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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента ***Бойчука Миколи Олексійовича***

академічної групи ***125-20-2***

спеціальності ***125 Кібербезпека***

спеціалізації[1]

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка політики безпеки підприємства фармацевтичної галузі ТОВ «Еліксир»***

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Магро В. І.	90	відмінно	
розділів:				
спеціальний	асист. Мілінчук Ю. А.	90	відмінно	
економічний	к.е.н., доц. Пілова Д.П.	85	добре	
Рецензент	к. т. н., доц. Шедловський І. А.	90	відмінно	
Нормоконтролер	ст. викл. Мєшков В.І.	90	відмінно	

Дніпро
2024

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Бойчуку Миколі Олексійовичу*** **академічної групи** ***125-20-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка політики безпеки підприємства фармацевтичної галузі ТОВ «Еліксир»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз актуальності впровадження політики інформаційної безпеки у робочий процес підприємств і процесу розробки корпоративної політики інформаційної безпеки, постановка задачі.	15.03.2024
Розділ 2	Аналіз інформації про діяльність, середовище користувачів та інформаційне середовище ТОВ «Еліксир», розробка моделей загроз ІКС і порушника ІБ ТОВ «Еліксир», розробка змісту документів ПІБ ТОВ «Еліксир».	10.05.2024
Розділ 3	Розрахунок капітальних та експлуатаційних витрат на впровадження та підтримку ПІБ ТОВ «Еліксир», визначення річного ефекту та аналіз показників економічної ефективності впровадження ПІБ ТОВ «Еліксир».	11.06.2024

Завдання видано _____ Валерій МАГРО
(підпис керівника) (ім'я, прізвище)

Дата видачі: 01.04.2024р.

Дата подання до екзаменаційної комісії: 28.06.2023р.

Прийнято до виконання _____ Микола БОЙЧУК
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 81 с., 3 рис., 13 табл., 17 джерел, 4 додатки.

Предмет розробки: політика безпеки інформації інформаційно-комунікаційної системи товариства з обмеженою відповідальністю «Еліксир».

Об'єкт розробки: інформаційно-комунікаційна система товариства з обмеженою відповідальністю «Еліксир».

Мета кваліфікаційної роботи: підвищити рівень інформаційної безпеки в інформаційно-комунікаційній системі підприємства фармацевтичної галузі за рахунок розробки політики безпеки задля її впровадження.

У першому розділі розглянуто стан питання розробки політики інформаційної безпеки, необхідні умови для проєктування її як частини СУІБ, проаналізовано теоретичні основи процесу розробки ПІБ корпоративної ІКС.

У другому розділі проаналізовано організаційну структуру, середовище користувачів та інформаційне середовище, класифіковано інформацію у корпоративній ІКС, розроблено модель порушника ІБ ТОВ «Еліксир», моделі загроз ІКС ТОВ «Еліксир» до та після впровадження ПІБ у робочий процес підприємства, а також документи політики інформаційної безпеки ТОВ «Еліксир».

У третьому розділі визначено капітальні та експлуатаційні витрати на розробку та підтримку виконання корпоративної ПІБ, показники економічної ефективності впровадження ПІБ, доведено економічну доцільність розробки ПІБ ТОВ «Еліксир».

Практичне значення роботи полягає у розробці політики інформаційної безпеки фармацевтичної компанії задля підвищення рівня захищеності інформації, що циркулює в інформаційно-комунікаційній системі реального підприємства.

ПОЛІТИКА БЕЗПЕКИ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ.

ABSTRACT

Explanatory note: 81 pp., 3 pictures, 13 tables, 17 applications, 4 sources.

Subject of development: information security policy of information and communication system of «Elixir» LLC.

Object of development: information and communication system of the LLC «Elixir».

The purpose of the qualification work: ensuring the appropriate level of information security in accordance with ISO standards in the information and communication system of the enterprise of the pharmaceutical industry by developing a security policy for its implementation.

In the first section, the state of the development of the information security policy, the necessary conditions for designing it as part of the information security management system and the analysis of the theoretical foundations of the process of developing the corporate information security policy are discussed.

In the second section, the organizational structure, user and information environment, information in the corporate information and communication system is classified, developed a model of IS violator of Elixir LLC before and after the introduction of an information security policy into the company's workflow, as well as information security policy documents of LLC «Elixir».

In the third section, the capital and operating costs for the development to support the implementation of the corporate name are defined, indicators of the economic efficiency of the name of the name, the economic feasibility of the name of Elixir LLC is proven.

The practical significance of the work consists in the development of the information security policy of the pharmaceutical company in order to increase the level of information, circulating in the information and communication system of a real enterprise.

SECURITY POLICY, INFORMATION AND COMMUNICATION SYSTEM, INFORMATION SECURITY MANAGEMENT SYSTEM, COMPLEX OF PROTECTION TOOLS, SOFTWARE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АЗ – апаратне забезпечення;

АС – автоматизована система;

БД – база даних;

ДСТУ – державний стандарт України;

ЕЦП – електронний цифровий підпис;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІКС – інформаційно-комунікаційна система;

ІТ – інформаційні технології;

ІТП – інженерно-технічний персонал;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

МТГ – міська територіальна громада;

НД – нормативний документ;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

ПІБ – політика інформаційної безпеки;

РС – робоча станція;

СУБД – система управління базами даних;

СУІБ – система управління інформаційною безпекою;

ТЗІ – технічний захист інформації;

ТОВ – товариство з обмеженою відповідальністю;

ТУ – технічні умови;

DB – Database;

IEC – International Electrotechnical Commission;

ISO – International Organization for Standardization;

LLC – Limited Liability Company;

OLP – Open License Program.

ЗМІСТ

с.

ВСТУП

В розвиненому світі інформаційні технології вже охоплюють всі аспекти життя людей. На побутовому рівні в розвинених країнах вже неможливо жити без постійного використання комп'ютерів, гаджетів, інформаційних мереж та інших систем обробки інформації.

За останні роки впровадження технологій автоматизованої обробки інформації вже охопило всі процеси у веденні економічної діяльності суб'єктів господарювання незалежно від галузі їх роботи. Наразі зберігання та обробка інформації у таких найважливіших галузях української економіки, як металургія, машинобудування, енергетика, хімічна промисловість, майже повністю здійснюються із широким залученням до них сучасних засобів автоматизованої обробки інформації. Тож задля утримання здатності до конкуренції на ринку підприємства постійно працюють над покращенням роботи своїх автоматизованих інформаційно-комунікаційних систем.

Головною умовою обробки інформації в ІКС підприємства є забезпечення безпеки інформації у цій системі. Безпека інформації – це стан захищеності інформації від загроз при якому забезпечується конфіденційність, цілісність та доступність інформації (тріада інформаційної безпеки). Метою інформаційної безпеки є зменшення та усунення загроз інформації, необхідної для роботи підприємства.

Для забезпечення інформаційної безпеки підприємства створюються системи управління інформаційною безпекою для конкретних установ. Системи управління інформаційною безпекою для того, щоб забезпечити конфіденційність, цілісність та доступність інформації в інформаційно-комунікаційній системі підприємства, використовують ризик-орієнтований підхід. Ключовою складовою СУІБ є політика інформаційної безпеки – сукупність загальних принципів та правил, якими керується об'єкт інформаційної діяльності.

Політика інформаційної безпеки - це сукупність документованих рішень, що приймаються керівництвом об'єкта кіберзахисту і спрямовані на захист

електронних комунікаційних та (або) технологічних мереж і систем, інформації та асоційованих з нею ресурсів (активів).

Актуальність теми кваліфікаційної роботи полягає у постійній необхідності підвищення безпеки інформації на підприємствах, зокрема підприємствах фармацевтичної галузі. Частиною роботи із забезпечення безпеки інформації на підприємстві є розробка політики інформаційної безпеки. Важливо приводити системи управління інформаційною безпекою підприємств до вимог стандарту ISO/IEC 27001:2022 задля гарантування захищеності інформації, що циркулює в ІКС підприємства.

Об'єкт дослідження: інформаційно-комунікаційна система товариства з обмеженою відповідальністю «Еліксир».

Предмет дослідження: політика безпеки інформації інформаційно-комунікаційної системи товариства з обмеженою відповідальністю «Еліксир».

