчастіше підключених за топологією «зірка». Кожний відділ має як мінімум по парі ПК та одному БФП. Також підприємство повинно мати свій сервер, як мінімум для зберігання даних з камер відеоспостереження, яке необхідно за законодавством для такого типу організацій. Основна інформація, яка циркулює на охоронному підприємстві описана в таблиці 2.4. Схема інформаційних потоків охоронного підприємства зображена у вигляді схеми на рисунку 2.2.

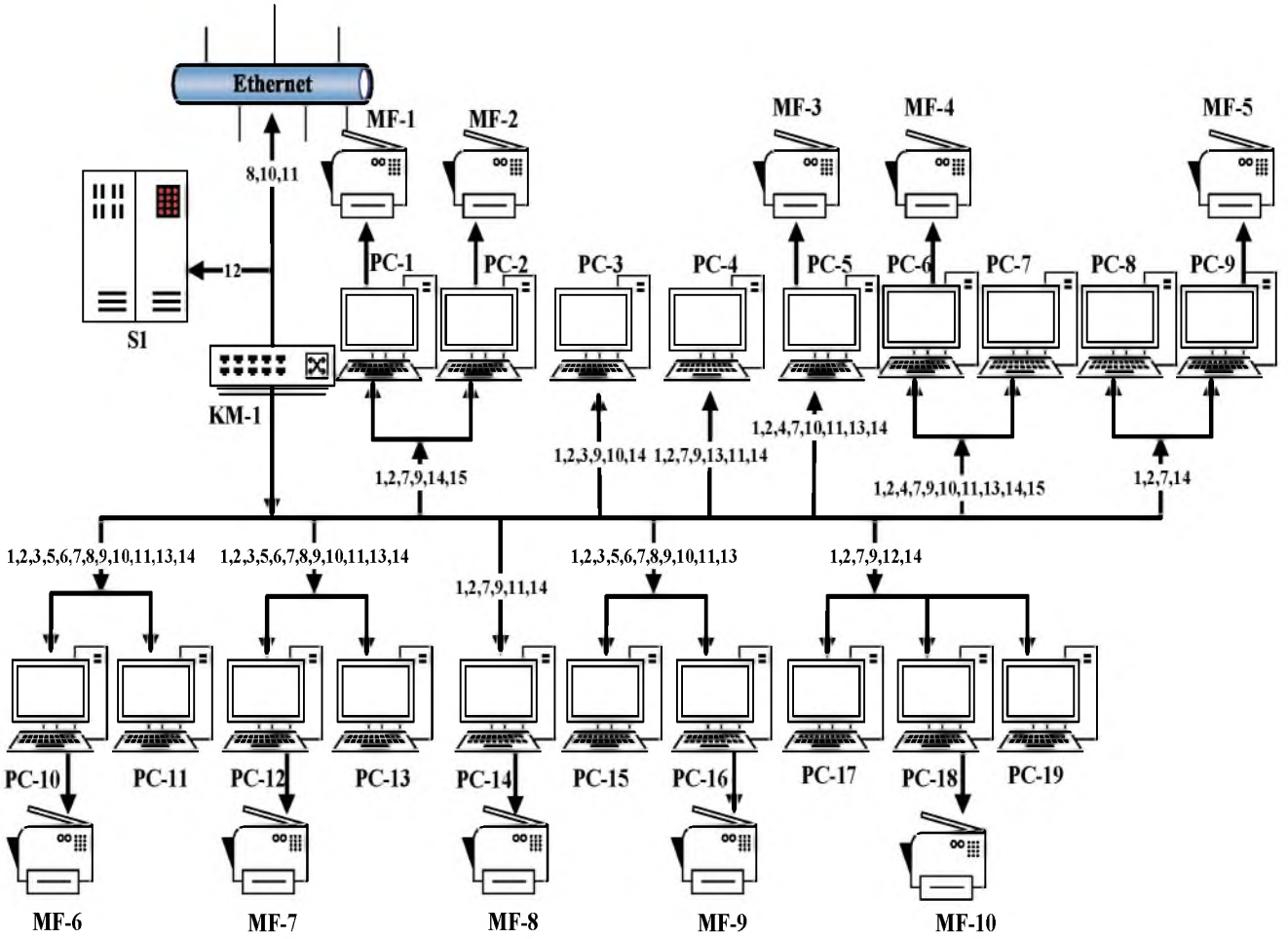


Рисунок 2.2 – Схема інформаційних потоків

Ролі та користувачі ІС вказані у таблиці 2.4.

Таблиця 2.4 – Користувачі ІКС

Використовує пристрій	Посада	Відділ	Роль у системі
PC-1	Генеральний директор	Керуючий	Користувач
PC-2	Секретар генерального директора		Користувач
PC-3	Завідуючий	Автотранспорту	Користувач
PC-4	Завідуючий	Фізичної охорони	Користувач
PC-5	Фінансовий директор	Відділ фінансів	Користувач
PC-6	Завідуючий	Юридичний	Користувач
PC-7	Юрист		Користувач
PC-8	Завідуючий	Кадрів	Користувач
PC-9	Працівник		Користувач
PC-10	Завідуючий(менеджер)	Охоронної сигналізації	Користувач
PC-11	Старший працівник		Користувач
PC-12	Завідуючий(менеджер)	Пожежної сигналізації	Користувач

Продовження таблиці 2.4

Використовує пристрій	Посада	Відділ	Роль у системі
PC-13	Старший працівник		Користувач
PC-14	Завідуючий(системний адміністратор)	Технічний	Адміністратор
PC-15	Завідуючий	Бухгалтерський	Користувач
PC-16	Бухгалтер		Користувач
PC-17	Завідуючий	Позавідомчої охорони	Користувач
PC-18	Оператор пульту		Користувач
PC-19	Диспетчер		Користувач

Основна інформація, яка циркулює на охоронному підприємстві описана в таблиці 2.5.

Таблиця 2.5 – Інформація яка циркулює в охоронному підприємстві

№	Інформація	Режим доступу	Правовий режим	Відділи, які використовують інформацію	Місце зберігання
1	Зарплатні відомості	Відкрита	немає	Всі відділи	РС Б
2	Особисті справи співробітників	ІзОД	Конфіденційна інформація	Всі відділи	РС ВК
3	Клієнтська база	ІзОД	Конфіденційна інформація	ВП, ВО, ВФО	РС ВП, ВО, ВФО
4	Бухгалтерські звіти	ІзОД	Конфіденційна інформація	ФД,Б	РС Б
5	Вхідні Плани об’єктів замовників	ІзОД	Конфіденційна інформація	ВП, ВО	РС ВП,ВО
6	Вихідні Плани об’єктів замовників	ІзОД	Конфіденційна інформація	ВП,ВО	РС ВП,ВО
7	Робочий графік	Відкрита	немає	Всі відділи	РС ФД, Б, ВП, ВО, ТВ, ЗА, ФВО
8	Дані замовлень	ІзОД	Конфіденційна інформація	ВП,ВО	РС ВП,ВО
9	Трудові договори	ІзОД	Конфіденційна інформація	Всі відділи	РС ВК
10	Договори про надання послуг	ІзОД	Конфіденційна інформація	ФД, Б, ВП, ВО, ВФО	РС ВП,ВО

Продовження таблиці 2.5

№	Інформація	Режим доступу	Правовий режим	Відділи, які використовують інформацію	Місце зберігання
11	Договори поставок обладнань	ІзОД	Конфіденційна інформація	ФД, Б, ВП, ВО, ТВ, ЗА	РС Б
12	Дані с камер відеоспостереження та записи розмов	ІзОД	Конфіденційна інформація	ВПО	S
13	Документи про службові відрядження працівників	ІзОД	Конфіденційна інформація	Б, ВО. ВП, ФД, ЗА	РС Б
14	Технологічна інформація	ІзОД	Конфіденційна інформація	Всі відділи	РС ФД, Б, ВП, ВО, ТВ, ФВО
15	Юридична документація	ІзОД	Конфіденційна інформація	ФД, Б, ЮВ	РС ЮВ

S – Сервер; ВО – Відділ охоронної сигналізації; ВП – Відділ пожежної сигналізації; ФД – Фінансовий директор; ВК – Відділ кадрів; ВФО – Відділ фізичної охорони; Б – Бухгалтерія; ЗА – Завідуючий автопарком; ВПО – Відділ позавідомчої охорони; ТВ – Технічний відділ; ГД – Генеральний директор та його секретар; ЮВ – Юридичний відділ.

Далі описується інформація, характерна для відділу охоронної сигналізації.

Охоронне підприємство, а саме відділ з охоронної сигналізації, використовує для збереження та обробки інформації пару ПК та БФП. Ноутбуки, яких може бути до десятків штук, в залежності від кількості працівників, які виконують замовлення. потрібні лише для програмного налаштування ППКОП через спеціальну програму «Конфігуратор» або її аналоги. У програму лише прописуються налаштування, які не зберігаються після закінчення роботи. Іншої цінної інформації в ноутбуках підприємства у даному відділі відсутня.

Робота з даними ведеться у паперовому та електронному вигляді. Характеристика інформації яка циркулює у відділі охоронної сигналізації описана у таблиці 2.6.

Таблиця 2.6 – Характеристика інформації

№	Назва	Деталі	
1	Клієнтська база	Ідентифікатор	27000101
		Власник	Завідуючий
		Зберігач	Завідуючий
		Користувачі	Завідуючий, Старший працівник
		Місце розташування	ПК завідуючого
		Регулярність оновлення резервного копіювання	Щомісяця
		Місце розташування резервних копій	ЗН, сейф завідуючого
		РК	3
		РЦ	3
		РД	2
2	Вхідні плани об’єктів замовників	Ідентифікатор	196448874
		Власник	Завідуючий
		Зберігач	Завідуючий, Старший працівник
		Користувачі	Працівники, Старший працівник
		Місце розташування	ПК завідуючого, старшого працівника
		Регулярність оновлення резервного копіювання	Щонеділі
		Місце розташування резервних копій	ЗН, сейф завідуючого
		РК	4
		РЦ	2
		РД	2

Продовження таблиці 2.6

№	Назва	Деталі	
3	Вихідні плани об'єктів замовників	Ідентифікатор	27000102
		Власник	Старший працівник
		Зберігач	Завідуючий, Старший працівник
		Користувачі	Працівники, Старший працівник
		Місце розташування	ПК завідуючого, старшого працівника
		Регулярність оновлення резервного копіювання	Щомісяця
		Місце розташування резервних копій	ЗН, сейф завідуючого
		РК	4
		РЦ	2
		РД	2
4	Дані замовлень	Ідентифікатор	27000103
		Власник	Завідуючий
		Зберігач	Завідуючий, Старший працівник
		Користувачі	Працівники, Старший працівник, Завідуючий
		Місце розташування	ПК завідуючого, старшого працівника
		Регулярність оновлення резервного копіювання	Щомісяця
		Місце розташування резервних копій	ЗН, сейф завідуючого
		РК	4
		РЦ	2
		РД	2
5	Робочий графік	Ідентифікатор	27000104
		Власник	Завідуючий
		Зберігач	Завідуючий
		Користувачі	Працівники, Завідуючий, Старший працівник
		Місце розташування	ПК завідуючого
		Регулярність оновлення резервного копіювання	Щомісяця
		Місце розташування резервних копій	ЗН, сейф завідуючого
		РК	1
		РЦ	1
		РД	1

Продовження таблиці 2.6

№	Назва	Деталі	
6	Технологічна інформація	Ідентифікатор	27000104
		Власник	Завідуючий
		Зберігач	Завідуючий
		Користувачі	Працівники, Завідуючий, Старший працівник
		Місце розташування	ПК завідуючого
		Регулярність оновлення резервного копіювання	Щомісяця
		Місце розташування резервних копій	ЗН, сейф завідуючого
		РК	4
		РЦ	3
		РД	3

ЗН – Зовнішній накопичувач.

Робочий графік – створюються завідуючим за допомогою офісного ПЗ, копія відсилається на Хмарне сховище с доступом до всіх працівників.

Клієнтська база – створюються завідуючим та заповнюються ним, копія яких зберігається на зовнішньому накопичувачі у сейфі .

Вхідні плани об’єктів замовників – приймаються у електронному вигляді через пошту, мессенджери або через зовнішній носій до ПК завідуючого або паперовому (для відцифрування їх у майбутньому) та передаються процівникам. Копії зберігаються на зовнішньому носії у сейфі. Являють собою точні плани об’єктів на якому описані місцезнаходження охоронного обладнання для монтажу та обслуговування.

Вихідні плани об’єктів замовників – виготовляються, коли замовник не має чіткого плану щодо розташування компонентів охоронної сигналізації, зберігаються у ПК завідуючого або старшого під час їх обробки, копії(після схвалення та затвердження підсумкового варіанту їх клієнтом) зберігаються на зовнішньому носії у сейфі. Являє собою точні плани об’єктів замовників, з розташуванням у ньому місцезнаходження охоронного обладнання для монтажу та

обслуговування, які будуть задовольняти вимоги заказу клієнта, та плани реалізації їх підсумкового монтажу.

Дані замовлень – являє собою інформацію про місцезнаходження об'єкту, його основну характеристику та вимоги клієнта.. Створюються завідуючим за допомогою офісного ПЗ, копії зберігаються на зовнішньому носії у сейфі.

Технологічна інформація – інформація, яка являє собою налаштування охоронної апаратури на об'єкті замовника та паролі. Паролі у більшості випадків використовуються для редагування, налаштування та додавання користувачів охоронної сигналізації через клавіатуру, яка з'єднана з ППКОП. Також до неї відносяться параметри входу до ПК завідуючого та старшого працівника. Створюються завідуючим за допомогою офісного ПЗ, копії зберігаються на зовнішньому носії у сейфі. Параметри входу до ПК створюються системним адміністратором, після якого працівник забов'язаний змінити на свій у найближчі часи після початку використання ІС.

Для ідентифікації інформаційних активів (Див.таб. 2.5) були використані рівні властивостей, що описані далі.

Рівні конфіденційності:

- К1 – рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;

- К2 – рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;

- К3 – рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;

- К4 – рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;

- К5 – критичний рівень конфіденційності інформації, що може призвести до краху компанії у разі втрати конфіденційності інформації.

Рівні цілісності:

- Ц1 – рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;

- Ц2 – рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;

- Ц3 – рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

- Ц4 – рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;

- Ц5 – критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

- Д1– рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;

- Д2 – рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;

- Д3 – рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;

- Д4 – рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;

- Д5 – критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

2.8 Оцінка ризиків обраної області діяльності

Враховуючи всі ресурси та інформаційні активи обраного відділу охоронного підприємства, можна оцінити найбільш типові ризики та з’ясувати їх рівень. В подальшому при систематичному перегляданні потенційних ризиків підприємство

буде розуміти свої вразливості, та зможе постійно їх мінімізувати до оптимального для неї рівня. Для кожного з активів буде використовуватися їх цінність, ступінь вразливості, оцінка вірогідності та загальний рівень . Рівні ступенів цих параметрів описані в таблицях 2.7-2.9.

Таблиця 2.7 – Цінність ресурсу

Рівень	Опис
1	Втрата конфіденційності та/або цінності та/або доступності ресурсу практично не призводить до наслідків із фінансовими втратами.
2	Втрата конфіденційності та/або цінності та/або доступності ресурсу призводить до незначних фінансових втрат і незначне впливом геть репутацію компанії.
3	Втрата конфіденційності та/або цінності та/або доступності ресурсу призводить до значних фінансових втрат і має значний вплив на репутацію компанії.
4	Втрата конфіденційності та/або цінності та/або доступності ресурсу призводить до великих фінансових втрат (визначити суму), має значний вплив на репутацію компанії та може призвести до зупинення роботи бізнес-процесу.

Таблиця 2.8 – Ступінь вразливості

Рівень	Опис
1	Вразливість практично не призводить до розкриття конфіденційної інформації.
2	Вразливість призводить до розкриття відомостей, які відносяться до конфіденційної інформації, персональних даних, та призводить до фінансових втрат.
3	Вразливість призводить до розкриття відомостей, які відносяться до конфіденційної інформації, персональних даних, та призводить до значних фінансових втрат, має значний вплив на репутацію компанії та може призвести до зупинення роботи бізнес-процесу.
4	Приводить до зупинки бізнес-процесу та порушення закону.