Мета роботи: забезпечити належний за стандартами ISO рівень інформаційної безпеки в інформаційно-комунікаційній системі підприємства фармацевтичної галузі за рахунок розробки політики безпеки задля її впровадження.

Для досягнення мети кваліфікаційної роботи необхідно виконати такі завдання:

1. Проаналізувати специфіку роботи та організаційну структуру підприємства;

2. Визначити види інформації, які циркулюють на підприємстві;

3. Визначити модель взаємодії користувачів з ІКС;

4. Розробити модель загроз ІКС підприємства;

5. Розробити модель порушника ІБ підприємства;

6. Систематизувати процес забезпечення ІБ ТОВ «Еліксир»;

7. Розробити політику інформаційної безпеки підприємства;

8. Розрахувати капітальні та експлуатаційні витрати на розробку ПІБ ТОВ «Еліксир».

Практичне значення роботи полягає у розробці політики інформаційної безпеки фармацевтичної компанії задля підвищення рівня захищеності інформації, що циркулює в інформаційно-комунікаційній системі реального підприємства.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Особливості організації роботи із захисту інформації на підприємствах фармацевтичної галузі

Предметом діяльності описаного у кваліфікаційній роботи підприємства фармацевтичної галузі ТОВ «Еліксир» є виробництво лікарських засобів, біологічно активних речовин з використанням природних ресурсів та їх постачання до аптечних і торгівельних мереж України з метою одержання прибутку.

Промислове шпигунство завжди залишається актуальною загрозою для підприємств. Найбільшу загрозу промислове шпигунство становить для фабрик, які виробляють унікальну продукцію за власноруч розробленими технологіями чи рецептурою. Фармацевтична галузь – один з напрямків прибуткової діяльності з найбільш розповсюдженою негативною практикою промислового шпигунства, спрямованою на викрадення рецептур та хімічного складу виробленої продукції.

Іншим напрямком діяльності із забезпечення інформаційної безпеки компанії є протидія імовірним кібератакам, які можуть здійснюватися відносно підприємства як з метою отримання несанкціонованого доступу до його фінансових ресурсів, так і задля проведення атаки на послуги забезпечення доступності з метою підривання безперервності роботи підприємства і зниження його виробничих можливостей.

Для того, щоб організувати роботу відділу системного адміністрування підприємства, необхідно, щоб такий підрозділ мав єдине зведення правил, якими він має керуватися у своїй діяльності. Тож виникає потреба у розробці політики інформаційної безпеки ТОВ «Еліксир», яку можуть розробити як спеціалісти цього підрозділу для самих себе, так і аутсорсингові спеціалісти.

Розробка політики інформаційної безпеки (ПІБ) є важливою частиною роботи відділу системного адміністрування компанії. Політика безпеки – обов'язкова умова безперебійної, коректної та якісної роботи підприємств хімічної промисловості. Галузь хімічних технологій, виробництва біологічно активних речовин та лікарських засобів передбачає найвищі вимоги до забезпечення безпеки

співробітників на виробництві та умов виробництва кінцевої продукції. Підвищена увага до підприємств фармацевтичної галузі з боку органів державного контролю, зокрема Державної служби України з лікарських засобів та контролю за наркотиками, органів із захисту прав споживачів пояснюється тим, що від якості вироблених позицій продуктової лінійки напряму залежить стан здоров'я та якість життя населення. З метою вдосконалення системи контролю якості лікарських засобів, профільні органи постійно вдосконалюють їх рецептурний склад, стандарти виробництва та вимоги до фармацевтичних компаній. Одним з етапів покращення безпеки виробництва стратегічно важливої продукції є впровадження у робочий процес підприємства культури дотримання принципів розроблюваної політики інформаційної безпеки.

1.2 Огляд нормативно-правового забезпечення процесу вдосконалення ІБ в Україні

Конституція України є основоположним документом прямої дії правової системи України.

Згідно Статті 3 Конституції України, людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю.

Закони України, що врегульовують галузь забезпечення ІБ, спираючись на Конституцію України, регламентують засади державної політики щодо захисту інформації перш за все в органах державної влади, на стратегічно важливих державних підприємствах. Втім, Закони України поширюються і на приватні компанії. Держава при розробці нормативно-правових актів у сфері кібербезпеки спирається на думки провідних фахівців із захисту інформаційних технологій. До їх рекомендацій та настанов варто звертатися і приватному сектору економіки.

Нормативно-правове забезпечення ІБ в Україні складають такі акти:

1. Закон України «Про інформацію» від 02.10.1992 р.

Закон України «Про інформацію» регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

3. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 р.

Закон України «Про захист інформації в інформаційно-комунікаційних системах» регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

4. Закон України «Про захист персональних даних» від 01.06.2010 р.

Закон України «Про захист персональних даних» регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних. Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

5. Закон України «Про державну таємницю» від 21.01.1994 р.

Закон України «Про державну таємницю» регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням,

розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

6. Постанова Кабінету Міністрів України «Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19.06.2019 р.

Загальні вимоги визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури.

7. Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» від 29.03.2006 р.

Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах визначають загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

При розробці ПІБ необхідно спиратися на положення відповідних нормативних документів технічного захисту інформації (НД ТЗІ). НД ТЗІ є частиною нормативно-правового забезпечення ІБ в Україні. Наступні НД ТЗІ використовуються для розробки ПІБ як частини КСЗІ на підприємствах:

8. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу

Цей документ установлює терміни і визначення понять у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Терміни, що установлюються цим документом, обов'язкові для застосування в усіх видах документації і літератури, що входять до системи технічного захисту інформації.

9. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі

Цей нормативний документ системи технічного захисту інформації (НД ТЗІ) встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації в автоматизованій системі - “Положення про службу захисту інформації в автоматизованій системі”.

НД ТЗІ призначений для суб’єктів відносин (власників або розпорядників АС, користувачів), діяльність яких пов’язана з обробкою в автоматизованих системах інформації, що підлягає захисту згідно з нормативно-правовими актами, а також для розробників комплексних систем захисту інформації в автоматизованих системах.

Використання цього НД ТЗІ створює умови для запровадження єдиного підходу щодо визначення і формування завдань, функцій, структури, повноважень служби захисту інформації, а також організації її робіт з захисту інформації впродовж всього життєвого циклу автоматизованих систем в державних органах, на підприємствах, в установах та організаціях усіх форм власності

10. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

Цей документ установлює принципи класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу.

Цей документ призначений для постачальників (розробників), споживачів (замовників, користувачів) автоматизованих систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації (інформації, яка потребує захисту), а також для державних органів, які здійснюють функції контролю за обробкою такої інформації.

Мета цього документа — надання нормативно-методологічної бази для вибору і реалізації вимог з захисту інформації в автоматизованій системі.

1.3 Значення обробки інформації. Класифікація інформації

Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Такі визначення інформації та захисту інформації наводить Закон України «Про інформацію». Також існує багато інших визначень інформації. Наприклад:

Інформація (від лат. informatio – роз'яснення) – відомості, які передають усним, писемним та іншими шляхами за допомогою умовних сигналів і технічних засобів.

Обробка інформації є основою робочого процесу підприємств будь-якого професійного профілю. Всі співробітники підприємства, що використовують ІКС, обробляють інформацію. Ця інформація може мати різне спрямування, значення, клас, але процеси діяльності співробітників щодо обробки інформації є схожими. Всі структурні підрозділи підприємства використовують ІКС підприємства. Ця система не може функціонувати без кваліфікованої підтримки відділу системного адміністрування. Значення роботи працівників фармацевтичної компанії, що розглядається, з інформацією є критичним.

Згідно Статті 20 Закону України «Про інформацію», за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Згідно Статті 21 Закону України «Про інформацію», інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація

може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом.

В ІКС ТОВ «Еліксир» окрім відкритої інформації циркулює конфіденційна інформація. Конфіденційною інформацією в ІКС компанії є комерційна таємниця.

1.4 Процес розробки політики інформаційної безпеки

Процес розробки політики інформаційної безпеки (ПІБ) в Україні визначається вимогами пункту 5 «Політика безпеки інформації в АС» Додатка «Методичні вказівки щодо структури та змісту плану захисту інформації в автоматизованій системі» до НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» як частина процесу створення корпоративної КСЗІ.

Згідно положень вищезгаданого документа, ПІБ в АС є одним з розділів плану захисту інформації в АС, який визначає властивості ІБ (конфіденційність, цілісність, доступність), котрі необхідно забезпечувати у процесі захисту інформації.