Таблиця 2.9 – Оцінка вірогідності

Рівень	Опис
1	Загроза має місце у історичному аспекті
2	Загроза виникає 2-3 десь у рік у галузі
3	Загроза мала місце 1 раз у компанії.
4	Загроза проявляється 2-3 рази на рік у компанії.

Загальний рівень розраховується за формулою наступною формулою.

$$Р = ЦР \quad СВ \quad ОВ \tag{2.1}$$

де Р – загальний рівень;

ЦР – цінність активу;

СВ – ступінь вразливості;

ОВ – оцінка вірогідності.

Усі данні з типовими загрозами вносяться у таблицю 2.10

Таблиця 2.10 – Оцінка ризиків

Ресурс	Джерело	Загроза	Вразливість	ЦР	СВ	ОВ	Р
РС завідуючого, старшого працівника	Внутрішні (працівники)	Порушення працездатності системи	Відсутність оновлень ПЗ, наявність старих версій	2	2	1	4
РС завідуючого, старшого працівника	Внутрішні (працівники)	Порушення КДЦ через можливе відкриття фішингового листу, перехід по стороннім посиланням, або неправильне використання ПЗ	Відсутність відділу ІБ	3	4	2	24
РС завідуючого, старшого працівника	Внутрішні (працівники)	Передача доступної інформації через електронні ресурси	Відсутність контролю за потоками інформації на РС працівників	3	3	1	9
Всі інформаційні активи відділу	Внутрішні (працівники)	Підкупи або шантаж працівника\ів підприємства конкурента-ми	Недостатньо замотивований, або не комфортні умови роботи робітників чи їх поганий підбір, велика конкуренція	3	2	2	12
Технологічна інформація, вхідні\вихідні плани об’єктів замовників	Зовнішнє (конкуренти)	Втручання, зміни або підглядання за діяльністю працівників під час виконання робіт на об’єктах.	Присутність посторонніх осіб при монтажу або обслуговуванні обладнання на об'єктах підприємств	3	3	2	18

Після оформлення таблиці оцінки ризиків, підприємство має наглядне уявлення щодо актуальних вразливостей у даному відділі. Підприємство може

також обрати ступені щодо необхідності обробки ризику використовуючи критерії їх градації які описані в таблиці 2.11.

Таблиця 2.11 – Критерії щодо обробки ризиків

Умовні значення ризику	Числове значення оцінки ризику	Рішення щодо подальшої обробки ризику
Низький ризик	1-10	Ризик вважається незначним. Обробка ризиків не потрібна
Середній ризик	11-21	Обробка ризику може виконуватись або не виконуватись
Високий ризик	22-64	Ризик вважається суттєвим. Обробка ризиків обов'язковим

Числове значення оцінювання ризику підприємство може обирати своє, але суть її остається однаковою, головне щоб підприємство розуміло, коли потрібно оброблювати ризики, щоб зменшити подальші витрати від їх загроз[10].

2.9 Аналіз значущих ризиків та вразливостей у підприємстві

Для ІКС можуть бути характерними наступні вразливості:

1) Недостатньо замотивований, або не комфортні умови роботи робітників чи їх поганий підбір, велика конкуренція;

2) Присутність посторонніх осіб при монтажу або обслуговуванні обладнання на об'єктах підприємств

3) Відсутність відділу ІБ;

Перша вразливість має у собі комплексний характер, тому що на поточний час держава вже котрі роки переносить важкі часи(Такі як COVID-19 та війна з агресором у лиці РФ), через це багато охоронних підприємств, в особливості їх співробітників мушуть виконувати роботи у більш важких умовах. Через це в підприємстві можуть проходити постійний відток та приток кадрів, а це насамперед

не дає змогу повністю розробити довірений та гарно злагоджений персонал. І це значно впливає на загальний рівень ІБ у підприємстві.

Друга вразливість виходе з того, що клієнти стали все частіше при будівництві або інших робіт з об'єктом виконувати у ньому багато різних процесів в один час, що може спричинити до неправильних робіт з монтажу або проблем з ним. Ці проблеми можуть випливти згодом, коли клієнт або підприємство може навіть і не здогадуватись. Прикладом такої проблеми можуть бути те що посторонні особи, які були під час монтажу, матимуть інформацію щодо розташувань системи охоронної сигналізації, її конфігурацію, проблеми або технологічну інформацію до них. Тому при роботі з монтажу на об'єкті повинні бути тільки сам клієнт-замовник та довірені йому особи, і це повинно заздалегіть обумовлено з підприємством.

Третя вразливість саме критична, як для звичайного функціонування підприємства, так і для впровадження СУІБ у ньому. На підприємстві повинне бути таке відділення або хоча б відноситись до технічного відділу, яке буде постійно виконувати моніторинг за ІБ охоронної організації та виконувати систематичні інструктажі з ІБ працівникам. Також для впровадження СУІБ такий відділ буде членом комісії та команди, яка буде брати участь в ній. Такі впровадження матимуть для підприємства більше вигоди, ніж залучати сторонніх компаній до процесу, як впровадження СУІБ так і до звичайного підвищення кваліфікації з ІБ працівників.

2.10 Політика інформаційної безпеки

Організації, що займаються обробкою інформації щодо фізичної охорони, у тому числі конфіденційної інформації щодо об'єктів клієнтів, повинні мати політику ІБ в письмовому вигляді, схвалену керівництвом, опубліковану, а потім доведену до всіх співробітників і відповідних сторонніх організацій.

Політика інформаційної безпеки, як правило, є документом найвищого рівня, який описує основну мету СУІБ. Головні ж цілі в СУІБ зазвичай можуть бути виділені до окремого документу, але також вони можуть бути включені до політики інформаційної безпеки.

Також крім дотримання інструкцій, зазначених у ISO/IEC 27002, щодо того, що має містити документ про політику ІБ, цей документ повинен враховувати :

1) необхідність захисту інформації в охоронних підприємствах;

2) мету та цілі захисту інформації;

3) сферу та області застосування;

4) законодавчі, нормативні та контрактні вимоги, включаючи ті, що стосуються захисту інформації, а також юридичних та етичних обов'язків працівників для захисту цієї інформації;

5) засоби для оповіщення про інциденти в системі захисту інформації, у тому числі канали зв'язку, де розглядатиметься питання про порушення конфіденційності, не побоюючись звинувачень або взаємних закидів.

Теоретично перегляд змісту цієї політики буде залежати від результатів оцінки ризиків організації, хоча сама політика повинна тільки ставити напрямок, встановлювати принципи і вказувати на інші документи, де слід знайти (частіше ті, які постійно змінюються) особливості.

Політика інформаційної безпеки знаходиться у додатку Ґ.

Для більш наглядної демонстрації розроблена схема політики безпеки, яка зображена у додатку Г.

2.11 Цілі заходів безпеки та заходи безпеки

Положення щодо застосовності(таблиця з додатку А у ISO/IEC 27001)

Положення щодо застосовності можна розглядати як короткий огляд стану захисту інформації в організації, трактування організацією вимог захисту та її

стратегії для реалізації рішень у галузі ІБ. Цей документ ведеться особою, відповідальною за захист інформації, або аналогічною відповідальною особою за дорученням, і він має бути наданим службам з управління організацією з метою формування основної частини пакету документів з управління. Також його формат зазвичай підходить для використання в якості інструменту з оцінки або підтвердження для підтримки зовнішнього аудиту та інших наглядових перевірок.

Цілі заходів безпеки та заходи безпеки, у якості прикладу, наведені в додатку Д. Наповнення цієї таблиці залежить від сформованості ризиків ІБ та може змінюватись або доповнюватись підприємством.

Також слід виділити документ о неперервності бізнесу, який теж є складовим СУІБ. Він повинен мати у своєму складі наявність інструкцій на випадок надзвичайних ситуацій, таких як пожежа, відсутність електропостачання, недоступність каналів зв'язку та ін. Її головна мета, це наявність методик проведення навчань з персоналом підприємства і акт, підтверджуючий проведення навчань по факту реагування у випадку надзвичайних ситуацій.

2.12 Необхідність в постійній гарантії ІБ

Підприємства с охоронних послуг у рамках СУІБ вимагають гарантії його ефективності за підтримки нинішнього рівня захисту та її постійного поліпшення відповідно до стратегії забезпечення захисту інформації відповідно до цілей організації.

Для забезпечення цієї гарантії доступна низка варіантів. Ці варіанти можуть бути використані у комбінації один з одним. Менш дорогі можливості надають пропорційно меншу гарантію, що відображає обмежену строгість і незалежність, що пропонуються ними. Охоронні підприємства організації повинні створювати програми для перевірки відповідності, які використовують комбінацію технології та підходи

До цих гарантій можуть бути віднесені:

- оцінка відповідності;

- рецензування;

- незалежний аудит;

- сертифікаційний аудит на відповідність.

Оцінка відповідності на базовому рівні, особливо там, де впровадження ISO/IEC 27001 проводиться виключно для внутрішніх цілей, а оцінка, яка виконана невеликою групою інших підрозділів організації, дасть деяке уявлення про ефективність СУІБ. Проте такий підхід часто може бути скомпрометований лояльністю та особистими або організаційними зобов'язаннями працівників.

Рецензування є дуже схожим на оцінку відповідності, але являється альтернативним варіантом, при якому різні організаційні зв'язки рецензентів здатні призвести до зростання об'єктивності, яке і може бути забезпеченням гарантії. Цей варіант також може бути здійснений безкоштовно, якщо він організований на взаємовигідних умовах, наприклад, між особами, відповідальними за захист інформації. Але це може призвести до домовленості про взаємно позитивних звітах.

Незалежні аудити можуть бути за певною вартістю проведені різними організаціями, такими як аудиторські та консалтингові компанії. Ймовірно, підсумковий звіт буде надійним і вищою якістю, відображаючи, як правило, вищий рівень компетентності. Такі перевірки дають «порівняльну оцінку», оскільки залучений до цієї роботи персонал, швидше за все, вже проводив інші подібні незалежні аудити, на основі яких, можуть проводити порівняння.

Сертифікаційні аудити зазвичай включають нараду з визначення обсягів робіт, огляд документа, а потім саму перевірку відповідності.

Грунтуючись на досвіді, накопиченому іншими сертифікованими організаціями, охоронні підприємства повинні залучати аудиторів цих організацій відразу після прийняття рішення про проведення сертифікації. Потім аудитор стає швидше партнером з проведення аудиту, а відповідь може бути досягнута поступово, наприклад, за попередньою домовленістю про те, що опис галузі

застосування, обумовлений у області, яку обрано для охоплення в СУІБ, правильно сформульований і може бути правильно представлений. Тим не менш, також варто розглянути можливість проведення рецензування або незалежного аудиту на проміжному етапі для подальшого запобігання будь-якій можливості виникнення проблем.

Поширеною помилкою є те, що сертифікація здійснюється лише якщо захист інформації та ІБ у підприємстві є «ідеальним». Вимогою є лише наявність вже функціонуючої СУІБ, чітке розуміння ризиків та впливів і план управління зниження цих впливів до прийнятного рівня. У процесі аудиту може бути виявлено обмежену кількість недоліків, які, залежно від їх серйозності, можуть і не завадити успішному проведенню сертифікації. Існує також хибна думка, що сертифікація потребує багато часу. Проте, досвід показує, що сертифікаційні аудити різних підприємств, в яких охоронні організації навряд чи можуть стати винятком, не займають в аудитора по сертифікації понад 5-6 робочих днів. Остаточним незалежним аудитом є аудит, проведений компетентним, незалежним аудиторським органом відповідно до керівництва ISO 27001, як це встановлено в багатьох країнах. Даний вид аудиту є найкращим з перерахованих тут варіантів, так як він здійснюється професійним аудитором. Такий аудитор повинен також бути компетентним у сфері ІТ та захисту інформації. Отже, рівень ретельності проведеного аудиту та порівняльної оцінки методик, які можна очікувати від такого аудиту, високий, але вартість такого аудиту іноді може бути не прийнятною[10].

2.13 Висновок

Під час виконання спеціального розділу було виконане обстеження типового підприємства з надання охоронних послуг. Визначена цінність інформації таких підприємств та проаналізовані бізнес-процеси, які потенційно можуть входити в

область дії СУІБ. Виходячи з цих даних, були розраховані потенційні загрози та вразливості. Також було проаналізовано перелік документів, які необхідні для впровадження СУІБ враховуючи їх особливості. Згідно усіх зібраних матеріалів сформовані такі документи, як політика інформаційної безпеки та положення щодо застосовності. Усі ці документи будуть мани гарантію щодо її впровадження та переглядань задля постійної актуальності.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Одна з вагомих цілей захисту інформаційних ресурсів від загроз є мінімізація збитків через порушення інформаційної безпеки підприємства. Метою виконання економічних розрахунків кваліфікаційної роботи є обґрунтування доцільності запровадження запропонованих в роботі рішень.

Для виконання економічного розділу необхідно:

- розрахувати капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення та ін.;

- розрахувати річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

- визначити річний економічний ефект;

- визначити показники економічної ефективності.

3.1 Розрахунок капітальних витрат на створення основних документів

Спочатку, необхідно визначити трудомісткість створення основних документів для впровадження СУІБ.

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д} \text{ годин}, \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_в$ – тривалість розробки концепції безпеки інформації у організації;

$t_а$ – тривалість процесу аналізу ризиків;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_д$ – тривалість документального оформлення політики безпеки. Таким чином трудомісткість розробки політики безпеки дорівнює:

$$t = 20+12+20+30+15+17+52$$

$$t = 166 \text{ год.}$$

Розрахуємо витрати на створення основних документів СУІБ. Розрахунок проводиться за формулою 3.2:

$$K_{рп} = З_{зп} + З_{мч} \text{ грн.} \quad (3.2)$$

де $K_{рп}$ – витрати на створення основних документів СУІБ;

$З_{зп}$ – заробітна плата спеціаліста з інформаційної безпеки;

$З_{мч}$ – вартість витрат машинного часу, що необхідні для створення ПБ. Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою 3.3:

$$З_{зп} = t \cdot З_{іб}, \text{ грн,} \quad (3.3)$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Середньогодинна заробітна плата спеціаліста з інформаційної безпеки становить – 95 грн/год.

Відповідно до формули 3.3, витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 166 \text{ год} \cdot 95 \text{ грн/год},$$

$$З_{зп} = 15\,770 \text{ грн}.$$

У свою чергу, витрати машинного часу визначаються за формулою 3.4:

$$З_{мч} = t \cdot С_{мч} \text{ грн}. \quad (3.4)$$

де t – трудомісткість розробки політики безпеки інформації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою 3.5:

$$С_{мч} = P \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн}, \quad (3.5)$$

де P – встановлена потужність ПК, кВт;

$С_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$t_{нал}$ – кількість задіяних робочих станцій, які задіяні;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня Fр = 1920).

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

$$С_{мч} = 0,25 \cdot 1 \cdot 3,45 + (13000*0,6)\backslash 1920 + (6700*0,4)\backslash 1920 \text{ грн},$$

$$С_{мч} = 6,31 \text{ грн.}$$

$$З_{мч} = 6,31*166=1047,46 \text{ грн.}$$

Отже, витрати на створення основних документів СУІБ за формулою 3.2 становлять:

$$К_{рп} = 1047,46+15770= 16817,46 \text{ грн.}$$

В результаті розрахунків, вартість створення основних документів СУІБ становить – 16817,46 гривень.

Повна вартість капітальних витрат розраховується за формулою 3.6:

$$К = К_{рп} + К_{аз} + К_{зпз} + К_{пр} + К_{навч} + К_{н} \text{ грн.} \quad (3.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн. Зовнішні консультанти не наймалися, тому даний коефіцієнт не враховується;

$К_{зпз}$ – вартість закупівлі ліцензійного основного й додаткового ПЗ, тис. грн. Додаткове ПЗ не закуповувалося, тому даний коефіцієнт не враховується.

$К_{рп}$ – вартість розробки створення основних документів СУІБ, тис. грн.;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн. Додаткове апаратне забезпечення не закуповувалося, тому даний коефіцієнт не враховується.