Захист інформації на підприємстві є мультизадачною роботою. Для захисту ІКС необхідно працювати над виявленням загроз різного походження (з боку порушників ІБ, недостатньо компетентних у галузі забезпечення ІБ працівників підприємства, несправних технічних засобів та можливих несприятливих умов зовнішнього середовища) для ІКС та їх знешкодженням за допомогою апаратних, програмних та організаційних рішень, виявленням та реєстрацією пов'язаних зі спробами порушення ІБ або отримання несанкціонованого доступу подій в системі розподілом ролей та доступів користувачів ІКС.

Корпоративна ПІБ поширюється на відомості у будь-яких формах їх представлення, віднесені до ІзОД, на АЗ та ПЗ в ІКС, на БД і корпоративні сервери (на підприємстві, що розглядається – 4 хости: поштовий сервер, вебсервер, файловий сервер і сховище БД), на систему охорони об'єкта (систему відеокамер),

а також поширюється на весь персонал підприємства з ролями користувачів або адміністраторів, що використовує ІКС.

Відомості, що становлять комерційну таємницю, на підприємстві можуть зберігатися на матеріальних носіях різних форм: паперових, оптичних, цифрових та інших, тож ПІБ має поширюватися не тільки на процес комп'ютеризованої обробки інформації, а й на інші її носії.

ПІБ визначає мету і задачі із забезпечення ІБ підприємства, напрямки роботи підрозділу забезпечення ІБ підприємства (у випадку підприємства, що розглядається – відділу системного адміністрування), порядок роботи співробітників підприємства із конфіденційною інформацією, викладені у зрозумілій для користувачів ІКС формі. ПІБ зазвичай складається з декількох документів. Розроблюваними документальними елементами корпоративної ПІБ є:

- політика автентифікації користувачів корпоративної ІКС ТОВ «Еліксир» з використанням особистих ключів і паролів;
- політика безпеки корпоративних серверів ТОВ «Еліксир»;
- політика використання систем виявлення вторгнень та організації антивірусного захисту ІКС ТОВ «Еліксир»;
- політика організації доступу до конфіденційної інформації в інформаційному середовищі ТОВ «Еліксир»;
- політика організації роботи відділу системного адміністрування ТОВ «Еліксир».

Окремими частинами корпоративної ПІБ є модель загроз та модель порушника. Ці моделі можуть як оформлюватися у вигляді окремих документів ПІБ, так і надаватися керівництву підприємства відділом системного адміністрування як рекомендації, спрямовані на покращення роботи із забезпечення ІБ компанії. Впровадження цих моделей в рамках ПІБ необхідне для вдосконалення СУІБ підприємства, виокремлення найбільш значущих загроз, джерел їх походження та протидії цим загрозам.

1.5 Висновок

У першому розділі розглянуто стан питання розробки політики інформаційної безпеки, необхідні умови для проєктування її як частини СУІБ, наведено короткий огляд нормативно-правового забезпечення процесу вдосконалення ІБ в Україні, розкрито значення обробки інформації для робочого процесу підприємства фармацевтичної галузі, проаналізовано теоретичні основи процесу створення ПІБ в ІКС, її структури на значення для роботи підприємства з підвищеними вимогами до забезпечення ІБ.

У процесі розробки політики інформаційної безпеки підприємства послуговуватимемося вимогами та рекомендаціями міжнародних стандартів групи ISO/IEC 27000.

1.6 Постановка задачі

Спираючись на вищенаведену інформацію, на підприємствах фармацевтичної галузі існує необхідність вдосконалення системи забезпечення ІБ. Засобом підвищення стану захищеності інформації, що обробляється на підприємствах фармацевтичної галузі є впровадження у робочий процес політики інформаційної безпеки. Тому метою кваліфікаційної роботи є розробка корпоративної ПІБ, що необхідно для систематизації організованої роботи із захисту інформації. Для того, щоб реалізувати мету кваліфікаційної роботи, необхідно виконати такі завдання:

- розробити моделі загроз ІКС ТОВ «Еліксир» до та після впровадження розробленої ПІБ у робочий процес підприємства;
- розробити модель порушника ІБ ТОВ «Еліксир»;
- розробити політику інформаційної безпеки підприємства;
- розрахувати капітальні та експлуатаційні витрати на розробку ПІБ ТОВ «Еліксир».

Процес виконання цих завдань представлений у спеціальному розділі кваліфікаційної роботи.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Стан питання

При розробці політики інформаційної безпеки необхідно враховувати, що на підприємстві уся інформація, що має захищатися, має розподілятися за ступенем критичності для роботи підприємства. Для спрощення подальшого обслуговування СУІБ, політика безпеки повинна мати розгалужену та гнучку структуру, правила якої можуть змінюватися щодо різних типів інформації, що циркулюють на підприємстві.

Політика ІБ має регулювати діяльність із підтримки безпеки інформації перед лицем загроз різного походження. Напрямками виникнення загроз для ІБ є отримання несанкціонованого доступу (НСД) до інформації, кібератаки на інформацію, представлену в ІКС підприємства з боку зловмисників, вторгнення до корпоративної ІКС та інші загрозливі дії.

Розроблювана якісна політика інформаційної безпеки обов'язково має відповідати вимогам групи міжнародних стандартів у галузі управління інформаційною безпекою ISO/IEC 27000, перш за все – стандарту ISO/IEC 27001:2022 «Information technology – Security techniques – Information security management systems – Requirements», який визначає вимоги до проєктування, впровадження, обслуговування та модернізації СУІБ на підприємствах, а також стандарту ISO/IEC 27002:2022 «Information technology – Security techniques – Code of practice for information security management», який надає практичні поради з управління інформаційною безпекою на підприємствах та стандарту ISO/IEC 27003:2017 «Information technology – Security techniques – Information security management systems – Guidance», який містить керівні вказівки стосовно вимог до СУІБ, визначених стандартом ISO/IEC 27001:2022.

Проаналізувавши ІКС підприємства, основні напрямки загроз для конфіденційності, цілісності та доступності інформації, розробивши модель загроз та модель порушника, описавши доступний для використання КЗЗ ІКС підприємства, розробник отримує всі необхідні дані для створення політики ІБ.

Дотримання ПІБ при адмініструванні корпоративної ІКС та у процесі діяльності її користувачів – співробітників підприємства важливо настільки ж критично, наскільки дотримання технічних умов виробництва продукції. Виконання вимог ПІБ є обов'язковим для всіх співробітників. Важливим напрямом діяльності відділу системного адміністрування є підвищення рівня обізнаності щодо безпечної експлуатації ІКС підприємства серед співробітників.

Наразі зростає кількість підприємств, які користуються послугами ІТ-спеціалістів напрямку кібербезпеки з метою розробки систем управління інформаційною безпекою (СУІБ), комплексних систем захисту інформації (КСЗІ), політик інформаційної безпеки та надання інших послуг в галузі захисту інформації та з управління інформаційною безпекою, тому що з плином часу зростає складність загроз, які можуть становити підприємствам зовнішні загрози, наприклад зловмисні дії недоброзичливців та внутрішні загрози, такі як ненавмисні руйнівні дії співробітників компаній. Постійно покращуються навички хакерів, їх апаратне та програмне забезпечення. Послуги з розробки ПІБ стають лише більш розповсюдженими та актуальними.

Результатом виконання кваліфікаційної роботи стане варіант надання такої послуги забезпечення інформаційної безпеки, як розробка моделі загроз ІБ та моделі порушника ІБ, розробка документів політики інформаційної безпеки підприємства фармацевтичної галузі.

2.2 Загальні відомості про підприємство. Опис діяльності підприємства

Товариство з обмеженою відповідальністю «Еліксир» - приватна компанія, що виробляє, продає оптово та постачає лікарські засоби та біологічно активні речовини на український фармацевтичний ринок.

Виробництво лікарських засобів та біологічно активних речовин підприємством складається з таких основних виробничих процесів:

- Закупівля сировини рослинного, тваринного та синтетичного походження для здійснення хімічних технологічних процесів в лабораторних умовах;
- Переробка отриманих вихідних продуктів, їх перетворення у стан, прийнятний для споживання шляхом спресовування отриманих речовин у таблетки, капсули, порошки для пероральних суспензій, розбавлення порошкоподібних речовин задля їх перетворення на лікувальні мазі та косметичні креми для зовнішнього застосування;
- Фасування отриманих кінцевих продуктів у споживацьку тару: банки, туби, ящики;
- Пакування розфасованих кінцевих продуктів в упаковки, що необхідно для спрощення реалізації вироблених товарів в аптечних і торгівельних мережах України, підвищення привабливості вироблених продуктів на фармацевтичному ринку;
- Проведення державного контролю якості вироблених лікарських засобів Державною службою України з лікарських засобів та контролю за наркотиками з метою отримання сертифікату відповідності Державним стандартам України (ДСТУ) та технічним умовам (ТУ) у сфері фармакології, як обов'язкової вимоги для реалізації продукції.
- Організація процесу транспортування та реалізації сертифікованих лікарських засобів та біологічно активних речовин у торгівельних мережах з метою отримання прибутку та розширення можливостей для подальшого розвитку приватної компанії.

Компанія розміщується в одноповерховій будівлі, на одній території з якою обладнано майданчик для заїзду вантажних автомобілів, які навантажують товарами робітники-вантажники та розвантажують їх.

Територія компанії знаходиться за адресою: 49032, Україна, Дніпропетровська область, Дніпровський район, Дніпровська МТГ, селище міського типу Авіаторське, вулиця Аеродром, будинок 145.

Графік роботи підприємства: з понеділка до п’ятниці з 09:00 до 17:00.

Річний обіг грошових коштів - 22,5 млн грн.

2.3 Організаційна структура підприємства

Підприємство знаходиться у приватній власності.

Підприємство має у своїй структурі такі підрозділи:

- відділ хімічних технологій;
- лабораторія;
- відділ продажів;
- юридичний відділ;
- відділ фінансових операцій;
- пакувальний цех (лінія);
- відділ системного адміністрування;
- кабінет директора;
- приймальня директора;
- пост охорони.

Таблиця 2.1 - Список співробітників ТОВ «Еліксир»

№ з/п	ПІБ	Посада	Адреса ел. пошти	Номер телефону
1	Фролов Олексій Андрійович	Директор	Frolov@elixyr.com	0562651230
2	Ворона Ірина Максимівна	Секретар	Vorona@elixyr.com	0562651231
3	Донцов Дмитро Романович	Бухгалтер	Dontsov@elixyr.com	0562651232
4	Бойчук Микола Олексійович	Системний адміністратор	Boichuk@elixyr.com	0562651233
5	Зініна Оксана Олександрівна	Провідний юрисконсульт	Zinina@elixyr.com	0562651234
6	Кольченко Вероніка Марківна	Юрисконсульт	Kolchenko@elixyr.com	0562651235
7	Дольчук Генадій Петрович	Головний хімік-технолог	Dolchuk@elixyr.com	0562651236
8	Єненко Юрій Миколайович	Хімік-технолог	Yenenko@elixyr.com	0562651237

Продовження таблиці 2.1

№ з/п	ПІБ	Посада	Адреса ел. пошти	Номер телефону
9	Тимашевська Марія Антонівна	Хімік-технолог	Tymashevska@elixyr.com	0562651238
10	Тимашевський Віктор Дмитрович	Хімік-технолог, завідувач лабораторією	Tymashevskyy@elixyr.com	0562651239
11	Павлов Кирило Владиславович	Фасувальник	Pavlov@elixyr.com	0562651240
12	Грушка Іван Михайлович	Фасувальник	Hrushka@elixyr.com	0562651241
13	Романов Микита Олегович	Пакувальник	Romanov@elixyr.com	0562651242
14	Шепелевич Олександр Іванович	Пакувальник	Shepelevych@elixyr.com	0562651243
15	Леньов Андрій Петрович	Провідний менеджер з продажів	Leniov@elixyr.com	0562651244
16	Плетньова Валерія Леонідівна	Менеджер з продажів	Pletniova@elixyr.com	0562651245
17	Руднєв Сергій Миколайович	Менеджер з продажів	Runov@elixyr.com	0562651246
18	Усова Валерія Богданівна	Старший охоронець	Usov@elixyr.com	0562651247
19	Хмизенко Кирило Володимирович	Охоронець	Khmyzenko@elixyr.com	0562651248
20	Скороход Володимир Євгенович	Охоронець	Skorokhod@elixyr.com	0562651249
21	Сухий Станіслав Станіславович	Водій	-	0562651250
22	Хутірний Микита Тимурович	Водій	-	0562651251
23	Борисова Світлана Анатоліївна	Прибиральниця	-	0562651252
24	Руденко Віталій Романович	Вантажник	-	0562651253
25	Котов Юрій Ілліч	Вантажник	-	0562651254
26	Мальцев Назар Олексійович	Вантажник	-	0562651255

2.4 Обов’язки співробітників підприємства

Обов’язки директора підприємства: визначає напрямків діяльності підприємства, організовує роботу, виробничий процес компанії, укладає договори із продажу та постачання продукції підприємства, забезпечує ефективну взаємодію структурних підрозділів підприємства, керує притягненням працівників до

дисциплінарної відповідальності у випадках невиконання ними їх посадових обов'язків та заохоченням працівників у відповідних ситуаціях, забезпечує відповідність якості продукції, що виробляється, вимогам державних стандартів України, контролює дотримання норм охорони праці, комплектує підприємство кваліфікованими кадрами та контролює дотримання правил трудової дисципліни.

Директор підприємства надає допуск до інформації з обмеженим доступом (ІзОД), яка зберігається та обробляється в ІКС підприємства.

Директору підпорядковуються секретар, бухгалтер, системний адміністратор, провідний юрисконсульт, провідний менеджер з продажів, головний хімік-технолог, старший охоронець.

Обов'язки секретаря: подає документи на затвердження директором підприємства, готує необхідні для роботи документи, зберігає печатки юридичної особи підприємства, веде протоколи нарад і засідань, приймає вхідну кореспонденцію та телефонні дзвінки, відповідає на електронні листи споживачів, зберігає ключі від приміщень підприємства.

Обов'язки бухгалтера: веде бухгалтерський облік активів, грошових коштів на рахунках компанії, проводить інвентаризацію активів, готує фінансову звітність підприємства, проводить розрахунки з кредиторами та виплати податків до державного бюджету через банківські установи, надає звіти про виконану роботу директору підприємства.

Обов'язки системного адміністратора: налаштовує апаратне та програмне забезпечення в ІКС підприємства, забезпечує безперервність роботи ІКС підприємства, налаштовує комп'ютерну мережу компанії, управляє системами контролю трафіку, відповідає за забезпечення кібербезпеки ввіреної ІКС, надає звіти про виконану роботу директору підприємства.

Обов'язки юрисконсульта: здійснює юридичний супровід підприємства у судових інстанціях, ділових переговорах, керує процесом оформлення внутрішньої документації на підприємстві та разом з директором підприємства складає договори, необхідні для провадження торгівельних відносин з іншими суб'єктами господарювання, зберігає матеріали судових справ, надає інформаційні послуги з

питань чинного законодавства, надає звіти про виконану роботу директору підприємства.

Обов'язки хіміка-технолога: знає хімічний склад, рецептури, характеристики та властивості продуктів, що виробляє компанія, технологічний процес виробництва, зміст державних стандартів, технічних умов, контролює якість і відповідність виробленої продукції державним стандартам, технічним умовам, аналізувати причини вироблення бракованої продукції та проводити заходи із попередження випуску низькоякісної продукції, має загальне уявлення про передові наукові розробки у галузі виробництва фармацевтичної продукції, надає звіти про виконану роботу директору підприємства.

Обов'язки менеджера з продажів: спільно з директором підприємства та юрисконсультом укладає договори щодо продажу продукції підприємства та її постачання до торгівельних і аптечних мереж, консультує зацікавлених покупців продукції компанії стосовно умов придбання продукції оптом та в роздріб, приймає замовлення на купівлю партій продукції, розміщує рекламу продукції у засобах масової інформації, надає звіти про виконану роботу директору підприємства.

Обов'язки фасувальника: фасує у тару за вагою тверді, рідкі і аерозольні лікарські засоби та біологічно активні речовини, проводить ваговий контроль готової до постачання до аптечних і торгівельних мереж продукції, налагоджує високоточні апарати вимірювання ваги та інші контрольно-вимірювальні прилади.