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн. Технічні фахівці і обслуговуючий персонал будуть навчатися за рахунок

найманого фахівця з ІБ, який буде проводити систематичні заходи задля підвищення обізнаності в сфері ІБ.

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн. Додаткове обладнання не закуповувалось, тому даний коефіцієнт не враховується.

Таким чином, згідно з формулою 3.6:

$$K = 16817{,}46 \text{ грн.}$$

3.2 Розрахунок поточних(експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

Поточні витрати розраховуються за формулою 3.7:

$$C = C_з + C_е + C_{тос} \text{ грн,} \quad (3.7)$$

де $C_з$ – річний фонд заробітної плати інженерно-технічного персоналу;

$C_е$ – вартість електроенергії, що споживається апаратурою;

$C_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки, яке становить 2% від капітальних витрат (3363,5 грн).

У свою чергу, витрати на заробітну плату інженерно-технічного персоналу розраховуються за формулою 3.8:

$$C_з = З_{осн} + З_{дод1} \text{ грн,} \quad (3.8)$$

де $З_{осн}$ – основна заробітна плата працівника з інформаційної безпеки складає 15200 грн і відповідно 182400 грн на рік;

$З_{дод1}$ – додаткова заробітна плата яка складає 10% від основної заробітної плати;

За формулою 3.8 можна розрахувати:

$$С_з = 182400 + 18240 = 200640 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою становить розраховують за формулою 3.9:

$$С_е = P \cdot F_р \cdot Ц_е, \text{ грн} \quad (3.9)$$

де P – встановлена потужність апаратури інформаційної безпеки яка на 19 ПК працівників складає 4,75 кВТ ;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки складає 1920 год;

$Ц_е$ – тариф на електроенергію який складає 3,45 грн/кВт годин

$$С_е = 4,75 \cdot 1920 \cdot 3,45 = 31464 \text{ грн.}$$

Отже повна вартість річних експлуатаційних витрат становить:

$$С = 31464 + 200640 + 3363,5 = 235467,5 \text{ грн.}$$

Таким чином повна вартість річних експлуатаційних витрат становить 235467,5 грн.

3.3 Розрахунок витрат при виникненні загроз

Метою цієї оцінки є визначення обсягів матеріальних збитків, виходячи з імовірності реалізації конкретної загрози й можливих матеріальних втрат від неї. Для подальших розрахунків потрібно знати загальну суму заробітної плати працівників обслуговування та співробітників відділу підприємства, місячна плата яких зазначена в таблиці 3.1.

Таблиця 3.1 – Заробітна плата працівників підприємства

Посада	Розмір заробітної плати в місяць, грн
Завідуючий відділення	25000
Старший працівник	20000
Персонал з монтажу охоронної сигналізації(10 осіб)	15000
Персонал з обслуговування охоронної сигналізації(6 осіб)	13000
Системний адміністратор	9000
Працівник ІБ	15200

Загальна сума заробітних плат співробітників підприємства становить 273 000 грн/місяць. Загальна сума заробітних плат працівників обслуговування становить 24200 грн.

Необхідні вхідні данні для розрахунку:

Для розрахунку збитків від реалізації даних загроз потрібно використати формулу 3.10:

t_n – час простою вузла або сегмента корпоративної мережі внаслідок атаки становить 3 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу становить 1 година;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі становить 2 години;

$З_о$ – заробітна плата співробітників обслугованого персоналу, 9700 грн/місяць;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 273 000 грн/місяць;

$Ч_о$ – чисельність обслугованого персоналу 2 особи.

$Ч_с$ – чисельність співробітників атакованого вузла 2 особи.

$О$ – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік становить 4800000 грн;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 3000 грн;

$І$ – число атакованих вузлів або сегментів корпоративної мережі становить 2;

N – середнє число атак на рік 6.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі яка розраховується формулою 3.10 становить:

$$U = П_п + П_в + V \text{ грн}, \tag{3.10}$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн;

$П_в$ – вартість відновлення працездатності вузла (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати

(оплата непродуктивної праці) за час простою внаслідок атаки які використовуються у формулі 3.11:

$$П_п = \frac{\sum З_с \cdot Ч_с}{F} \cdot t_п \text{ грн,} \quad (3.11)$$

де F – місячний фонд робочого часу при 1920 годинам на рік це 160 годин на місяць;

$$П_п = ((273\,000 \quad 2/160)) \cdot 3 = 10\,237{,}5 \text{ грн.}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових які використовуються у формулі 3.12:

$$П_в = П_{ви} + П_{пв} + П_{зч} \text{ грн,} \quad (3.12)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$ які використовуються у формулі 3.13:

$$П_{ви} = \frac{\sum З_с \cdot Ч_с}{F} \cdot t_{ви} \text{ грн,} \quad (3.13)$$

$$П_{ви} = ((273\,000 \quad 2/160)) \cdot 2 = 6825 \text{ грн.}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_В$ і розміром середньогодинної

заробітної плати обслуговуючого персоналу (адміністраторів) які використовуються у формулі 3.14:

$$П_{пв} = \frac{\sum З_О \cdot Ч_О}{F} \cdot t_в \text{ грн}, \quad (3.14)$$

$$П_{пв} = ((24200 \cdot 2/160)) \cdot 1 = 302{,}5 \text{ грн}.$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі які використовуються у формулі 3.15:

$$V = \frac{O}{F_r} \cdot (t_п + t_в + t_{ви}) \text{ грн}, \quad (3.15)$$

де F_r – річний фонд робочого часу.

$$V = 4800000 / 1920 \cdot (3 + 1 + 2) = 15000 \text{ грн}.$$

Отже упущена вигода згідно формули 3.12 становить:

$$П_в = 6825 + 302{,}5 + 15000 = 22127{,}5 \text{ грн}.$$

Отже упущена вигода згідно формули 3.10 становить:

$$U = 10\,237{,}5 + 22127{,}5 + 15000 = 47364 \text{ грн}.$$

Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації розраховується за формулою 3.16.

$$В = \sum_i \sum_n U. \quad (3.16)$$

$$В = 6 \cdot 2 \cdot 47364 = 568\ 368 \text{ грн.}$$

3.4 Визначення та аналіз показників економічної ефективності

Загальний ефект від впровадження системи інформаційної безпеки розраховується за формулою 3.17:

$$E = B \cdot R - C \text{ грн,} \tag{3.17}$$

де B – загальний збиток від атаки на вузол корпоративної мережі, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці яка складає 0,5;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, грн. Отже, економічний ефект становить:

$$E = 568\ 368 \cdot 0{,}5 - 235467{,}5 = 48716{,}5 \text{ грн.}$$

Оцінка економічної ефективності системи захисту інформації здійснюється на основі визначення та аналізу наступних показників:

– сукупна вартість володіння (ТСО) не використовується, оскільки було визначено величину відверненого збитку;

– коефіцієнт повернення інвестицій ROSI (Return on Investment for Security);

– термін окупності капітальних інвестицій T_o.

ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки, розраховується за формулою 3.18:

$$ROSI = \frac{E}{K}, \text{ частки одиниці} \quad (3.18)$$

де E – загальний ефект від впровадження системи інформаційної безпеки, грн;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, 16817,46 грн.

Таким чином,

$$ROSI = 48716,5 / 16817,46 = 2,89.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупаються за рахунок загального ефекту від впровадження системи інформаційної безпеки, розраховується за формулою 3.19:

$$T_O = \frac{E}{K} = \frac{1}{ROSI} = 0,34 \text{ року.} \quad (3.19)$$

3.5 Висновок

Під час виконання економічної частини проведені

А саме під час підрахунків було визначено, що:

1. Капітальні витрати створення основних документів СУІБ становить 16817,46 грн.

2. Повна вартість річних експлуатаційних витрат становить 235467,5 грн.

3. Загальний збиток від атаки складатиме 568 368 грн.

4. Загальний ефект від впровадження системи інформаційної безпеки становить 48716,5 грн.

5. Термін окупності капітальних інвестицій складає 0, 34 року.

Отже дані які були отримані в ході виконання економічної частини, вказують на доцільність.

ВИСНОВКИ

Об’єкт розробки кваліфікаційної роботи є ІКС охоронного підприємства.

Під час виконання першого розділу кваліфікаційної роботи вирішений загальний стан питання щодо необхідності у впровадженні СУІБ в охоронні підприємства задля підвищення загального стану захисту інформації, конкурентоспроможності та іміджу. Була розглянута сама сутність СУІБ, проаналізована необхідна для виконання роботи нормативно-правова база.

В ході виконання другого розділу були описані усі процеси та послідовність їх для впровадження СУІБ, розглянуто основні документи, які необхідні для неї. Також була розглянута типова структура охоронного підприємства, а саме проаналізовані види діяльності та повний спектр послуг, які надає підприємство та цінність інформації яка циркулює у ньому. Визначено ієрархію охоронних підприємств та розгалуження їх по підрозділам. Було виконане обгрунтування основних бізнес-процесів на підприємствах задля розуміння, яка область або процеси буде охоплювати СУІБ в ній. В обраній області діяльності були проаналізовані основні інформаційні активи та їх критичність для підприємства. Враховуючи усю отриману інформацію, було здійснено оцінювання ризиків та їх вразливість, після якого виконаний їх аналіз. Отримавши всі данні, були сформовані основні елементи політики інформаційної безпеки з урахуванням постійного переглядання цього документу та положення щодо застосовності задля розуміння цілей заходів безпеки та самих заходів.

Виконання економічного розділу підтвердило доцільність впровадження основних документів для впровадження СУІБ через отримані дані. До цих даних відносяться розрахунки щодо капітальних витрат на створення в експлуатацію ПБ, річних експлуатаційних витрат, загальний ефект після впровадження розроблених елементів та період окупності даних інвестицій.

ПЕРЕЛІК ПОСИЛАНЬ

1 Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью [Текст]: учеб. пособие для ВУЗов; 2-е изд., испр. / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – М.: Горячая линия – Телеком, 2014. – 214 с.

2 "Інтерфакс-Україна" [Електронний ресурс] //Режим доступу до ресурсу: https://ua.interfax.com.ua/news/blog/677434.html

3 ДСТУ ISO/IEC 27001:2015 [Електронний ресурс] // ДСТУ. – 2015. – Режим доступу до ресурсу:http://online.budstandart.com/ua/catalog/doc-page?id_doc=66910

4 ДСТУ ISO/IEC 27002:2015 [Електронний ресурс] // ДСТУ. – 2015. – Режим доступу до ресурсу:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911

5 ДСТУ ISO/IEC 27005:2019 [Електронний ресурс] // ДСТУ. – 2019. – Режим доступу до ресурсу:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912

6 Закон України "Про інформацію" [Електронний ресурс] // 2657-XII. – 16.07.2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

7 Закон України "Про захист інформації в інформаційно-комунікаційних системах" [Електронний ресурс] // № 1089-IX від 16.12.2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

8 Офіційний сайт ISACA. COBIT [Електронний ресурс] // Режим доступу https://www.isaca.org/resources/cobit/

9 Information technology. Security techniques. Information security management. Measurement: ISO/IEC 27004:2016 [Електронний ресурс] // Режим доступу: https://www.iso.org/standard/64120.html

10 Методические рекомендации компании IT Task по построению и сертификации СУИБ в соответствии с требованиями ISO/IEC 27001 версии 2013 г. [Електронний ресурс] //Режим доступу до ресурсу: http://www.iso27000.ru

11 Кваліфікаційна робота магістра. Методичні рекомендації до виконання для студентів спеціальності 125 «Кібербезпека» (освітньо-професійна програма «Кібербезпека») / Упоряд.: О.Ю.Гусєв, В.І.Корнієнко, В.І.Магро, Д.С. Тимофєєв; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Д.: НТУ «ДП», 2022. – 34 с.

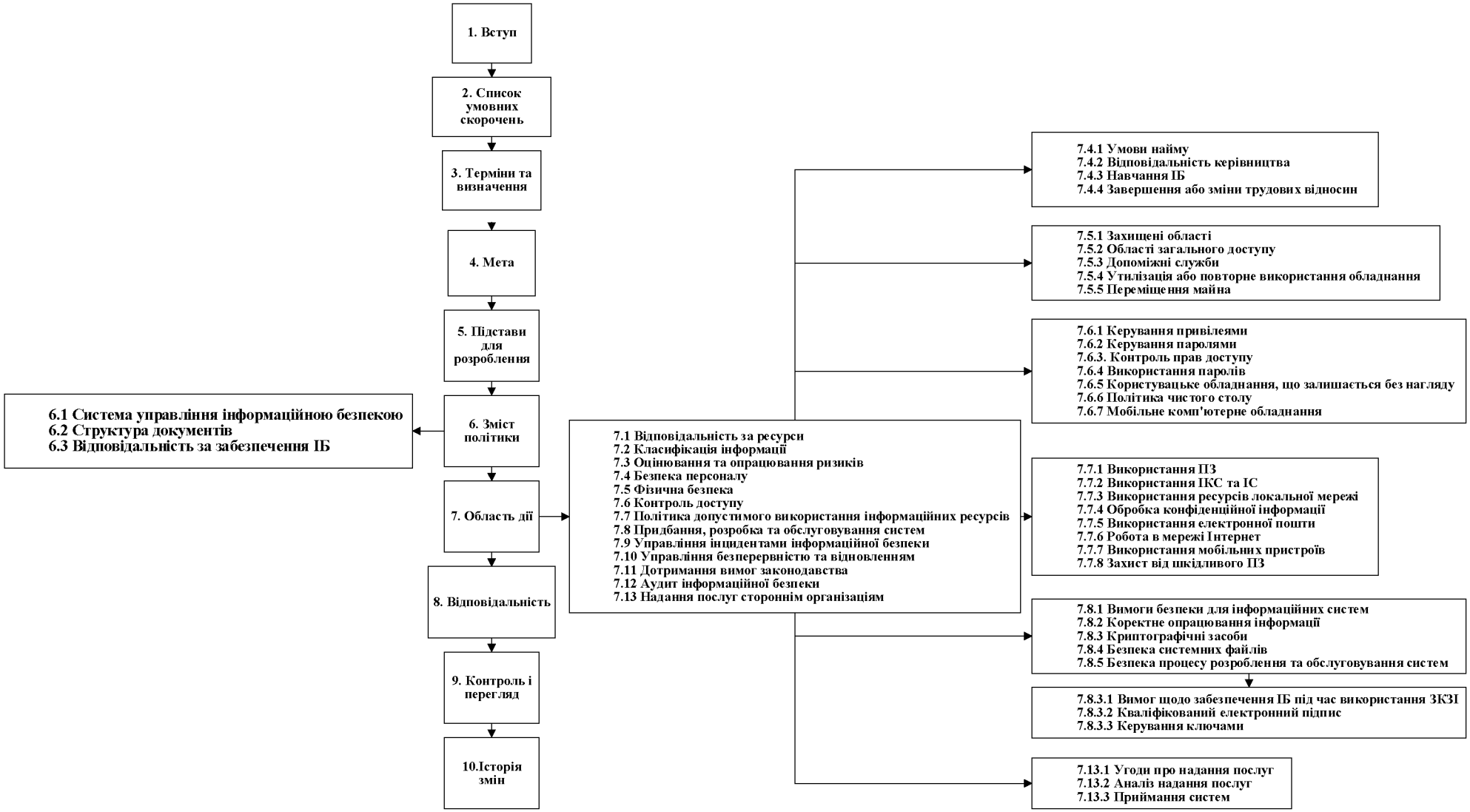
12 Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д.П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка» , 2019. – 16с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість аркушів	Примітки
		Документація		
1	А4	Реферат	2	
2	А4	Список умовних позначень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	10	
6	А4	Спеціальна частина	28	
7	А4	Економічна частина	13	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	47	
14	А4	Додаток Ґ	4	
15	А4	Додаток Д	1	
16	А4	Додаток Е	1	
17	А4	Додаток Є	2	

ДОДАТОК Б. Схема організаційної структури підприємства

ДОДАТОК В. Схема структури інформаційної безпеки



ДОДАТОК Г. Політика інформаційної безпеки

Політика інформаційної безпеки

1. Вступ

Політика інформаційної безпеки (далі – Політика) організація з надання послуг з фізичної охорони (далі – Підприємство) визначає систему поглядів на проблему забезпечення інформаційної (далі – ІБ). Являє собою систематизований виклад високорівневих цілей і завдань захисту, якими необхідно керуватися в охоронній діяльності, а також основних принципів побудови системи управління інформаційною безпекою (далі – СУІБ) Підприємства. Забезпечення інформаційної безпеки – необхідна умова для успішного здійснення статутної діяльності Підприємства. Забезпечення інформаційної безпеки включає будь-яку діяльність, спрямовану на захист інформаційних ресурсів та/або підтримуючої інфраструктури у ньому. Політика охоплює всі автоматизовані та комунікаційні системи, власником і користувачем яких є підприємство. Реалізація Політики має виходити з передумови, що неможливо забезпечити необхідний рівень захищеності інформаційних ресурсів не тільки за допомогою окремого засобу, а й за допомогою їх простої сукупності. Необхідне їх системне, узгоджене між собою застосування, а окремі елементи інформаційної системи, що розробляються, слід розглядати як частину єдиної інформаційної системи в захищеному виконанні за оптимального співвідношення технічних і організаційних заходів.