Обов'язки пакувальника: забезпечує цілісність готової продукції в упаковці на шляху від виробничих потужностей підприємства до кінцевого споживача, упаковує готову продукцію у тару, укріплює крихкі частини тари та продукції при пакуванні для перевезення готових товарів.

Обов'язки охоронця: охороняє об'єкти та матеріальні цінності ТОВ «Еліксир», контролює доступ до приміщення підприємства співробітників компанії, клієнтів та сторонніх осіб, веде облік відвідувачів компанії, керує роботою системи відеоспостереження, за потреби проводить огляд відвідувачів приміщення підприємства та їх особистих речей.

Обов'язки водія: управляє легковими та вантажними автомобілями підприємства, доставляє вироблену на підприємстві готову продукцію до торгівельних і аптечних мереж з використанням транспортних засобів компанії, заправляє транспортні засоби необхідними для їх роботи паливно-мастильними матеріалами за кошти компанії, щодня проводить контрольну перевірку технічного стану ввіреного водієві транспортного засобу.

Обов'язки вантажника: готує вантажі виробленої на підприємстві готової продукції для перевезення до торгівельних мереж, завантажує запаковану готову продукцію у транспортні засоби компанії, розвантажує необхідну для роботи підприємства сировину з транспортних засобів її постачальників.

Обов'язки прибиральниці: прибирає сміття та відходи виробництва з приміщень підприємства, підтримує приміщення підприємства у чистоті, дезінфікує приміщення лабораторії та пакувального цеху з використанням спеціальних дезінфікуючих хімічних речовин посиленої дії.

2.5 Середовище користувачів ІКС ТОВ «Еліксир»

Загалом у штаті підприємства 26 співробітників. З них 20 використовують ІКС підприємства.

Список персоналу, який використовує ІКС підприємства:

1. Директор - 1 особа;
2. Секретар - 1 особа;
3. Бухгалтер - 1 особа;
4. Системний адміністратор - 1 особа;
5. Юрисконсульти - 2 особи;
6. Хіміки-технологи - 4 особи;
7. Пакувальники - 2 особи;
8. Фасувальники - 2 особи;
9. Менеджери з продажів - 3 особи;
10. Охоронці - 3 особи;

Таблиця 2.2 - Список персоналу, який використовує ІКС підприємства

№ з/п	ПІБ	Посада	Адреса ел. пошти	Номер телефону	Роль в ІС
1	Фролов Олексій Андрійович	Директор	Frolov@elixyr.com	0562651230	Користувач
2	Ворона Ірина Максимівна	Секретар	Vorona@elixyr.com	0562651231	Користувач
3	Донцов Дмитро Романович	Бухгалтер	Dontsov@elixyr.com	0562651232	Користувач
4	Бойчук Микола Олексійович	Системний адміністратор	Boichuk@elixyr.com	0562651233	Адміністратор
5	Зініна Оксана Олександрівна	Провідний юрисконсульт	Zinina@elixyr.com	0562651234	Користувач
6	Кольченко Вероніка Марківна	Юрисконсульт	Kolchenko@elixyr.com	0562651235	Користувач
7	Дольчук Генадій Петрович	Головний хімік-технолог	Dolchuk@elixyr.com	0562651236	Користувач
8	Єненко Юрій Миколайович	Хімік-технолог	Yenenko@elixyr.com	0562651237	Користувач
9	Тимашевська Марія Антонівна	Хімік-технолог	Tymashevska@elixyr.com	0562651238	Користувач
10	Тимашевський Віктор Дмитрович	Хімік-технолог	Tymashevskyy@elixyr.com	0562651239	Користувач
11	Павлов Кирило Владиславович	Фасувальник	Pavlov@elixyr.com	0562651240	Користувач
12	Грушка Іван Михайлович	Фасувальник	Hrushka@elixyr.com	0562651241	Користувач
13	Романов Микита Олегович	Пакувальник	Romanov@elixyr.com	0562651242	Користувач
14	Шепелевич Олександр Іванович	Пакувальник	Shepelevych@elixyr.com	0562651243	Користувач
15	Леньов Андрій Петрович	Провідний менеджер з продажів	Leniov@elixyr.com	0562651244	Користувач
16	Плетньова Валерія Леонідівна	Менеджер з продажів	Pletniova@elixyr.com	0562651245	Користувач
17	Руднєв Сергій Миколайович	Менеджер з продажів	Runov@elixyr.com	0562651246	Користувач
18	Усов Валерій Богданович	Старший охоронець	Usov@elixyr.com	0562651247	Користувач
19	Хмизенко Кирило Володимирович	Охоронець	Khmyzenko@elixyr.com	0562651248	Користувач
20	Скороход Володимир Євгенович	Охоронець	Skorokhod@elixyr.com	0562651249	Користувач

2.6 Види інформації, які циркулюють в ІКС ТОВ «Еліксир»

Згідно Статті 10 Закону України «Про інформацію», за своїм змістом інформація класифікується на такі види:

- інформація про фізичну особу;
- інформація довідково-енциклопедичного характеру;
- інформація про стан довкілля (екологічна інформація);
- інформація про товар (роботу, послугу);
- науково-технічна інформація;
- податкова інформація;
- правова інформація;
- статистична інформація;
- соціологічна інформація;
- критична технологічна інформація;
- інші види інформації.

Діяльність підприємства супроводжується розповсюдженням таких видів інформації:

- інформація про фізичних осіб - інформація про співробітників та інформація про клієнтів;
- комерційна інформація - інформація про товари, які виробляє компанія та про послуги, які вона надає, рекламна інформація компанії, інформація про макрофінансові показники компанії (витрати, доходи, прибутки);
- науково-технічна інформація - довідники, підручники, наукова та науково-популярна медична література, дані наукових лабораторних досліджень;
- податкова інформація - інформація про виплачені податки і єдиний соціальний внесок, про виконання законодавства у сфері оподаткування юридичних осіб, про інші взаємовідносини з Державною фіскальною службою України;
- правова інформація - нормативно-правові акти, кодекси України в електронній та паперовій формах;

- статистична інформація - інформація про результати маркетингових досліджень щодо обсягу продажів продукції у різних часових проміжках, виробленої компанією, інформація про результати соціологічних досліджень на теми оцінки якості продукції з боку споживачів, оцінки обсягу продажів вироблених лікарських засобів та біологічно активних речовин у торгівельних мережах аптек та супермаркетів.
- фінансова інформація - інформація про обсяги коштів на банківських рахунках компанії, кількісні характеристика активів і майна компанії,
- юридична інформація - інформація про стан розгляду судових справ ТОВ «Еліксир», рішення судових інстанцій, судова кореспонденція.

Таблиця 2.3 - Перелік інформації, що циркулює в інформаційній системі підприємства та класифікація цієї інформації за режимом доступу:

Вид інформації	**Клас за режимом доступу**
Інформація про фізичних осіб	З обмеженим доступом
Комерційна інформація	Відкрита / З обмеженим доступом
Науково-технічна інформація	Відкрита
Податкова інформація	Відкрита
Правова інформація	Відкрита
Статистична інформація	Відкрита / З обмеженим доступом
Фінансова інформація	З обмеженим доступом
Юридична інформація	З обмеженим доступом

Таблиця 2.4 - Перелік інформації, що циркулює в інформаційній системі підприємства та класифікація цієї інформації за режимом доступу

Вид інформації	Режим доступу	Носій інформації	Вимоги К	Вимоги Ц	Вимоги Д
Особисті дані персоналу	ІзОД	Електронний та паперовий	+	+	+
База даних підприємства	ІзОД	Електронний	+	+	+

Продовження таблиці 2.4

Вид інформації	Режим доступу	Носій інформації	Вимоги К	Вимоги Ц	Вимоги Д
Договори, укладені з клієнтами	ІзОД	Електронний та паперовий	+	+	+
Бухгалтерська звітність	ІзОД	Електронний	+	+	+
Інформація про стан ІС та її компонентів	ІзОД	Електронний	+	+	+
Інформація про засоби захисту інформації	ІзОД	Електронний	+	+	+
Трудові договори	ІзОД	Електронний та паперовий	+	+	+
Інформація, пов'язана з виробничою діяльністю	ІзОД	Електронний та паперовий	+	+	+
Інформація про послуги та їх вартість	Відкрита	Електронний та паперовий	-	+	+
Інформація про діяльність підприємства	Відкрита	Електронний та паперовий	-	+	+
Статутні документи підприємства	Відкрита	Електронний та паперовий	-	+	+

Умовні позначення до Таблиці 4

К - вимоги до конфіденційності;

Ц - вимоги до цілісності;

Д - вимоги до доступності;

+ - вимоги наявні; - - вимоги відсутні;

2.7 Інвентаризаційний список АЗ ІКС ТОВ «Еліксир»

Разом з розробленими моделлю порушника, моделлю загроз і документами політики інформаційної безпеки, керівництву компанії подаються інвентаризаційні списки апаратного та програмного забезпечення. Складання інвентаризаційних списків АЗ і ПЗ необхідно для спрощення проєктування, встановлення та налагодження корпоративної комп'ютерної мережі ІКС ТОВ «Еліксир».

Інвентаризаційний список АЗ ІКС ТОВ «Еліксир» наведено у Таблиці 2.5.

Таблиця 2.5 - Інвентаризаційний список АЗ ІКС ТОВ «Еліксир»

Найменування	Призначення	Модель/Характеристики	Дата придбання	Вартість, грн.	IP-адреса	MAC-адреса	Користувач
ПК № 1	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.1	D6:C5:A3:EA:61:27	Фролов О. А.
ПК № 2	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.2	D6:B5:B3:8C:7B:28	Ворона І. М.
ПК № 3	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.3	D6:F9:56:2E:4F:AF	Донцов Д. Р.
ПК № 4	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.4	D6:C2:54:7C:19:B1	Бойчук М. О.
ПК № 5	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.5	D6:AD:5B:57:11:5A	Усов В. Б., Хмизенко К. В., Скороход В. Є
ПК № 6	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.6	D6:84:F0:06:DC:8B	Зініна О. О.
ПК № 7	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.7	D6:F3:6B:B0:7B:61	Кольченко В. М.
ПК № 8	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.8	D6:4A:75:8B:B0:A8	Леньов А. П.
ПК № 9	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.9	D6:96:E1:17:3A:D0	Плетньова В. Л.
ПК № 10	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.10	EF:FB:D2:88:85:05	Руднєв С. М.
ПК № 11	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.11	47:22:CB:D0:D7:0F	Дольчук Г. П.
ПК № 12	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.12	3B:52:29:4B:43:0A	Єненко Ю. М.
ПК № 13	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.13	24:03:79:CE:14:8D	Тимашевська М. А.
ПК № 14	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.14	76:F6:48:73:F7:2D	Тимашевський В. Д.

Продовження таблиці 2.5

Найменування	Призначення	Модель/Характеристики	Дата придбання	Вартість, грн.	IP-адреса	MAC-адреса	Користувач
ПК № 15	Робоча станція	HP HSTNN-Q72C, 4 GB DDR4, Intel Core R3	19.03.2024	8999	192.168.1.15	A3:55:FB:27:08:43	Павлов К. В.
Сервер № 1	Сервер	DELL T110 II (4x3.5) LFF	19.03.2024	6081	192.168.1.20	D6:3E:0B:C8:6F:E4	Бойчук М. О.
Маршрутизатор № 1	Маршрутизатор	TP-LINK TL-WR841N	17.03.2024	750	109.155.209.166 192.168.1.30	DB:B8:FC:40:FC:7B	Бойчук М. О.
Маршрутизатор № 2	Маршрутизатор	TP-LINK TL-WR841N	17.03.2024	750	109.155.209.167 192.168.1.31	59:5C:C0:0B:3D:26	Бойчук М. О.
Комутатор № 1	Комутатор	Mercusys MS105G	22.03.2024	400	192.168.1.51	D6:25:BC:9A:70:9E	Бойчук М. О.
Комутатор № 2	Комутатор	Mercusys MS105G	22.03.2024	400	192.168.1.52	D6:25:BC:9A:70:9E	Бойчук М. О.
Комутатор № 3	Комутатор	Mercusys MS105G	22.03.2024	400	192.168.1.53	D6:25:BC:9A:70:9E	Бойчук М. О.
Комутатор № 4	Комутатор	Mercusys MS105G	22.03.2024	400	192.168.1.54	D6:25:BC:9A:70:9E	Бойчук М. О.
Комутатор № 5	Комутатор	Mercusys MS105G	22.03.2024	400	192.168.1.55	D6:25:BC:9A:70:9E	Бойчук М. О.
Комутатор № 6	Комутатор	Mercusys MS105G	22.03.2024	400	192.168.1.5	D6:25:BC:9A:70:9E	Бойчук М. О.
Принтер № 1	Принтер	Canon i-Sensys MF3010	25.03.2024	12390	192.168.1.2	66:2B:53:28:D1:F2	Ворона І. М.
Принтер № 2	Принтер	Canon i-Sensys MF3010	25.03.2024	12390	192.168.1.6	97:48:94:A7:01:A9	Зініна О. О.
Принтер № 3	Принтер	Canon i-Sensys MF3010	25.03.2024	12390	192.168.1.8	EE:3A:8A:AA:83:8A	Леньов А. П.
Принтер № 4	Принтер	Canon i-Sensys MF3010	25.03.2024	12390	192.168.1.11	D6:CD:64:81:56:85	Дольчук Г. П.

Продовження таблиці 2.5

Найменування	Призначення	Модель/Характеристики	Дата придбання	Вартість, грн.	IP-адреса	MAC-адреса	Користувач
Камера № 1	Камера відеоспостере-ження	TP-LINK Tapo C510W	07.03.2024	2799	192.168.1.5	BF:EE:BC:6D:F7:53	Усов В. Б.
Камера № 2	Камера відеоспостере-ження	TP-LINK Tapo C510W	07.03.2024	2799	192.168.1.5	A0:1A:C9:DA:30:47	Усов В. Б.
Камера № 3	Камера відеоспостере-ження	TP-LINK Tapo C510W	07.03.2024	2799	192.168.1.5	FC:72:4D:FD:71:53	Усов В. Б.
Камера № 4	Камера відеоспостере-ження	TP-LINK Tapo C510W	07.03.2024	2799	192.168.1.5	E9:B1:69:F0:9E:B3	Усов В. Б.
Камера № 5	Камера відеоспостере-ження	TP-LINK Tapo C510W	07.03.2024	2799	192.168.1.5	30:E2:AE:14:C6:2A	Усов В. Б.
Камера № 6	Камера відеоспостере-ження	TP-LINK Tapo C510W	07.03.2024	2799	192.168.1.5	31:BA:1D:BE:23:27	Усов В. Б.
Камера № 7	Камера відеоспостере-ження	TP-LINK Tapo C510W	07.03.2024	2799	192.168.1.5	DF:02:AC:89:96:99	Усов В. Б.

2.8 Інвентаризаційний список ПЗ ІКС ТОВ «Еліксир»

Таблиця 2.6 - Інвентаризаційний список ПЗ ІКС ТОВ «Еліксир»

Назва	**Тип**	**Ліцензія**	**Обладнання**
Windows 10 PRO 64-bit	Системне	Commercial	ПК № 1-15
Windows Server 2016 Essentials	Системне	Commercial	Поштовий сервер, файл-сервер
Microsoft Office 2013	Системне	Commercial	ПК № 1-15
Avira	Системне	Commercial	ПК № 1-15
Adobe Acrobat Reader	Прикладне	OLP	ПК № 1-15
Microsoft Teams	Прикладне	Commercial	ПК № 1-15
Total Commander	Системне	OLP	ПК № 1-15
Adobe Photoshop	Прикладне	Commercial	ПК № 1-15
7-Zip	Прикладне	OLP	ПК № 1-15
Microsoft SQL Server	Системне	Commercial	ПК № 1-15
Microsoft Access	Системне	Commercial	ПК № 1-15
Google Chrome	Прикладне	OLP	ПК № 1-15
Дебет Плюс	Прикладне	Commercial	ПК № 3

Програмне забезпечення модулів управління ІКС підприємства представлене наступними операційними системами, додатками та сервісами:

1. Операційні системи (ОС):

- Windows 10 PRO 64-bit для ПК;
- Windows Server 2016 Essentials для корпоративного сервера.