2. Список умовних скорочень

ЗКЗІ – засіб криптографічного захисту інформації;

ІБ – інформаційна безпека;

ІКС – інформаційна комунікаційна система;

ІР – інформаційний ресурс;

ІС – інформаційна система;

ІТ – інформаційні технології;

КЕП – кваліфікований електронний підпис;

НСД – несанкціонований доступ;

ПЗ – програмне забезпечення;

СУІБ – система управління інформаційною безпекою.

3. Терміни та визначення

Автоматизована система – система, що складається з персоналу та комплексу засобів автоматизації його діяльності, яка реалізує інформаційну технологію виконання встановлених функцій.

Авторизація – надання суб'єкту прав на доступ, а також надання доступу відповідно до встановлених прав на доступ.

Автентифікація – перевірка приналежності суб'єкту доступу пред'явленого ним ідентифікатора; підтвердження автентичності.

Безпека інформації – захищеність інформації від її небажаного розголошення (порушення конфіденційності), спотворення (порушення цілісності), втрати або зниження ступеня доступності, а також незаконного її тиражування.

Бізнес-процес – послідовність технологічно пов'язаних операцій з надання продуктів, послуг та/або здійснення конкретного виду діяльності Підприємства.

Власник активу – фізична або юридична особа, яка наділена адміністративною відповідальністю за керівництво виготовленням, розробкою, зберіганням, використанням і безпекою активу. Термін "власник" не означає, що ця людина фактично має право власності на цей актив.

Власник інформаційних ресурсів, інформаційних систем, технологій та засобів їх забезпечення – суб'єкт, який здійснює володіння та користування зазначеними об'єктами і реалізує повноваження розпорядження в межах, встановлених законом.

Документ – зафіксована на матеріальному носії інформація з реквізитами, що дають змогу її ідентифікувати.

Доступність інформації – стан, що характеризується здатністю ІС забезпечувати безперешкодний доступ до інформації суб'єктів, які мають на це повноваження.

Захист інформації – діяльність, спрямована на запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, що захищається, і засоби доступу до неї.

Ідентифікація – присвоєння суб'єктам доступу, об'єктам доступу ідентифікаторів(унікальних імен) і (або) порівняння пред'явленого ідентифікатора з переліком присвоєних ідентифікаторів.

Інформація – відомості про осіб, предмети, факти, події, явища і процеси незалежно від форми їх подання.

Інформаційна безпека (ІБ) – стан захищеності інтересів Підприємства.

Інформаційна система – сукупність інформації, що міститься в базах даних, та інформаційних технологій і технічних засобів, що забезпечують її обробку.

Інформаційний процес – процеси збирання, опрацювання, накопичення, зберігання, пошуку та поширення інформації.

Інформаційний ресурс (актив) – усе, що має цінність і перебуває в розпорядженні Підприємства.

Інцидент – непередбачувана або небажана подія (група подій) безпеки, що призвела(можуть призвести) до порушення функціонування інформаційної системи або виникнення загроз безпеці інформації (порушення конфіденційності, цілісності, доступності).

Інцидент інформаційної безпеки – одна або серія небажаних або несподіваних подій ІБ, що мають значну ймовірність порушення бізнес-процесів або становлять загрозу ІБ.

Комерційна таємниця – конфіденційність інформації, що дає змогу її володареві за наявних або можливих обставин збільшити доходи, уникнути невиправданих витрат, зберегти становище на ринку товарів, робіт, послуг або отримати іншу комерційну вигоду.

Контрольована зона – простір (територія, будівля, частина будівлі), у якому унеможливлено неконтрольоване перебування осіб, а також транспортних, технічних чи інших засобів.

Конфіденційна інформація – інформація з обмеженим доступом, що не містить відомостей, які становлять державну таємницю, доступ до якої обмежується відповідно до законодавства України.

Конфіденційність інформації – стан захищеності інформації, що характеризується здатністю ІС забезпечувати збереження в таємниці інформації від суб'єктів, які не мають повноважень на ознайомлення з нею.

Несанкціонований доступ – доступ до інформації або дії з інформацією, що порушують правила розмежування доступу з використанням штатних засобів, що надаються засобами обчислювальної техніки або автоматизованими системами.

Опрацювання ризику – процес вибору та реалізації заходів щодо модифікації (зниження) ризику.

Політика – загальні цілі та вказівки, формально виражені керівництвом.

Привілеї – це права довіреного об'єкта на вчинення будь-яких дій щодо об'єктів системи.

Ризик – поєднання ймовірності події та її наслідків.

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління, заснована на оцінці ризиків, призначена для створення, впровадження, експлуатації, моніторингу, аналізу, супроводу та вдосконалення ІБ. Власник інформаційних ресурсів, інформаційних систем, технологій і засобів їх забезпечення – суб'єкт, який у повному обсязі реалізує повноваження володіння, користування, розпорядження зазначеними об'єктами.

Події інформаційної безпеки – ідентифікований стан системи, сервісу або мережі, що свідчить про можливе порушення політики безпеки або відсутність механізмів захисту, або раніше невідома ситуація, яка може мати відношення до безпеки.

Загроза – Небезпека, що передбачає можливість втрат (збитків).

Цілісність інформації – стійкість інформації до несанкціонованого доступу або випадкового впливу на неї в процесі опрацювання технічними засобами, результатом якого може бути знищення та спотворення інформації.

4. Мета

Основною метою, на досягнення якої спрямовані всі положення цієї Політики, є захист інформаційних ресурсів охоронного підприємства від можливого заподіяння їм матеріальної, фізичної, моральної чи іншої шкоди, за допомогою випадкового або навмисного впливу на інформацію, її носії, процеси оброблення та передавання, а також мінімізація ризиків ІБ.

Для досягнення основної мети необхідно забезпечувати ефективне вирішення таких завдань:

- своєчасне виявлення, оцінка та прогнозування джерел загроз ІБ;
- створення механізму оперативного реагування на загрози ІБ;
- запобігання та/або зниження збитків від реалізації загроз ІБ;
- захист від втручання в процес функціонування ІС сторонніх осіб;
- відповідність вимогам державного законодавства, нормативно-методичних документів та договірним зобов'язанням у частині ІБ;
- забезпечення безперервності критичних бізнес-процесів;
- досягнення адекватності заходів щодо захисту від загроз ІБ;
- вивчення партнерів, клієнтів, конкурентів і кандидатів на роботу;
- недопущення проникнення структур організованої злочинності та окремих осіб із протиправними намірами;
- виявлення, попередження і припинення можливої протиправної та іншої негативної діяльності співробітників;
- підвищення ділової репутації та корпоративної культури.

5. Підстави для розроблення

Цю політику розроблено на основі вимог законодавства, накопиченого в Підприємстві досвіду в галузі забезпечення ІБ, інтересів і цілей Підприємства.

Під час написання окремих положень цієї політики використовувалися такі нормативні документи:

- ДСТУ ISO/IEC 27001:2015 – Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою;

- ДСТУ ISO/IEC 27002:2015 – Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки;

- ДСТУ ISO/IEC 27005:2019 – Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки;

- Закон України «Про захист персональних даних» ;

- Закон України «Про інформацію» ;

- Закон України «Про електронні довірчі послуни».

Ця Політика поширюється на всі бізнес-процеси відділу\ів охоронного Підприємства й обов'язкова для застосування всіма співробітниками та керівництвом Підприємства, а також користувачами її інформаційних ресурсів.

Ця політика поширюється на інформаційні системи підприємства. Особи, які здійснюють розробку внутрішніх документів Підприємства, що регламентують питання інформаційної безпеки, зобов'язані керуватися цією Політикою.

6. Зміст політики

6.1 Система управління інформаційною безпекою

Для досягнення зазначених цілей і завдань в Підприємстві впроваджується система управління інформаційною безпекою.

СУІБ задокументована у цій політиці, у правилах, процедурах, робочих інструкціях, які є обов'язковими для всіх працівників Підприємства в області дії системи. Документовані вимоги СУІБ доводяться до відома працівників Підприємства.

Засоби управління інформаційною безпекою впроваджуються за результатами проведення оцінки ризиків інформаційної безпеки.

Вартість впроваджуваних засобів управління інформаційною безпекою не повинна перевищувати можливий збиток, що виникає під час реалізації загроз.

6.2 Структура документів

З метою створення взаємопов'язаної структури нормативних документів Підприємства у сфері забезпечення інформаційної безпеки, нормативні документи, що розробляються та оновлюються, повинні відповідати такій ієрархії(Див. рис.2):

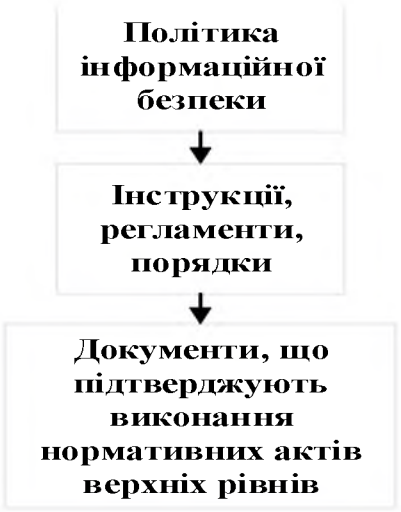


Рисунок 2 – ієрархія нормативних документів

1) Ця Політика є внутрішнім нормативним документом з ІБ першого рівня.

2) Документи другого рівня – інструкції, порядки, регламенти та інші документи, що описують дії співробітників Підприємства щодо реалізації документів першого і другого рівня.

3) Документи третього рівня – звітні документи про виконання вимог документів верхніх рівнів.

6.3 Відповідальність за забезпечення ІБ

Для безпосередньої організації та ефективного функціонування системи забезпечення інформаційної безпеки в Підприємстві функції забезпечення ІБ

покладено на відділ ІБ. На цей підрозділ покладається вирішення таких основних завдань:

- проведення в життя Політики ІБ;

- визначення вимог до захисту інформації;

- організація заходів і координація робіт усіх підрозділів з питань комплексного захисту інформації;

- контроль і оцінка ефективності вжитих заходів і застосовуваних засобів захисту;

- надання методичної допомоги співробітникам у питаннях забезпечення інформаційної безпеки;

- регулярна оцінка та управління ризиками інформаційної безпеки відповідно до встановлених процедур у сфері управління ризиками;

- вибір і впровадження засобів захисту інформації, включно з організаційними, фізичними, технічними, програмними та програмно-апаратними засобами забезпечення СУІБ;

- забезпечення мінімально-необхідного доступу до інформаційних ресурсів, ґрунтуючись на вимогах бізнес-процесів;

- інформування, навчання та підвищення кваліфікації працівників Підприємства у сфері інформаційної безпеки;

- розслідування інцидентів інформаційної безпеки;

- збір, накопичення, систематизація та обробка інформації з питань інформаційної безпеки;

- забезпечення необхідного рівня відмовостійкості ІТ-сервісів і доступності даних для підрозділів.

Для вирішення завдань, покладених на відділ ІБ, його співробітники мають такі права:

- визначати необхідність і розробляти нормативні документи, що стосуються питань забезпечення безпеки інформації, включно з документами, що регламентують діяльність користувачів інформаційної системи в зазначеній галузі;

- отримувати інформацію від користувачів інформаційних систем Підприємства з будь-яких аспектів застосування інформаційних технологій в Підприємстві;

- брати участь у опрацюванні технічних рішень з питань забезпечення безпеки інформації під час проектування та розроблення нових інформаційних технологій;

- брати участь у випробуваннях розроблених інформаційних технологій з питань оцінки якості реалізації вимог щодо забезпечення безпеки інформації;

- контролювати діяльність користувачів з питань забезпечення ІБ;

- готувати пропозиції керівництву щодо забезпечення вимог ІБ.

7. Область дії

7.1 Відповідальність за ресурси

В підприємстві мають бути виявлені та оцінені з погляду їх важливості всі ресурси. Для всіх цінних ресурсів має бути складено реєстр (перелік). Завдяки інформації про ресурси Підприємства реалізується захист інформації, ступінь якого співмірна цінності та важливості ресурсів.

В ІС Підприємства присутні такі типи ресурсів:

- інформаційні ресурси, що містять конфіденційну інформацію, та/або відомості обмеженого доступу, у тому числі інформацію про фінансову діяльність Підприємства;

- відкрито поширювана інформація, необхідна для роботи Підприємства, незалежно від форми та виду її подання;

- інформаційна інфраструктура, включно із системами оброблення та аналізу інформації, технічними та програмними засобами її оброблення, передавання та відображення, зокрема каналами інформаційного обміну та комунікаційними, системами та засобами захисту інформації, об'єктами і приміщеннями, в яких розміщені такі системи.

Для кожного ресурсу має бути призначений власник, який відповідає за відповідну класифікацію інформації та ресурсів, пов'язаних із засобами оброблення інформації, а також за призначення та періодичну перевірку прав доступу та категорій, визначених політиками управління доступом.

7.2 Класифікація інформації

Усі інформаційні ресурси, що підлягають захисту, мають бути класифіковані відповідно до важливості та ступеня доступу. Класифікація інформації має бути документована і затверджена керівництвом Підприємства.

Класифікація інформації повинна проводитися власником ресурсу, що зберігає або обробляє інформацію, для визначення категорії ресурсу. Періодично класифікація має переглядатися для підтримання актуальності її відповідності з категорією ресурсу.

Ресурси, що містять конфіденційну або критичну інформацію, повинні мати відповідну позначку (гриф).

7.3 Оцінювання та опрацювання ризиків

В підприємстві визначені вимоги до безпеки шляхом методичної оцінки ризиків. Оцінки ризиків мають виявити, визначити кількість і розташувати за пріоритетами ризики відповідно до критеріїв прийняття ризиків і бізнес-цілей підприємства. Результати оцінки визначають відповідну реакцію керівництва, пріоритети управління ризиками ІБ та набір механізмів контролю для захисту від цих ризиків.

Оцінка ризиків передбачає системне поєднання аналізу ризиків та оцінювання ризиків.

Крім того, оцінювання ризиків і вибір механізмів контролю мають здійснюватися періодично, щоб:

- врахувати зміни бізнес-вимог і пріоритетів;
- взяти до уваги нові загрози та вразливості;
- переконатися в тому, що реалізовані засоби зберегли свою ефективність.

Перед опрацюванням кожного ризику Установа має критерії для визначення можливості прийняття цього ризику. Ризик може бути прийнятий, якщо його величина є достатньо малою і вартість опрацювання є нерентабельною для Підприємства. Такі рішення реєструються у відповідних документах.

Для кожного з оцінених ризиків ухвалюватиметься одне з рішень щодо його обробки:

- застосування відповідних механізмів контролю для зменшення величини ризику до прийнятного рівня;

- свідоме та об'єктивне прийняття ризику, якщо він точно задовольняє Політиці Підприємства та критеріям прийняття ризиків;

- ухилення від ризику шляхом недопущення дій, що можуть бути його причиною;

- передача ризиків іншій стороні (аутсорсинг, страхування тощо).

7.4 Безпека персоналу

Ролі та обов'язки щодо забезпечення безпеки інформаційних ресурсів, описані відповідно до Політики ІБ Підприємства, повинні бути доведені до співробітника під час працевлаштування та внесені до його посадових обов'язків. Сюди входять як загальні обов'язки з реалізації та підтримки політики безпеки, так і конкретні обов'язки щодо захисту ресурсів і виконання конкретних операцій, пов'язаних із безпекою.

7.4.1 Умови найму

Усі співробітники, яких приймають на роботу, повинні схвалити і підписати свої трудові договори, в яких встановлюється їхня відповідальність за ІБ. До договору включено згоду співробітника на проведення контрольних заходів з боку Підприємства щодо перевірки виконання вимог ІБ, а також зобов'язання щодо нерозголошення конфіденційної інформації. У договорі описано заходи, які буде вжито в разі недотримання співробітником вимог ІБ.

Обов'язки щодо забезпечення ІБ мають бути включені до посадових інструкцій кожного співробітника Підприємства.

Усі співробітники, яких приймають, повинні бути ознайомлені під розпис із переліком інформації, обмеженого доступу, зі встановленим режимом роботи з нею та із заходами відповідальності за порушення цього режиму.

При наданні співробітнику доступу до ІС Підприємства він повинен ознайомитися під розпис з інструкцією користувача ІС.

7.4.2 Відповідальність керівництва

Керівництво Підприємства повинно вимагати від усіх співробітників, підрядників і користувачів сторонніх організацій вжиття заходів безпеки відповідно до встановлених в Підприємстві політик і процедур.

Уповноважені керівництвом Підприємства співробітники мають право в установленому порядку, без повідомлення користувачів, проводити перевірки:

- виконання чинних інструкцій з питань ІБ;

-даних, що знаходяться на носіях інформації;

- порядку використання співробітниками інформаційних ресурсів;

- змісту службового листування.

7.4.3 Навчання ІБ

Усі співробітники повинні проходити періодичну підготовку в галузі політики та процедур ІБ, прийнятих в Підприємстві. Цими підготовками займаються співробітник з ІБ. Періодичність таких заходів раз у квартал. Кожен такий захід документується.

7.4.4 Завершення або зміни трудових відносин

При звільненні всі надані співробітнику права доступу до ресурсів ІС повинні бути видалені. При зміні трудових відносин видаляються тільки ті права, необхідність в яких відсутня в нових відносинах.

7.5 Фізична безпека

7.5.1 Захищені області

Засоби обробки інформації, що підтримують критично важливі та вразливі ресурси Підприємства, розміщені в захищених областях. Такими засобами є: сервери, магістральне комунікаційне обладнання, телефонні станції, кросові панелі, обладнання, що забезпечує обробку та зберігання конфіденційної інформації.

Захищені області повинні забезпечуватися відповідними засобами контролю доступу, що забезпечують можливість доступу тільки авторизованого персоналу.

Забороняється приймання відвідувачів у приміщеннях, коли здійснюється обробка інформації обмеженого доступу.

Для зберігання службових документів і машинних носіїв із захищеною інформацією приміщення забезпечуються сейфами, металевими шафами або шафами, обладнаними замком.

Приміщення мають бути забезпечені засобами знищення документів.

7.5.2 Області загального доступу

Місця доступу, через які неавторизовані особи можуть потрапити до приміщень Підприємства, повинні контролюватися і, якщо це можливо, мають бути ізольовані від засобів обробки інформації з метою запобігання несанкціонованому доступу.

7.5.3 Допоміжні служби

Усі допоміжні служби, як-от електроживлення, водопостачання, каналізація, опалення, вентиляція та кондиціювання повітря, повинні забезпечувати гарантовану та стійку працездатність компонентів ІС Підприємства. Ці служби повинні систематично обслуговуватись.

7.5.4 Утилізація або повторне використання обладнання

З усіх носіїв інформації, якими укомплектоване обладнання, що утилізується, повинні гарантовано видалятися всі конфіденційні дані та ліцензійне ПЗ. Відсутність інформації, що захищається, на носіях має бути перевірена відділом ІБ Підприємства, про що має бути зроблена відмітка в акті списання.

7.5.5 Переміщення майна

Обладнання, інформація або ПЗ повинні переміщатися за межі Підприємства тільки за наявності письмового дозволу керівництва. Співробітники, які мають право переміщати обладнання та носії інформації за межі Підприємства, мають бути чітко визначені. Час переміщення обладнання за межі Підприємства та час його повернення повинні реєструватися

7.6 Контроль доступу

Основними користувачами інформації в інформаційній системі Підприємства є співробітники структурних підрозділів. Рівень повноважень кожного користувача визначається індивідуально. Кожен співробітник користується тільки визначеними йому правами стосовно інформації, з якою йому необхідно працювати відповідно до посадових обов'язків.

Допуск користувачів до роботи з інформаційними ресурсами має бути строго регламентований. Будь-які зміни складу і повноважень користувачів підсистем мають відбуватися в установленому порядку, згідно з регламентом надання доступу користувачів.

Кожному користувачеві, допущеному до роботи з конкретним інформаційним активом Підприємства, має бути співставлене персональне унікальне ім'я (обліковий запис користувача), під яким він реєструватиметься і працюватиме з ІР.

У разі виробничої необхідності деяким співробітникам можуть бути зіставлені кілька унікальних імен (облікових записів).

Тимчасовий обліковий запис може бути заведений для користувача на обмежений термін для виконання завдань, що вимагають розширених повноважень, або для проведення налаштування, тестування інформаційної системи, для організації гостьового доступу (відвідувачам, співробітникам сторонніх організацій, стажистам та іншим користувачам з тимчасовим доступом до інформаційної системи).

У загальному випадку заборонено створювати і використовувати загальний користувацький обліковий запис для групи користувачів. У випадках, коли це необхідно, зважаючи на особливості автоматизованого бізнес-процесу або організацію праці (наприклад, позмінне чергування), використання спільного облікового запису повинно супроводжуватися відміткою в журналі обліку машинного часу, яка повинна однозначно ідентифікувати поточного власника облікового запису в кожен момент часу. Одночасне використання одного спільного користувацького облікового запису користувача різними користувачами заборонено.

Облікові записи, що реєструються, поділяються на:

- користувацькі – призначені для автентифікації користувачів IP Підприємства;

- системні – використовувані для потреб операційної системи;

- службові – призначені для функціонування окремих процесів або додатків.

Системні облікові записи формуються операційною системою і повинні використовуватися тільки у випадках, визначених документацією на операційну систему.

Службові облікові записи використовуються тільки для запуску та роботи сервісів або додатків.

Використання системних або службових облікових записів для реєстрації користувачів у системі категорично заборонено.

Процедури реєстрації та блокування облікових записів користувачів мають застосовуватися з дотриманням таких правил:

- використання унікальних ідентифікаторів (ID) користувачів для однозначного визначення і зіставлення особистості з вчиненими нею діями;

- використання групових ID дозволяти тільки в разі, якщо це необхідно для виконання завдання;

- надання та блокування прав мають бути санкціоновані та документовані;

- надання прав доступу до IP, тільки після узгодження з власником даного IP;

- реєстрація та блокування облікових записів допускається з окремого дозволу керівництва Підприємства;

- рівень наданих повноважень має відповідати виробничій необхідності та цій Політиці і не ставити під загрозу розмежування режимів роботи;

- узгодження зміни прав доступу з відділом ІБ;

- документальна фіксація призначених користувачеві прав доступу;

- ознайомлення користувачів під підпис із письмовими документами, в яких регламентуються їхні права доступу;

- надання доступу з моменту завершення процедури реєстрації;

- забезпечення створення і підтримання формального списку всіх користувачів, зареєстрованих для роботи з IP або сервісом;

- негайне видалення або блокування прав доступу користувачів, які змінили посаду, форму зайнятості або звільнилися з Підприємства;

- аудит ID і облікових записів користувачів на наявність невикористовуваних, їх видалення та блокування;

- забезпечення того, щоб зайві ID користувачів не були доступні іншим користувачам;

- забезпечити можливість надання користувачам доступу відповідно до їхніх посад, що ґрунтуються на виробничих вимогах, шляхом підсумовування деякої кількості прав доступу в типові профілі доступу користувачів.

7.6.1 Керування привілеями

Доступ співробітника до інформаційних ресурсів Підприємства має бути санкціонований керівником структурного підрозділу, в якому значиться згідно зі штатним розписом цей співробітник, і власниками відповідних інформаційних ресурсів. Управління доступом здійснюється відповідно до встановлених процедур.

Наділення привілеями та їхнє використання має бути строго обмеженим і керованим. Розподіл привілеїв має управлятися за допомогою процесу реєстрації цих привілеїв. Мають бути розглянуті такі етапи:

- мають бути ідентифіковані привілеї доступу, пов'язані з кожним системним продуктом, наприклад, з операційною системою, системою управління базою даних і кожним додатком, а також користувачі, яким вони мають бути надані;

- привілеї повинні надаватися користувачам на підставі "виробничої необхідності" і тільки на період часу, необхідний для того, щоб для досягнення поставлених цілей, наприклад, привілеї, мінімально необхідні для виконання їхніх функціональних обов'язків, тільки тоді, коли ці привілеї необхідні;

- має бути забезпечено процес санкціонування всіх наданих привілеїв і створення звітів щодо них, привілеї не можна надавати до завершення процесу їхньої реєстрації;

- унікальні привілеї повинні присвоюватися на інший ID користувача, не той, який використовується під час звичайної роботи користувача.

Контроль і періодичний перегляд прав доступу користувачів до інформаційних ресурсів Підприємства здійснюється в процесі аудиту ІБ відповідно до правил аудиту ІБ та встановлених процедур.

7.6.2 Керування паролями

Паролі – засіб перевірки особи користувача для доступу до ІС або сервісу, що забезпечує ідентифікацію та автентифікацію на основі відомостей, відомих тільки користувачеві.

Надання паролів має контролюватися за допомогою офіційної процедури, що відповідає таким вимогам:

- усі користувачі мають бути ознайомлені під розпис із вимогою збереження в таємниці особистих і групових паролів;

- за наявності можливості, необхідно налаштувати систему таким чином, щоб під час першого входу користувача з призначеним йому тимчасовим паролем система відразу ж вимагала його змінити;

- тимчасові паролі повинні призначатися користувачеві тільки після його ідентифікації;

- необхідно уникати передавання паролів з використанням третіх осіб або незашифрованою електронною поштою;

- тимчасові паролі не повинні бути вгадуваними і повторюваними від користувача до користувача;

- користувач має підтвердити отримання пароля;

- паролі мають зберігатися в електронному вигляді тільки в захищеній формі;

- призначені виробником ПЗ паролі мають бути змінені відразу після завершення інсталяції;

- необхідно встановити вимоги до довжини пароля, набору символів і кількості спроб введення;

- необхідно змінювати паролі користувача не рідше одного разу на 90 днів.

За необхідності можна розглянути можливість використання інших технологій ідентифікації та автентифікації користувачів, зокрема, біометричних технологій, перевірки підпису та апаратних засобів (смарт-картки, e-Token/uaToken, чіпи тощо).

7.6.3 Контроль прав доступу

Щоб забезпечити ефективний контроль доступу, необхідно запровадити офіційний процес регулярної перевірки прав доступу користувачів, що відповідає таким вимогам:

- права доступу користувачів мають перевірятися через регулярні інтервали (нерідше ніж один раз на півроку), а також після внесення будь-яких змін до ІС;

- права доступу користувачів повинні перевірятися і перепризначатися при зміні їхніх посадових обов'язків в Підприємстві, а також при переході з однієї роботи на іншу в межах Підприємства;

- перевірка прав користувачів, які мають особливі привілеї для доступу в систему, має проводитися частіше (не рідше ніж один раз на 3 місяці);

- необхідно регулярно перевіряти адекватність призначених привілеїв, щоб уникнути отримання будь-ким із користувачів зайвих прав;

- зміна привілейованих облікових записів має протоколюватися.

Контроль над виконанням процедур управління доступом користувачів має включати:

- контроль над додаванням, видаленням и зміною ідентифікаторів, автентифікаційних даних та інших об'єктів ідентифікації;

- перевірку автентичності користувачів перед зміною паролів;

- негайне блокування прав доступу в разі звільнення;

- блокування облікових записів, неактивних понад 45 днів;

- увімкнення облікових записів, використовуваних постачальниками для віддаленої підтримки, тільки на час виконання робіт;

- відстеження віддалених облікових записів, використовуваних постачальниками, під час робіт;

- запобігання повторному використанню ідентифікатора користувача та (або) пристрою протягом щонайменше трьох років;

- ознайомлення з правилами та процедурами автентифікації всіх користувачів, які мають доступ до відомостей обмеженого поширення;

- використання механізмів автентифікації під час доступу до будь-якої бази даних, що містить відомості обмеженого розповсюдження, зокрема доступу з боку застосунків, адміністраторів і будь-яких інших користувачів;

- дозвіл запитів і прямого доступу до баз даних тільки для адміністраторів баз даних;

- блокування облікового запису на період, що дорівнює 30 хвилинам або до розблокування облікового запису адміністратором;

- блокування облікових записів користувачів у разі виявлення за результатами моніторингу (перегляду, аналізу) журналів реєстрації подій безпеки дій користувачів, які віднесені оператором до подій порушення безпеки інформації.

7.6.4 Використання паролів

Ідентифікатор і пароль користувача в ІС є обліковими даними, на підставі яких співробітнику Підприємства надаються права доступу, протоколюються дії, які він виконує в системі, і забезпечується режим конфіденційності, оброблюваної (створюваної, переданої та збереженої) співробітником інформації.

Не допускається використання різними користувачами одних і тих самих облікових даних.

Початкове значення пароля облікового запису користувача встановлює Адміністратор безпеки.

Особисті паролі встановлюються перший раз співробітниками відділу ІБ. Після першого входу в систему і надалі паролі обираються користувачами автоматизованої системи самостійно з урахуванням таких вимог:

1) довжина пароля має бути не менше 8 символів;

2) серед символів пароля мають бути присутні три з чотирьох видів символів:

2.1) букви у верхньому регістрі;

2.2) букви в нижньому регістрі;

2.3) цифри;

2.4) спеціальні символи (! @ # $ % ^ & * ( ) - _ + = ~ [ ] { } | \ : ; ' ' ' < > , . ? /);

3) пароль не повинен містити легко обчислювані поєднання символів, наприклад,

3.1) імена, прізвища, номери телефонів, дати;

3.2) послідовно розташовані на клавіатурі символи ("12345678", "QWERTY", тощо);

3.3) загальноприйняті скорочення ("USER", "TEST" тощо);

3.4) повсякденно використовуване слово, наприклад, імена або прізвища друзів, колег, акторів або казкових персонажів, клички тварин;

3.5) комп'ютерний термін, команда, найменування компаній, web сайтів, апаратного або програмного забезпечення;

3.6) що-небудь із перерахованого вище у зворотному написанні;

3.7) що-небудь із перерахованого вище з додаванням цифр на початку або наприкінці;

4) під час зміни пароля значення нового має відрізнятися від попереднього не менше ніж у 4 позиціях;

5) для різних ІС необхідно встановлювати власні, відмінні паролі.

Співробітнику рекомендується обирати пароль за допомогою такої процедури:

- обрати фразу, яку легко запам'ятати. Наприклад, "Рве та стогне Дніпр широкий";

- вибрати перші дві літери з кожного слова "рвтастдниш";

- набрати отриману послідовність, переключившись на англійську розкладку клавіатури: "hdnfcnlyib";

- вибрати номер символу, який записуватиметься у верхньому регістрі та після якого буде спеціальний символ. Наприклад, це буде п'ятий символ, а як спеціальний символ обрано "%". Отримуємо: " hdnF%cnlyib ".

Співробітникові забороняється:

- повідомляти свій пароль будь-кому;

- вказувати пароль у повідомленнях електронної пошти;

- зберігати паролі, записані на папері, у легко доступному місці;

- використовувати той самий пароль, що і для інших систем (наприклад, домашній інтернет провайдер, безкоштовна електронна пошта, форуми тощо);

- використовувати один і той самий пароль для доступу до різних корпоративних ІС.