2. Пакет офісних програм Microsoft Office 2013:

- Текстовий редактор Microsoft Word;
- Табличний процесор Microsoft Excel;
- Додаток для створення та демонстрації презентацій Microsoft PowerPoint;
- Сервіс електронної пошти, персональний та корпоративний планувальник робочого часу Microsoft Outlook;
- Додаток для роботи з замітками Microsoft OneNote;
- Реляційна система керування базами даних (СКБД) Microsoft Access;
- Додаток для підготовки публікацій Microsoft Publisher;
- Сервіс перегляду баз даних та відбору інформації з них Microsoft Query;
- Додаток для роботи з діаграмами та для приведення даних до вигляду діаграм Microsoft Visio;
- Менеджерська система управління проєктами Microsoft Project.

3. Антивірусна програма Avira;
4. Програма для перегляду файлів Adobe Acrobat Reader;
5. Програма для проведення відеодзвінків та групових відеоконференцій Microsoft Teams;
6. Файловий менеджер Total Commander;
7. Програма для обробки зображень Adobe Photoshop;
8. Програма-архіватором 7-Zip;
9. Реляційна СКБД Microsoft SQL Server.

2.9 Інформаційне середовище ТОВ «Еліксир»

Інформація на підприємстві зберігається на двох носіях: електронних і паперових. Більша частина інформації зберігається на електронних носіях, а саме: -на жорстких дисках комп'ютерів, SSD-накопичувачах, USB-флешках, оптичних дисках.

Інформаційне середовище підприємства представлене локальною мережею, яка має вихід до глобальної мережі Internet. Локальна мережа складається з 15 ПК, 4 серверів, 6 комутаторів, 2 маршрутизаторів (1 маршрутизатор для підключення корпоративної комп'ютерної мережі до глобальної мережі Інтернет і 1 Wi-Fi-роутер для використання співробітниками для особистих потреб), 4 принтери, 7 камер відеоспостереження.

Для спрощення графічного представлення комп'ютерної мережі підприємства, розроблено схему корпоративної комп'ютерної мережі та генеральний план підприємства, із вказаним на ньому обладнанням, що входить до складу ІС підприємства.

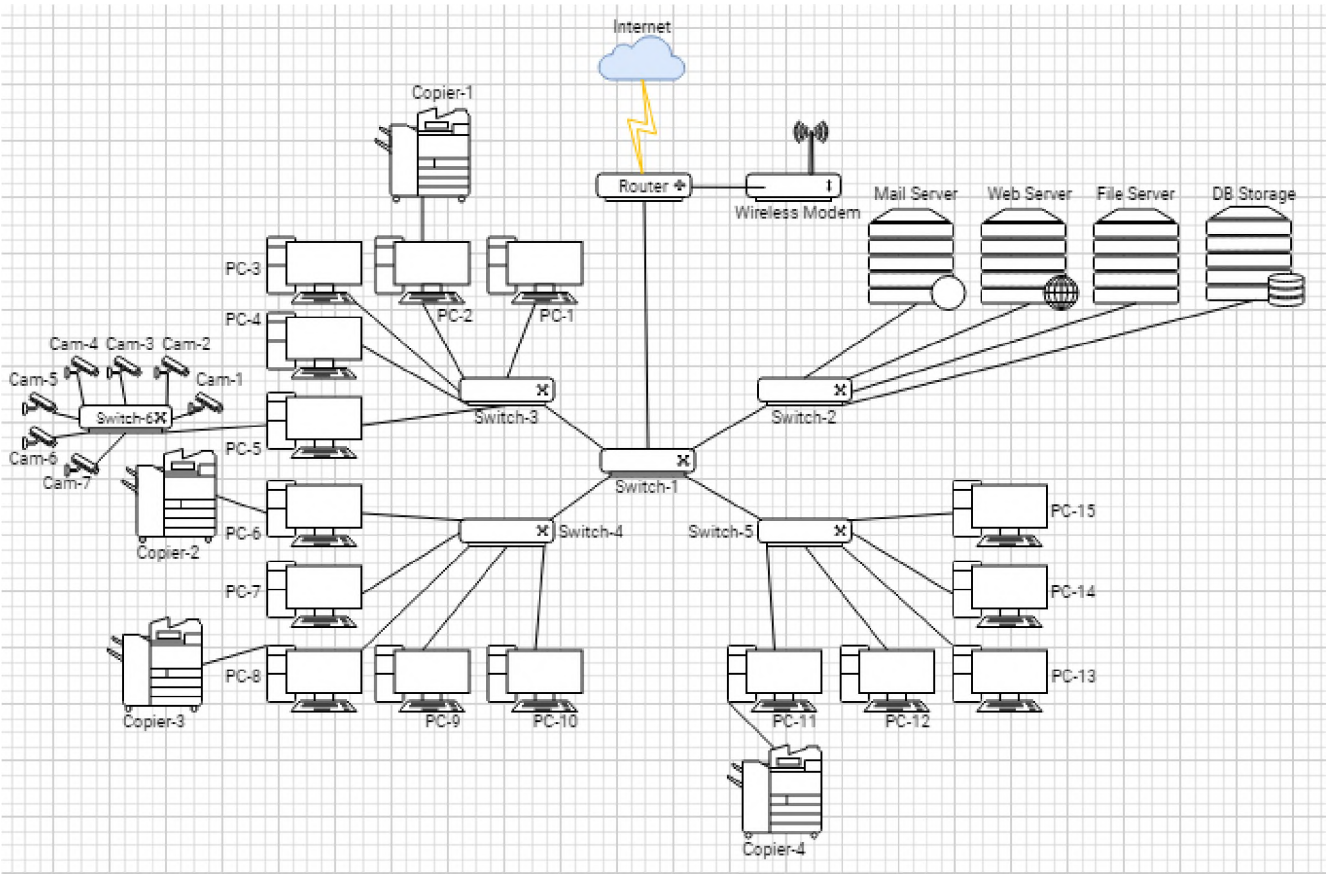

Рисунок 2.1 - Схема комп'ютерної мережі ТОВ «Еліксир»

Мережевий рівень моделі OSI у роботі локальний комп'ютерних мереж виконує дві основні функції: перенаправлення і маршрутизація.

Перенаправлення - це передавання пакету даних між входами і виходами одного маршрутизатора.

Маршрутизація - це передавання пакетів даних, до процесу якого залучено всі маршрутизатори корпоративної локальної мережі. Ці маршрутизатори взаємодіють між собою через протоколи маршрутизації пакетів даних і визначають шляхи передавання пакетів у мережі.

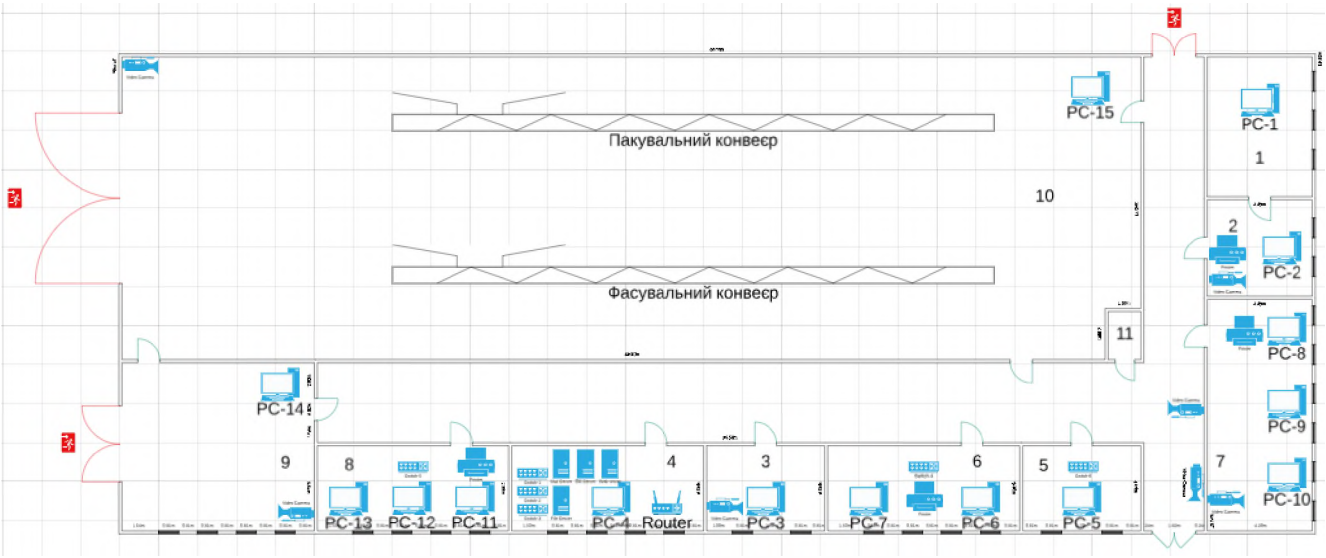

Рисунок 2.2 - Генеральний план ТОВ «Еліксир»