Вхід користувача в систему не повинен виконуватися автоматично. Залишаючи робоче місце, користувач зобов'язаний заблокувати комп'ютер (використовуючи комбінації Win + "L" або Ctrl + Alt + Delete → "Блокувати комп'ютер").

Співробітник зобов'язаний:

- у разі підозри на те, що пароль став кому-небудь відомим, поміняти пароль і повідомити про факт компрометації співробітнику відділу ІБ;

- негайно повідомити співробітника відділу ІБ у разі отримання від будь-кого прохання повідомити пароль;

- змінювати пароль кожні 90 днів;

- змінювати пароль на вимогу Адміністратора ІБ.

Після 5 невдалих спроб введення пароля обліковий запис блокується на 10 хвилин. У разі систематичного блокування облікового запису працівником (понад 3 рази) сповіщається Адміністратор ІБ.

Установа залишає за собою право:

- здійснювати періодичну перевірку стійкості паролів користувачів, що використовуються співробітниками для доступу до ІС;

- вживати заходів дисциплінарного характеру до співробітників, які порушують положення цієї політики.

7.6.5 Користувацьке обладнання, що залишається без нагляду

Користувачі повинні забезпечувати необхідний захист обладнання, що залишається без нагляду. Усі користувачі мають бути обізнані про вимоги ІБ і правила захисту обладнання, що залишається без нагляду, а також про свої обов'язки щодо забезпечення цього захисту.

7.6.6 Політика чистого столу

Співробітники Підприємства зобов'язані:

- зберігати відомі їм паролі в таємниці;

- закривати активні сеанси після завершення роботи, якщо тільки їх не можна захистити відповідним блокувальним механізмом, наприклад, захищений паролем хранитель екрана;

- після завершення сеансу виходити із системи в універсальних ЕОМ, серверів і офісних ПК.

Забороняється вести запис паролів (наприклад, на папері, у програмному файлі або в кишеньковому пристрої), за винятком випадків, коли запис може зберігатися безпечно, а метод зберігання було затверджено.

Документи і носії з конфіденційною інформацією повинні прибиратися в місця, що замикаються (сейфи, шафи тощо), особливо, коли ви йдете з робочого місця.

Комп'ютери та термінали мають бути залишені в стані виконаного виходу із системи, коли вони перебувають без нагляду.

Вхід користувача в систему не повинен виконуватися автоматично. Залишаючи робоче місце, користувач зобов'язаний заблокувати комп'ютер (використовуючи комбінації Win + "L" або Ctrl + Alt + Delete → "Блокувати комп'ютер").

7.6.7 Мобільне комп'ютерне обладнання

Під час використання мобільних засобів (наприклад, ноутбуків, планшетів і мобільних телефонів) необхідно дотримуватися особливих запобіжних заходів, щоб не допустити компрометації інформації, що належить Підприємстві. Необхідно прийняти офіційну політику, що враховує ризик, пов'язаний з використанням мобільних комп'ютерів, і зокрема з роботою в незахищеному середовищі.

7.7 Політика допустимого використання інформаційних ресурсів

Загальні обов'язки користувача:

- під час роботи з ПЗ керуватися нормативною документацією (керівництвом користувача);

- звертатися до служби підтримки користувачів або до фахівців, призначених відповідальними за системне адміністрування та інформаційну безпеку, з усіх технічних питань, пов'язаних із роботою в корпоративній ІС (підключення до корпоративної ІС/домену, інсталяція та налаштування ПЗ, видалення вірусів, надання доступу в мережу Інтернет і до внутрішніх мережевих ресурсів, ремонт і технічне обслуговування тощо), а також за необхідною методологічною/консультаційною допомогою з питань застосування технічних і програмних засобів корпорації.

- знати ознаки правильного функціонування встановлених програмних продуктів і засобів захисту інформації;

- мінімізувати виведення на друк оброблюваної інформації.

Користувачеві заборонено здійснювати несанкціоноване розповсюдження довідкової інформації, яка стає доступною при підключенні до корпоративної ІС Підприємства.

7.7.1 Використання ПЗ

На ІКС охоронного підприємства допускається використання тільки ліцензійного програмного забезпечення, затвердженого в переліку дозволеного програмного забезпечення .

Заборонено незаконне зберігання на жорстких дисках ІКС охоронного підприємства інформації, що є об'єктом авторського права (ПЗ, фотографії, музичні файли, ігри тощо).

Рішення про придбання та встановлення програмного забезпечення, необхідного для реалізації охоронних, фінансових, адміністративно-господарських

та інших завдань приймає фінансовий директор після обґрунтування в необхідності одним з завідуючих відділом підприємства, в якому вона з'явилася.

Документи, що підтверджують купівлю програмного забезпечення, зберігаються в бухгалтерії протягом усього часу використання ліцензії, копії зазначених документів разом з ліцензійними угодами на ПЗ, ключами захисту ПЗ і дистрибутивами зберігаються в технічному відділі.

Користувачі ІКС не мають права видаляти, змінювати, доповнювати, оновлювати програмну конфігурацію на ІКС охоронного підприємства. Зазначені роботи, а також роботи зі встановлення, реєстрації та активації придбаного ліцензійного ПЗ можуть бути виконані тільки співробітниками технічного відділу.

Відомості про новопридбане програмне забезпечення мають бути внесені до переліку дозволеного програмного забезпечення.

7.7.2 Використання ІКС та ІС

До роботи в ІС Підприємства допускаються особи, які призначені на відповідну посаду та пройшли інструктаж з питань інформаційної безпеки.

Кожному співробітнику Підприємства, якому необхідний доступ до ІР у рамках його посадових обов'язків, видаються під розпис необхідні засоби. Відповідальність за встановлення та підтримку всіх комп'ютерних систем, що функціонують в Підприємстві, покладено на технічний відділ.

Кожен співробітник Підприємства, забезпечений ІКС, отримує персональне мережеве ім'я, пароль, адресу електронної пошти та особистий каталог у мережі, який призначений для зберігання робочих файлів.

Роботу в ІС співробітникам дозволено тільки на закріплених за ними ІР, у певний час і тільки з дозволеним програмним забезпеченням і мережевими ресурсами.

Усі ІКС, встановлені в Підприємстві, мають уніфікований набір офісних програм, призначених для отримання, оброблення та обміну інформацією, визначений у стандарті робочих місць Підприємства. Зміна встановленої

конфігурації можлива після внесення відповідних поправок до стандарту робочих місць або за службовою запискою, погодженою з відділом ІБ. Комплектація персональних комп'ютерів апаратними та програмними засобами, а також розташування комп'ютерів контролюється відділом ІБ.

Самостійне встановлення програмного забезпечення на ІКС заборонено. Встановлення і видалення будь-якого програмного забезпечення здійснюється тільки співробітниками технічного відділу.

У разі виявлення несправності комп'ютерного обладнання або програмного забезпечення, користувач має звернутися до технічного відділу.

Співробітники технічного відділу та ІБ мають право здійснювати контроль над встановленим на комп'ютері програмним забезпеченням і вживати заходів щодо обмеження можливостей несанкціонованого встановлення програм.

Передача документів усередині Підприємства здійснюється тільки за допомогою загальних папок, а також засобами електронної пошти. Під час роботи в ІКС Підприємства співробітник зобов'язаний:

1) знати та виконувати вимоги внутрішніх організаційно-розпорядчих документів Підприємства;

2) використовувати ІКС Підприємства виключно для виконання своїх службових обов'язків;

3) ставити до відома відділ ІБ про будь-які факти порушення вимог ІБ;

4) ставити до відома технічний відділ про будь-які факти збоїв ПЗ, некоректного завершення значущих операцій, а також пошкодження технічних засобів;

5) негайно виконувати приписи технічного відділу та ІБ Підприємства.

6) Надавати ІКС співробітникам відділу ІБ для контролю;

7) За необхідності припинення роботи на деякий час коректно закривати всі активні завдання, блокувати ІКС;

8) У разі необхідності продовження роботи після закінчення робочого дня проінформувати про це відділ ІБ.

При використання ІКС Підприємства забороняється

1) використовувати ІКС в особистих цілях;

2) відключати засоби управління та засоби захисту, встановлені на робочій станції;

3) передавати:

3.1) конфіденційну інформацію за винятком випадків, коли це входить до службових обов'язків і спосіб передачі є безпечним, погодженим з відділом ІБ;

3.2) інформацію, файли або ПЗ, здатні порушити або обмежити функціональність будь-яких програмних і апаратних засобів, а також посилання на вищевказані об'єкти;

3.3) загрозливу, наклепницьку, непристойну інформацію;

4) самовільно вносити зміни в конструкцію, конфігурацію, розміщення ІКС та інших вузлів ІС Підприємства;

5) надавати співробітникам Підприємства (за винятком адміністраторів ІС та ІБ) і третім особам доступ до свого ІКС;

6) запускати на ІКС ПЗ, що не входить до Реєстру дозволеного до використання ПЗ;

7) захищати інформацію способами, не погодженими з відділом ІБ заздалегідь;

8) самостійно підключати робочу станцію та інші технічні засоби до корпоративної ІС Підприємства;

9) здійснювати пошук засобів і шляхів пошкодження, знищення технічних засобів і ресурсів ІС або здійснювати спроби несанкціонованого доступу до них;

10) використовувати для виконання службових обов'язків локальні (не доменні) облікові записи ІКС.

Інформація про відвідувані ресурси ІС протоколюється і, за необхідності, може бути представлена Керівникам структурних підрозділів, а також Керівництву Підприємства.

Усі електронні повідомлення та документи в електронному вигляді, що передаються за допомогою ІС Підприємства, підлягають обов'язковій перевірці на відсутність шкідливого ПЗ.

7.7.3 Використання ресурсів локальної мережі

Для виконання своїх службових обов'язків кожен співробітник забезпечується доступом до відповідних інформаційних ресурсів. Інформаційними ресурсами є каталоги та файли, що зберігаються на дисках серверів Підприємства, бази даних, електронна пошта.

Основними робочими каталогами є особисті каталоги співробітників і каталоги підрозділів, створені відповідно до особливостей їхньої роботи. Доступ співробітників до ресурсів мережі здійснюється згідно з матрицею доступу. Тимчасове розширення прав доступу здійснюється відділом ІБ Підприємства відповідно до Порядку надання(зміни) повноважень користувача.

7.7.4 Обробка конфіденційної інформації

При обробці конфіденційної інформації співробітники зобов'язані:

1) знати і виконувати вимоги інструкції по роботі з конфіденційною інформацією;

2) за необхідності розміщувати конфіденційну інформацію на відкритому ресурсі корпоративної мережі Підприємства застосовувати засоби захисту від неавторизованого доступу;

3) розміщувати екран монітора таким чином, щоб унеможливити перегляд оброблюваної інформації сторонніми особами;

4) не відправляти на друк конфіденційні документи, якщо відсутня можливість контролю виведення на друк і вилучення надрукованих документів із принтера одразу після закінчення друку;

5) обов'язково перевіряти адреси одержувачів електронної пошти на предмет правильності їхнього вибору;

6) не запускати виконувані файли на знімних накопичувачах, отримані не з довіреного джерела;

7) не передавати конфіденційну інформацію відкритими каналами зв'язку, крім мереж корпоративної ІС;

не залишати без особистого нагляду на робочому місці або де б то не було електронні носії інформації (CD/DVD-диски, Flash-пристрої тощо), а також роздруки з принтера або паперові копії документів, що містять конфіденційну інформацію.

7.7.5 Використання електронної пошти

Електронна пошта використовується для обміну в межах ІС Підприємства та загальнодоступних мереж інформацією у вигляді електронних повідомлень і документів в електронному вигляді.

Для забезпечення функціонування електронної пошти допускається застосування ПЗ, що входить до реєстру дозволеного до використання ПЗ.

При роботі з корпоративною електронною поштою Підприємства користувач повинен враховувати:

- електронна пошта не є засобом гарантованої доставки відправленого повідомлення до адресата;

- електронна пошта не є засобом передавання інформації, що гарантує конфіденційність переданої інформації (передавання конфіденційної інформації поза локальною мережею Підприємства необхідно здійснювати тільки в зашифрованому вигляді);

- електронна пошта не є засобом передавання інформації, що гарантовано ідентифікує відправника повідомлення.

Організацією та забезпеченням порядку роботи електронної пошти в Підприємстві займається відділ ІБ. Кожен співробітник Підприємства отримує поштову адресу виду name@hotmail.com у домені Підприємства. Адреса електронної пошти видається співробітником відділу ІБ під час початкової

реєстрації користувача в домені Підприємства. Корпоративна електронна пошта Підприємства призначена виключно для використання у службових цілях.

Функціонування електронної пошти забезпечується обладнанням, каналами зв'язку та іншими ресурсами, що належать Підприємстві. Усі поштові повідомлення, передані або прийняті з використанням корпоративної електронної пошти належать Підприємстві та є невід'ємною частиною її виробничого процесу.

Будь-які повідомлення корпоративної електронної пошти можуть бути прочитані, використані в інтересах Підприємства або видалені уповноваженими співробітниками Підприємства.

Користувачам корпоративної електронної пошти Підприємства заборонено вести приватне листування з використанням засобів корпоративної електронної пошти Підприємства. До приватного листування належить листування, не пов'язане з виконанням співробітником своїх посадових обов'язків.

Використання корпоративної електронної пошти Підприємства для приватного листування співробітником, належним чином ознайомленим з цією Політикою, є порушенням трудової дисципліни Підприємства. Підписуючись в ознайомленні з цією Політикою, співробітник дає згоду на ознайомлення та інше використання в інтересах Підприємства його листування, здійснюваного з використанням корпоративної електронної пошти, і погоджується з тим, що будь-яке використання його листування, здійснюваного з використанням корпоративної електронної пошти, не може розглядатися як порушення таємниці зв'язку.

Кожен співробітник Підприємства має право на перегляд або інше використання в інтересах Підприємства повідомлень корпоративної електронної пошти, що надіслані або отримані ним, відповідно, з його або на його корпоративну електронну адресу.

Використання повідомлень корпоративної електронної пошти здійснюється уповноваженими співробітниками Підприємства відповідно до їхніх функцій, визначених у цій Політиці та в інших локальних нормативних актах Підприємства. Перегляд та інше використання повідомлень електронної пошти в інтересах

Підприємства здійснюється співробітниками Підприємства з метою забезпечення захисту конфіденційних відомостей, забезпечення нормальної працездатності системи електронної пошти, в рамках обслуговування сервісів електронної пошти, при виконанні ручного пересилання повідомлень, що надходять на корпоративні електронні адреси Підприємства співробітникам або групам співробітників, а також за вмотивованим запитом прямих або безпосередніх керівників будь-яких співробітників, чию пошту необхідно переглядати, а також за мотивованим запитом будь-яких керівників.

Використання повідомлень корпоративної електронної пошти в інтересах Підприємства, у тому числі ознайомлення зі змістом повідомлень, здійснюється відповідно до прав доступу до інформації, встановлених внутрішніми Положеннями про конфіденційну інформацію та іншими правовими актами, що регламентують порядок поводження з інформацією обмеженого доступу. Вихідні електронні повідомлення співробітників Підприємства повинні містити такі поля:

- адреса одержувача;
- тема електронного повідомлення;
- текст електронного повідомлення (вкладені файли);
- підпис відправника;
- попередження про службовий характер повідомлення та його конфіденційність.

Формат підпису відправника:

З повагою,

<Прізвище ім'я>

<Посада>

<Структурний підрозділ>

<Назва Підприємства>

<Адреса>

<номери контактів: телефон, месенджери, адреси електронної пошти>

<сайт>

Формат попередження про службовий характер повідомлення та його конфіденційність:

"Це електронне повідомлення та будь-які документи, додані до нього, містять конфіденційну інформацію. Цим повідомляємо Вас про те, що якщо це повідомлення не призначене Вам, використання, копіювання, розповсюдження інформації, що міститься в цьому повідомленні, а також здійснення будь-яких дій на основі цієї інформації, суворо заборонене та захищається законодавством. Якщо Ви отримали це повідомлення помилково, будь ласка, повідомте про це відправника електронною поштою та видаліть це повідомлення. CONFIDENTIALITY NOTICE: Цей електронний лист і будь-які файли, прикріплені до нього, є конфіденційними. Якщо ви не є передбачуваним одержувачем, ви повідомляєте, що використання, копіювання, розповсюдження або вчинення будь-яких дій, які спираються на вміст цієї інформації, категорично заборонені та охороняються законами. Якщо ви отримали цей електронний лист помилково, будь ласка, повідомте про це відправника та видаліть цей лист". Під час формування відповідей на отримані електронні повідомлення можна використовувати такий спрощений підпис:

З повагою,

<Прізвище ім'я>

<Номера телефонів, месенджери, адреси електронної пошти>

У разі отримання службового повідомлення про неможливість доставки повідомлення адресату або отримання повідомлення від адресата про те, що він не отримав відправлене йому повідомлення, необхідно зв'язатися зі співробітником відділу ІБ.

Відмова від подальшого надання співробітнику Підприємства послуг електронної пошти може бути викликана порушеннями вимог цієї політики. Припинення надання співробітнику Підприємства послуг електронної пошти настає при припиненні дії трудового договору (контракту) співробітника.

7.7.6 Робота в мережі Інтернет

Доступ до мережі Інтернет надається співробітникам Підприємства з метою виконання ними своїх службових обов'язків, що вимагають безпосереднього підключення до зовнішніх інформаційних ресурсів.

Для доступу співробітників Підприємства до мережі Інтернет допускається застосування ПЗ, що входить до Реєстру дозволеного до використання ПЗ.

При використанні мережі Інтернет необхідно:

1) дотримуватися вимог цієї Політики;

2) використовувати мережу Інтернет виключно для виконання своїх службових обов'язків;

3) ставити до відома відділ ІБ про будь-які факти порушення вимог цієї Політики;

При використанні мережі Інтернет заборонено:

1) використовувати наданий Установою доступ до мережі Інтернет в особистих цілях;

2) використовувати несанкціоновані апаратні и програмні засоби, що дають змогу отримати несанкціонований доступ до мережі Інтернет;

3) здійснювати будь-які дії, спрямовані на порушення нормального функціонування елементів ІС Підприємства;

4) публікувати, завантажувати та поширювати матеріали, що містять:

4.1) Конфіденційну інформацію, а також інформацію, що становить комерційну таємницю, за винятком випадків, коли це входить до посадових обов'язків і спосіб передавання є безпечним, погодженим з відділом ІБ;

4.2) загрозливу, наклепницьку, непристойну інформацію;

4.3) шкідливе ПЗ, призначене для порушення, знищення або обмеження функціональності будь-яких апаратних і програмних засобів, для здійснення несанкціонованого доступу, а також посилання на нього;

4.4) фальсифікувати свою IP-адресу, а також іншу службову інформацію.

Установа залишає за собою право блокувати або обмежувати доступ користувачів до Інтернет-ресурсів, зміст яких не має відношення до виконання службових обов'язків, а також до ресурсів, зміст і спрямованість яких заборонені законодавством.

Блокування та обмеження доступу користувачів до Інтернет-ресурсів здійснюється на основі Регламенту застосування категорій Інтернет-ресурсів.

Інформація про Інтернет-ресурси, які відвідують співробітники Підприємства, протоколюється для подальшого аналізу і, за необхідності, може бути подана Керівникам структурних підрозділів, а також Керівництву Підприємства для контролю.

Зміст Інтернет-ресурсів, а також файли, що завантажуються з мережі Інтернет, підлягають обов'язковій перевірці на відсутність шкідливого ПЗ.

7.7.7 Використання мобільних пристроїв

Під використанням мобільних пристроїв і носіїв інформації в ІС Підприємства розуміють їхнє підключення до інфраструктури ІС з метою оброблення, приймання/передавання інформації між ІС і мобільними пристроями, а також носіями інформації.

На наданих Установою мобільних пристроях допускається використання ПЗ, що входить до Реєстру дозволеного до використання ПЗ.

До наданих Установою мобільних пристроїв і носіїв інформації висуваються ті самі вимоги ІБ, що й для стаціонарних ІКС. Доцільність додаткових заходів забезпечення ІБ визначається відділом ІБ.

Під час використання наданих Установою мобільних пристроїв і носіїв інформації, співробітник зобов'язаний:

- дотримуватися вимог цієї Політики;

- використовувати мобільні пристрої та носії інформації виключно для виконання своїх службових обов'язків;

- ставити до відома відділ ІБ про будь-які факти порушення вимог цієї Політики;

- експлуатувати и транспортувати мобільні пристрої и носії інформації відповідно до вимог виробників;

- забезпечувати фізичну безпеку мобільних пристроїв і носіїв інформації всіма розумними способами;

- сповіщати відділ ІБ про факти втрати (крадіжки) мобільних пристроїв і носіїв інформації.

Під час використання наданих співробітника Підприємства мобільних пристроїв і носіїв інформації заборонено:

- використовувати мобільні пристрої та носії інформації в особистих цілях;

- передавати мобільні пристрої та носії інформації іншим особам (за винятком адміністраторів ІС та ІБ);

- залишати мобільні пристрої та носії інформації без нагляду, якщо не вжито заходів щодо забезпечення їхньої фізичної безпеки.

Будь-яка взаємодія (обробка, приймання\передавання інформації), ініційована співробітником Підприємства між ІС і неврахованими (особистими) мобільним і пристроями, а також носіями інформації, розглядається як несанкціонована (за винятком випадків, обумовлених з адміністраторами ІС заздалегідь). Заклад залишає за собою право блокувати або обмежувати використання таких пристроїв і носіїв інформації;

Інформація про використання співробітниками Підприємства мобільних пристроїв і носіїв інформації в ІС протоколюється і, за необхідності, може бути представлена Керівникам структурних підрозділів, а також керівництву Підприємства.

Інформація, що зберігається на мобільних пристроях і носіях інформації, які надаються Установою, підлягає обов'язковій перевірці на відсутність шкідливого ПЗ.

У разі звільнення, надані йому мобільні пристрої та носії інформації вилучаються.

7.7.8 Захист від шкідливого ПЗ

Відділ ІБ регулярно перевіряє мережеві ресурси Підприємства антивірусним програмним забезпеченням і забезпечує захист вхідної електронної пошти від проникнення вірусів та іншого шкідливого ПЗ.

У разі виникнення підозри на наявність комп'ютерного вірусу (нетипова робота програм, поява графічних і звукових ефектів, викривлень даних, пропажа файлів, часта поява повідомлень про системні помилки, збільшення вихідного/вхідного трафіку тощо) працівник Підприємства має негайно сповістити про це відділ ІБ. Після чого адміністратор ІБ повинен провести позачергову повну перевірку на віруси робочої станції користувача, перевіривши насамперед працездатність антивірусного ПЗ.

В випадок виявлення під час проведенні антивірусної перевірки заражених комп'ютерними вірусами файлів співробітники підрозділів зобов'язані:

- призупинити роботу;

- негайно довести до відома про факт виявлення зараження свого керівника і відділ ІБ, а також власника файлу і суміжні підрозділи, які використовують ці файли в роботі.

- спільно з власником заражених вірусом файлів провести аналіз необхідності подальшого їх використання.

Для попередження вірусного зараження рекомендується:

- ніколи не відкривати файли і не виконувати макроси, отримані в поштових повідомленнях від невідомого або підозрілого відправника. Видаляти підозрілі вкладення, не відкриваючи їх, і очищати кошик, де зберігаються видалені повідомлення;

- видаляти спам, рекламу та інші непотрібні повідомлення;

- ніколи не завантажувати файли та програмне забезпечення з підозрілих або невідомих джерел;

- періодично резервувати важливі дані та системну конфігурацію, зберігати резервні копії в безпечному місці.

7.8 Придбання, розробка та обслуговування систем

7.8.1 Вимоги безпеки для інформаційних систем

Під час опису вимог до створення нових систем або до вдосконалення наявних необхідно враховувати потребу в засобах забезпечення безпеки.

Вимоги до безпеки та засоби захисту повинні відповідати цінності використовуваних ІР і потенційним збиткам для Підприємства в разі збою або порушення безпеки. Основою для аналізу вимог до безпеки та вибору заходів для підтримки безпеки є оцінка ризиків та управління ризиками.

Системні вимоги до ІБ і процесів, що забезпечують захист інформації, мають бути включені на ранніх стадіях проектування ІС.

7.8.2 Коректне опрацювання інформації

Дані, що вводяться в прикладні системи, необхідно перевіряти, щоб гарантувати їх правильність і відповідність поставленому завданню.

7.8.3 Криптографічні засоби

Усі ЗКЗІ, що надходять до Підприємства, мають бути обліковані у відповідному журналі поекземплярного обліку ЗКЗІ.

В Підприємстві має здійснюватися управління ключами для ефективного застосування криптографічних методів. Компрометація або втрата криптографічних ключів може призвести до порушення конфіденційності, автентичності та/або цілісності інформації.

Усі ключі мають бути захищені від зміни, втрати та знищення. Крім того, секретні та закриті ключі мають бути захищені від несанкціонованого розкриття.

Обладнання, що використовується для генерації, зберігання та архівування ключів, має бути фізично захищене.

Угоди із зовнішніми постачальниками криптографічних послуг (наприклад, засвідчуваними центрами) щодо рівня сервісу, що надається, мають охоплювати питання відповідальності, надійності сервісу та часу реакції під час надання сервісу.

Криптографічні системи та методи слід використовувати для захисту конфіденційної інформації, коли інші засоби контролю не забезпечують адекватного захисту.

Для критичної інформації повинно використовуватися шифрування під час їхнього зберігання в базах даних або передачі комерційними чи відкритими мережами, такими як Інтернет. Шифрування будь-якої іншої інформації в ІС Підприємства має здійснюватися лише після отримання письмового дозволу на це.

7.8.3.1 Вимог щодо забезпечення ІБ під час використання ЗКЗІ

Шифрування - це криптографічний метод, який може використовуватися для забезпечення захисту конфіденційної, важливої або критичної інформації.

ЗКЗІ повинні постачатися розробниками з повним комплектом експлуатаційної документації, що містить опис ключової системи, правила роботи з нею та обґрунтування необхідного організаційно-штатного забезпечення. Порядок застосування ЗКЗІ визначається керівництвом Підприємства і має включати:

- порядок введення в дію, включно з процедурами вбудовування ЗКЗІ в ІС;
- порядок експлуатації;
- порядок відновлення працездатності в аварійних випадках;
- порядок внесення змін;
- порядок зняття з експлуатації;
- порядок управління ключовою інформацією;

- порядок поводження з ключовою інформацією, включно з діями у разі зміни та компрометації ключів.

Для шифрування конфіденційної інформації мінімально допустимою довжиною ключа є 128 біт.

Під час використання шифрування в ІС Підприємства мають застосовуватися тільки затверджені стандартні алгоритми і сертифіковані продукти, що їх реалізують.

7.8.3.2 Кваліфікований електронний підпис

КЕП забезпечують захист автентифікації та цілісності електронних документів.

КЕП можуть застосовуватися для будь-якої форми документа, оброблюваного електронним способом. КЕП має бути реалізовано з використанням криптографічного методу, що ґрунтується на однозначно пов'язаній парі ключів, де один ключ використовується для створення підпису (секретний/особистий ключ), а інший – для перевірки підпису (відкритий ключ).

Необхідно з особливою ретельністю забезпечувати конфіденційність особистого ключа, який слід зберігати в секреті, оскільки будь-хто, хто має до нього доступ, може підписувати документи (платежі, контракти), тим самим фальсифікуючи підпис власника ключа. Захисту цілісності відкритого ключа має забезпечуватися під час використання сертифіката відкритого ключа.

Криптографічні ключі, що використовуються для цифрових підписів, мають відрізнятися від тих, які використовуються для шифрування. Під час використання КЕП необхідно враховувати вимоги чинного державного законодавства, що визначає умови, за яких цифровий підпис має юридичну силу.

7.8.3.3 Керування ключами

Управління криптографічними ключами важливе для ефективного використання криптографічних засобів.

Будь-яка компрометація або втрата криптографічних ключів може призвести до компрометації конфіденційності, автентичності та/або цілісності інформації. Слід застосовувати систему захисту для забезпечення використання в ІС Підприємства криптографічних методів щодо відкритих ключів, де кожний користувач має пару ключів, відкритий ключ (який може бути показаний будь-кому) та особистий ключ (який має зберігатися в секреті).

Методи з відкритими ключами повинні використовуватися для шифрування і для генерації цифрових підписів. Ключі необхідно захищати від зміни та руйнування, а секретним і особистим ключам необхідний захист від неавторизованого розкриття.

Криптографічні методи можуть також використовуватися для цієї мети. Фізичний захист слід застосовувати для захисту обладнання, що використовується для виготовлення, зберігання та архівування ключів. Сервер сертифікованого центру ЦСК повинен зберігати поточні відкриті ключі для всіх авторизованих на це співробітників. Для безпечної взаємодії із зовнішніми користувачами ІС

Підприємства необхідно використовувати електронні сертифікати тільки із затвердженого списку сертифікованих центрів. Секретні ключі користувачів повинні зберігатися так само, як і паролі. Про будь-яку підозру на компрометацію секретного ключа користувач повинен негайно доповісти у відділ ІБ.

Необхідно, щоб система забезпечення безпеки використання ключів ґрунтувалася на узгодженні способів, процедур і безпечних методів для:

- генерації ключів під час використання різних криптографічних систем і додатків;

- генерації та отримання сертифікатів відкритих ключів;

- розсилки ключів, призначених користувачам, включно з інструкціями щодо їх активації під час отримання;

- зберігання ключів (при цьому необхідна наявність інструкції авторизованим користувачам для отримання доступу до ключів);

- зміни або оновлення ключів, включно з правилами порядку та строків зміни ключів;

- порядку дій щодо скомпрометованих ключів;

- анулювання ключів, зокрема способи анулювання або дезактивації ключів, якщо ключі були скомпрометовані або користувач звільнився з організації (у цьому разі ключі необхідно архівувати);

- відновлення ключів, які були загублені або зіпсовані, для розсекречення зашифрованої інформації;

- архівування та резервного копіювання ключів;

- руйнування ключів;

- реєстрація ключів та аудиту дій, пов'язаних з управлінням ключами.

Для зменшення ймовірності компрометації, для ключів необхідно визначити дати початку та кінця дії, щоб їх можна було використовувати лише протягом обмеженого періоду часу, який залежить від обставин використання криптографічних засобів, контролю та від ступеня ризику розкриття інформації. Може знадобитися наявність процедур опрацювання юридичних запитів, що стосуються доступу до криптографічних ключів, наприклад, щоб зашифрована інформація стала доступною в незашифрованому вигляді для доказів у суді.

Необхідно забезпечувати захист відкритих ключів від загроз підроблення цифрового підпису та заміни відкритого ключа користувача своїм. Ця проблема вирішується за допомогою сертифіката відкритих ключів. Сертифікати необхідно виготовляти в такий спосіб, який однозначно пов'язував би інформацію, що відноситься до власника пари відкритого/секретного ключів, з відкритим ключем. Тому важливо, щоб процесу управління, в рамках якого формуються ці сертифікати, можна було довіряти. Угоди із зовнішніми постачальниками криптографічних послуг (наприклад, із засвідчуваними центрами) щодо рівня сервісу, що надається, мають охоплювати питання відповідальності, надійності сервісу та часу реакції під час надання сервісу.

7.8.4 Безпека системних файлів

Щоб звести до мінімуму ризик пошкодження ІС, в підприємстві необхідно забезпечити контроль над впровадженням ПЗ у робочих системах.

Тестові дані мають перебувати під контролем і захистом. Для випробувань зазвичай потрібні значні обсяги тестових даних, які максимально близько відповідають робочим даним. Необхідно уникати використання робочих баз даних, що містять конфіденційну інформацію. Якщо ці бази все ж будуть використовуватися, то конфіденційні дані мають бути видалені або змінені.

7.8.5 Безпека процесу розроблення та обслуговування систем

Щоб звести до мінімуму ймовірність пошкодження ІС Підприємства, слід запровадити суворий контроль над внесенням змін. Необхідно встановити офіційні правила внесення змін. Ці правила повинні гарантувати, що процедури, пов'язані з безпекою і контролем, не будуть порушені, що програмісти, які займаються підтримкою, отримають доступ тільки до тих частин системи, які необхідні для їхньої роботи, і що для виконання будь-якої зміни потрібно отримати офіційний дозвіл і підтвердження.

Після внесення змін до ІС критичні для бізнес-процесів Підприємства додатки мають аналізуватися та тестуватися, щоб гарантувати відсутність шкідливих наслідків для безпеки Підприємства. Слід перешкоджати внесенню змін до пакетів ПЗ, за винятком необхідних змін. Усі зміни мають суворо контролюватися.

7.9 Управління інцидентами інформаційної безпеки

В Підприємстві має бути розроблено та затверджено формальну процедуру повідомлення про події у сфері ІБ, а також процедуру реагування на такі події, що містить у собі дії, які мають виконуватися при надходженні повідомлень про подію.

Усі співробітники мають бути ознайомлені з процедурою повідомлення, а в їхні обов'язки має входити максимально швидке передання інформації про події.

На додаток до повідомлення про події ІБ і недоліки безпеки має використовуватися моніторинг систем, повідомлень і вразливостей для виявлення інцидентів ІБ. Цілі управління інцидентами ІБ мають бути узгоджені з керівництвом для врахування пріоритетів Підприємства при поводженні з інцидентами. Необхідно створити механізми, що дають змогу оцінювати і відстежувати типи інцидентів, їхній масштаб і пов'язані з ними витрати.

7.10 Управління безперервністю та відновленням

Необхідно розробити контрольований процес для забезпечення та підтримки безперервності бізнес-процесів Підприємства. Цей процес має об'єднувати в собі основні елементи підтримки безперервності бізнес-процесів.

В Підприємстві мають бути розроблені та реалізовані плани, що дадуть змогу продовжити або відновити операції та забезпечити необхідний рівень доступності інформації у встановлені терміни після переривання або збою критично важливих бізнес-процесів. У кожному плані підтримки безперервності бізнесу мають бути чітко вказані умови початку його виконання і співробітники, відповідальні за виконання кожного фрагмента плану. У разі появи нових вимог необхідно внести поправки до прийнятих планів дії в позаштатних ситуаціях.

Для кожного плану має бути призначений певний власник. Правила дії в позаштатних ситуаціях, плани ручного аварійного відновлення та плани відновлення діяльності мають перебувати у віданні власників відповідних ресурсів або процесів, до яких вони мають відношення.

7.11 Дотримання вимог законодавства

Усі значущі вимоги, встановлені чинним законодавством, підзаконними актами та договірними відносинами, а також підхід Підприємства до забезпечення відповідності цим вимогам мають бути явно визначеними, задокументованими та підтримуватися в актуальному стані. Необхідне дотримання регламентованого процесу, що запобігає порушенню цілісності, достовірності та конфіденційності ІР,

які містять персональні дані, починаючи зі стадії збору та введення даних до їх зберігання.

Персональні дані конкретного співробітника і процес їхнього опрацювання має бути відкритим для цього співробітника. В Підприємстві мають бути впроваджені відповідні процедури для забезпечення дотримання законодавчих обмежень, підзаконних актів і контрактних зобов'язань щодо використання матеріалів, що охороняються авторським правом, а також щодо використання ліцензійного ПЗ.

Важлива документація Підприємства має бути захищена від втрати, знищення та фальсифікації відповідно до вимог законодавства, підзаконних актів, контрактних зобов'язань та бізнес-вимог. Система зберігання та обробки повинна забезпечувати чітку ідентифікацію записів та їхнього періоду зберігання відповідно до вимог законів і нормативних актів. Ця система повинна мати можливість знищення записів після закінчення періоду зберігання, якщо ці записи більше не потрібні Підприємству. Криптографічні засоби мають використовуватися відповідно до всіх наявних угод, законодавчих і нормативних актів.

7.12 Аудит інформаційної безпеки

Установа повинна проводити внутрішні перевірки СУІБ через заплановані інтервали часу.

Основні цілі проведення таких перевірок:

- оцінка поточного рівня захищеності ІС;
- виявлення та локалізація вразливостей у системі захисту ІС;
- аналіз ризиків, пов'язаних із можливістю здійснення загроз безпеці щодо ІР;
- оцінка відповідності ІС вимогам цієї Політики;
- вироблення рекомендацій щодо вдосконалення СУІБ за рахунок впровадження нових і підвищення ефективності наявних заходів захисту інформації.

До переліку завдань, що вирішуються під час проведення перевірок та аудитів СУІБ, входять:

- збір та аналіз вихідних даних про організаційну та функціональну структуру ІС, необхідних для оцінки стану ІБ;

- аналіз наявної політики безпеки та інших організаційно-розпорядчих документів із захисту інформації щодо їхньої повноти та ефективності, а також формування рекомендацій щодо їх розроблення (або доопрацювання);

- техніко-економічне обґрунтування механізмів безпеки;

- перевірка правильності підбору та налаштування засобів захисту інформації, формування пропозицій щодо використання наявних і встановлення додаткових засобів захисту для підвищення рівня надійності та безпеки ІС;

- розбір інцидентів ІБ і мінімізація можливих збитків від їхнього прояву. Керівництво та співробітники Підприємства під час проведення в них аудиту СУІБ зобов'язані сприяти аудиторам і надавати всю необхідну для проведення аудиту інформацію.

7.13 Надання послуг стороннім організаціям

7.13.1 Угоди про надання послуг

До угод про надання послуг стороннім організаціям мають бути включені вимоги безпеки, опис, обсяги та характеристики якості послуг, що надаються.

7.13.2 Аналіз надання послуг

Послуги, звіти та записи, що надаються стороннім організаціям, мають постійно перевірятися й аналізуватися. У відносинах зі сторонньою організацією мають бути присутні такі процеси:

- контроль обсягу та якості послуг, обумовлених в угодах;

- надання сторонній організації інформації про інциденти ІБ, пов'язані з наданими послугами, і спільне вивчення цієї інформації;

- аналіз наданих сторонніми організаціями звітів про надані послуги;

- управління будь-якими виявленими проблемами.

7.13.3 Приймання систем

В підприємстві має бути розроблений і затверджений порядок приймання нових ІС, оновлення та нових версій ПЗ

8. Відповідальність

Директор Підприємства визначає пріоритетні напрями діяльності у сфері забезпечення ІБ, заходи щодо реалізації цієї Політики, затверджує списки об'єктів та відомостей, що підлягають захисту, а також здійснює загальне керівництво забезпеченням ІБ Підприємства.

Відповідальність за підтримання положень цієї Політики в актуальному стані, створення, впровадження, координацію та внесення змін до процесів СУІБ Підприємства лежить на керівництві відділу ІБ.

Усі керівники несуть пряму відповідальність за реалізацію Політики та її дотримання персоналом у відповідних підрозділах.

Працівники Підприємства несуть персональну відповідальність за дотримання вимог документів СУІБ і зобов'язані повідомляти про всі виявлені порушення у сфері інформаційної безпеки до відділу ІБ.

У трудових договорах і посадових інструкціях працівників установлюють відповідальність за збереження службової інформації, що стала відомою через виконання своїх обов'язків.

Керівництво Підприємства регулярно проводить наради, присвячені проблемам забезпечення інформаційної безпеки, з метою формування чітких вказівок з цього питання, здійснення контролю за їх виконанням, а також надання адміністративної підтримки ініціативам щодо забезпечення ІБ.

Порушення вимог нормативних актів Підприємства щодо забезпечення ІБ є надзвичайною подією та слугуватиме приводом і підставою для проведення службового розслідування.

9. Контроль і перегляд

Загальний контроль стану ІБ Підприємства здійснюється Директором. Поточний контроль дотримання цієї Політики здійснює відділ ІБ.

Контроль здійснюється шляхом проведення моніторингу та менеджменту інцидентів ІБ Підприємства, за результатами оцінки ІБ, а також у межах інших контрольних заходів.

Відділ ІБ щорічно переглядає положення цієї політики. Зміни та доповнення вносяться за ініціативою відділу ІБ або Директора і затверджуються Директором.

Порядок перегляду документів другого і третього рівнів визначається в цих документах.

Усі зміни, внесені до цієї Політики ІБ, мають враховуватися в аркуші "Історія змін"

10. Історія змін

При внесення змін у Політику ІБ заповнюється однойменний документ, який являє собою таблицю. Таблиця повинна мати відомості о версії Політики ІБ, даті її затвердження, зміни які відбулися у документі та працівник Підприємства який ці зміни вносив.

ДОДАТОК Ґ. Положення щодо застосовності

Таблиця додатку – Положення щодо застосовності

№ контролю	Назва контролю	Опис контролю	Застосовність контролю	Причина винятку з контролю	Метод реалізації
А.5 Політики безпеки					
А.5.1 Принципи управління інформаційною безпекою					
Ціль: Забезпечити принципи управління та підтримку інформаційної безпеки згідно з вимогами введення бізнесу та відповідними законами й нормативами					
А.5.1.1	Політики інформаційної безпеки	Набір політик щодо інформаційної безпеки повинен бути визначений, затверджений керівництвом, виданий і доведений до відома всього найманого персоналу та потрібних зовнішніх сторін	Так		Політика інформаційної безпеки сформована після всіх узгоджень, обґрунтувань, аналізів та впровадженнь у Підприємстві
А.5.1.2	Перегляд політики інформаційної безпеки	Політики інформаційної безпеки потрібно переглядати в заплановані інтервали часу або за появи істотних змін для забезпечення їх постійної придатності, адекватності й ефективності	Так		Відділ ІБ щорічно переглядає положення цієї політики. Зміни та доповнення вносяться за ініціативою відділу ІБ або Директора і затверджуються Директором.

Продовження таблиці додатку

№ контролю	Назва контролю	Опис контролю	Застосовність контролю	Причина винятку з контролю	Метод реалізації
А.6 Організація інформаційної безпеки					
А.6.1 Внутрішня організація					
Ціль: Визначити структуру управління для започаткування та контролю впровадження та функціонування інформаційної безпеки в організації					
А.6.1.1	Ролі та обов'язки щодо інформаційної безпеки	Усі обов'язки щодо інформаційної безпеки необхідно чітко визначити та розподілити	Так		Ролі та обов'язки щодо інформаційної безпеки описані в ПБ підприємства, головні частини обов'язків виділені відділу інформаційної безпеки підприємства
А.6.1.2	Розподіл обов'язків	Конфліктуючі обов'язки та сфери відповідальності мають бути розподілені для зменшення можливостей неавторизованої чи ненавмисної модифікації або неправильного використання ресурсів СУІБ організації	Так		Розподіл обов'язків описані в ПБ підприємства, задля мінімізації конфліктуючих обов'язків структура УІБ розподілена на кілька підрозділів підприємства.
А.6.1.3	Контакти з повноважними органами	Необхідно підтримувати належні контакти з відповідними повноважними органами	Так		Підприємство має документ забезпечення безперервності бізнесу

Продовження таблиці додатку

№ контролю	Назва контролю	Опис контролю	Застосовність контролю	Причина винятку з контролю	Метод реалізації
А.6.1.4	Контакти з групами фахівців з певної проблематики	Необхідно підтримувати належні контакти з групами фахівців з певної проблематики або іншими форумами фахівців з безпеки чи професійними об'єднаннями	Так		Підприємство здійснює навчання фахівців у галузі ІБ, участь у вебінарах, конференція, форумах з ІБ
А.6.1.5	Інформаційна безпека в управлінні проектами	Інформаційну безпеку потрібно брати до уваги під час управління проектами незалежно від типу проекту	Так		Політика аудиту інформаційної безпеки
А.7.1 Безпека людських ресурсів					
А.7.1 Перед наймом					
Ціль: Гарантувати, що найманий персонал та підрядники розуміють свої обов'язки, придатні до ролей, на які претендують					
А.7.1.2	Терміни та умови найму	Заходи безпеки, при яких, контрактні угоди з найманим персоналом та підрядниками має встановити взаємні відповідності щодо інформаційної безпеки	Так		Усі співробітники, яких приймають на роботу, повинні схвалити і підписати свої трудові договори, в яких встановлюється їхня відповідаль-ність за ІБ

Продовження таблиці додатку

№ контролю	Назва контролю	Опис контролю	Застосовність контролю	Причина винятку з контролю	Метод реалізації
А.8 Управління ресурсами СУІБ					
А.8.1 Відповідальність за ресурси СУІБ					
Ціль: Ідентифікувати ресурси СУІБ організації і визначити відповідні обов'язки щодо їх захисту					
А.8.1.1	Інвентаризація ресурсів СУІБ	Інформація, ресурсі СУІБ, пов'язані з інформацією та обладнанням для обробки інформації, мають бути ідентифіковані та має підтримуватися їх актуальний інвентарний опис	Так		Підприємство має складений перелік усіх інформаційних активів, з їх характеристиками та ідентифікаторами, які охоплює СУІБ
А.8.1.3	Припустиме використання ресурсів СУІБ	Правила щодо припустимого використання інформації та ресурсів СУІБ, пов'язаних із засобами оброблення інформації, мають бути ідентифіковані, задокументовані та впроваджені	Так		В ПБ сформовані основні правила та загальні обов'язки користувача інформаційних ресурсів.
А.9.1.1	Політика контролю доступу	Політика контролю доступу має бути розроблена, задокументована та переглядатися на основі вимог бізнесу та ІБ	Так		Кожен співробітник користується тільки визначеними йому правами стосовно інформації згідно політики ІБ

ДОДАТОК Д. Перелік документів на оптичному носії

Петренко_С.Ю._125м-21-1.docx

Петренко_С.Ю._125м-21-1.pdf

Петренко_С.Ю._125м-21-1.pptx

ДОДАТОК Е. Відгук керівника економічного розділу

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 85 б. («Добре»).

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Є. Відгук керівника кваліфікаційної роботи

Відгук

на кваліфікаційну роботу магістра на тему:
«Методика впровадження СУІБ для охоронних підприємств»
студента групи 125м-21-1
Петренка Сергія Юрійовича

Мета роботи – розробка рекомендацій із впровадження СУІБ за стандартами ISO/IEC 27k для охоронних підприємств.

Тема роботи безпосередньо пов'язана з об'єктом діяльності фахівця за спеціальністю 125 Кібербезпека – обґрунтовування використання, впровадження та аналізу кращих світових стандартів, практик з метою розв'язання складних задач в галузі інформаційної безпеки та/або кібербезпеки.

Задачі роботи (обґрунтування актуальності роботи, аналіз основних законодавчих та нормативних актів, що регламентують впровадження СУІБ, аналіз типових середовищ функціонування охоронних підприємств, формування та формалізація вимог до розробки, оцінка ризиків, розробка елементів політики безпеки) віднесені в освітньо-кваліфікаційній характеристиці магістра до класу евристичних, вирішення яких основане на знаково-розумових уміннях фахівця.

Оригінальність запропонованих рішень полягає у їх адаптованості до умов функціонування охоронних підприємств.

Практичне значення результатів проектування полягає в можливості впровадження СУІБ за стандартами ISO/IEC 27k для охоронних підприємств з врахування особливостей діяльності охоронних підприємств.

До недоліків дипломної роботи відносяться:

- недостатньо структуровано наведений аналіз актуальних загроз для типового охоронного підприємства;
- не в повному обсязі виконана формалізація вимог до розробки;
- деякі пункти політики безпеки мають загальний характер.

Оформлення пояснювальної записки до дипломного проекту виконано з деякими відхиленнями від стандартів.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог положення про систему виявлення та запобіганню плагіату.

Ступінь самостійності виконання дипломної роботи висока.

За час дипломування Петренко С.Ю. виявив себе фахівцем, здатним самостійно, на достатньо високому рівні вирішувати поставлені задачі.

В цілому кваліфікаційна робота виконана у відповідності до вимог, що ставляться до кваліфікаційної роботи магістра, заслуговує оцінки “добре”, а Петренко С.Ю. присвоєння йому кваліфікації магістр з кібербезпеки, освітньо-професійна програма «Кібербезпека».

Керівник спеціальної частини
дипломної роботи магістра,
старший викладач _____ О.В. Кручінін

Керівник дипломної
роботи магістра,
д.ф.-м.н., професор. _____ Т.С. Кагадій