Таблиця 2.7 - Умовні позначення на генеральному плані ТОВ «Еліксир»

Умовне позначення	Обладнання
	Робоча станція (ПК)
	Сервер
	Комутатор
	Камера відеоспостереження
	Маршрутизатор
	Принтер
	Конвеєр

Таблиця 2.8 - Відповідність ПК та мережевого обладнання до приміщень підприємства

Найменування	Тип обладнання	Призначення та номер приміщення	Користувач
ПК № 1	Робоча станція	Кабінет директора (№ 1)	Фролов О. А.
ПК № 2	Робоча станція	Приймальня директора (№ 2)	Ворона І. М.
ПК № 3	Робоча станція	Відділ фінансових операцій (№ 3)	Донцов Д. Р.
ПК № 4	Робоча станція	Відділ системного адміністрування (№ 4)	Бойчук М. О.
ПК № 5	Робоча станція	Пост охорони (№ 5)	Усов В. Б., Хмизенко К. В., Скороход В. Є.
ПК № 6	Робоча станція	Юридичний відділ (№ 6)	Зініна О. О.
ПК № 7	Робоча станція	Юридичний відділ (№ 6)	Кольченко В. М.
ПК № 8	Робоча станція	Відділ продажів (№ 7)	Леньов А. П.
ПК № 9	Робоча станція	Відділ продажів (№ 7)	Плетньова В. Л.
ПК № 10	Робоча станція	Відділ продажів (№ 7)	Руднєв С. М.
ПК № 11	Робоча станція	Відділ хімічних технологій (№ 8)	Дольчук Г. П.
ПК № 12	Робоча станція	Відділ хімічних технологій (№ 8)	Єненко Ю. М.
ПК № 13	Робоча станція	Відділ хімічних технологій (№ 8)	Тимашевська М. А.
ПК № 14	Робоча станція	Лабораторія (№ 9)	Тимашевський В. Д.
ПК № 15	Робоча станція	Пакувальний цех (№ 10)	Павлов К. В.
Комутатор № 1	Комутатор	Відділ системного адміністрування (№ 4)	Бойчук М. О.
Комутатор № 2	Комутатор	Відділ системного адміністрування (№ 4)	Бойчук М. О.
Комутатор № 3	Комутатор	Відділ системного адміністрування (№ 4)	Бойчук М. О.
Комутатор № 4	Комутатор	Юридичний відділ (№ 6)	Бойчук М. О.
Комутатор № 5	Комутатор	Відділ хімічних технологій (№ 8)	Бойчук М. О.
Комутатор № 6	Комутатор	Пост охорони (№ 5)	Бойчук М. О.
Маршрутизатор № 1	Маршрутизатор	Відділ системного адміністрування (№ 4)	Бойчук М. О.
Поштовий сервер	Сервер	Відділ системного адміністрування (№ 4)	Бойчук М. О.
Вебсервер	Сервер	Відділ системного адміністрування (№ 4)	Бойчук М. О.
Файл-сервер	Сервер	Відділ системного адміністрування (№ 4)	Бойчук М. О.
Сховище БД	Сервер	Відділ системного адміністрування (№ 4)	Бойчук М. О.

Для проведення обстеження інформаційного середовища підприємства необхідно визначити, що обстеженню підлягає інформація, яка зберігається та обробляється (одержується, використовується, поширюється) в ІКС підприємства.

В ІКС ТОВ «Еліксир» циркулюють відкрита інформація та ІзОД. До ІзОД в ІКС, що розглядається відносяться: інформація про фізичних осіб, фінансова інформація, юридична інформація, частини комерційної та статистичної інформацій, до яких обмежено доступ, зокрема відомості, що становлять комерційну таємницю.

Комерційна таємниця - це відомості про діяльність компанії, розголошення яких може нашкодити підприємству. Комерційною таємницею є ділова інформація, яка має фактичну або потенційну цінність для підприємства з комерційних причин. Ця інформація є комерційно вигідною для непорядних конкурентів у разі потрапляння до їх рук. Втрата комерційної таємниці може нанести значних збитків підприємству і призвести до його банкрутства.

Таблиця 2.9 - Визначення рівня вимог до забезпечення конфіденційності, цілісності та доступності інформації, що циркулює в ІКС підприємства

№ з/п	Вид інформації	Рівень конфіденційності	Рівень цілісності	Рівень доступності
1	Особисті дані персоналу	К4	Ц4	Д5
2	База даних підприємства	К5	Ц5	Д5
3	Договори, укладені з клієнтами	К3	Ц3	Д4
4	Бухгалтерська звітність	К4	Ц3	Д4
5	Інформація про стан ІС та її компонентів	К5	Ц5	Д5
6	Інформація про засоби захисту інформації	К5	Ц5	Д5
7	Трудові договори	К3	Ц4	Д3
8	Інформація, пов’язана з виробничою діяльністю	К5	Ц5	Д5
9	Інформація про послуги та їх вартість	К1	Ц2	Д4
10	Інформація про діяльність підприємства	К1	Ц2	Д4
11	Статутні документи підприємства	К1	Ц5	Д2

Для класифікації інформації 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.

Оскільки необхідно розробити політику інформаційної безпеки підприємства, потрібно обрати профіль захищеності інформаційно-комунікаційної системи. Політика інформаційної безпеки ІКС має бути наслідком застосування положень документу НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», яким встановлено вимоги до обробки інформації в ІКС.

На документ НД ТЗІ 2.5-004-99 необхідно спиратися не тільки при розробці комплексної системи захисту інформації, а й при проєктуванні системи управління інформаційною безпекою підприємства й при розробці політики ІБ підприємства як частини процесу розробки СУІБ.

ІКС підприємства, що розглядається, згідно НД ТЗІ 2.5-005-99 належить до класу «3», належність до якого характеризує інформаційну систему підприємства як розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію із різним ступенем обмеження доступу, тобто як відкриту інформацію, так і інформацію з обмеженим доступом. Клас ІКС «3» визначається також тим, що у такій системі наявні вузли, які реалізують різну політику ІБ.

Для забезпечення ІБ підприємства необхідно забезпечити дотримання всіх трьох основоположних принципів ІБ: конфіденційності, цілісності та доступності інформації у робочому процесі.

Виходячи з зазначеного, обираємо стандартний функціональний профіль захищеності в ІКС, що входить до складу класу «3» з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації:

3.КЦД.1 = { КД-2, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

2.10 Класифікація ІКС ТОВ «Еліксир» за призначенням

Інформаційні системи можна класифікувати за функціональною ознакою та рівнем управління.

Структура інформаційної системи може бути представлена як сукупність її функціональних підсистем, відповідно, інформаційна система класифікується за функціональною ознакою.

У практиці діяльності виробничих та комерційних об'єктів типовими видами діяльності, які визначають типову ознаку класифікації інформаційних систем, є виробнича, маркетингова, фінансова та кадрова діяльність.

Виробнича діяльність пов'язана з безпосереднім випуском продукції і спрямована на створення і впровадження у виробництво науково-технічних новацій.

Маркетингова діяльність включає:

- аналіз ринку виробників і споживачів продукції, що випускається;
- аналіз продажів;
- організацію рекламної компанії з "просування" продукції;
- раціональну організацію матеріально-технічного постачання.

Фінансова діяльність пов'язана із організацією контролю і аналізу фінансових ресурсів організації на основі бухгалтерської, статистичної та оперативної інформації.

Кадрова діяльність спрямована на підбір і розстановку необхідних фахівців, а також ведення службової документації з різних аспектів.

Зазначені напрями діяльності визначають типовий набір інформаційних систем:

- виробничі системи;
- системи маркетингу;

- фінансові системи і системи обліку;
- кадрові системи;
- інші типи систем, що виконують допоміжні функції залежно від специфіки діяльності підприємства (організації).

ІКС, що аналізується, за своїми функціональними ознаками характеризується як комплексна інформаційна система, тому що її призначення охоплює діяльність всіх підрозділів, з яких складається компанія, незалежно від напряму діяльності кожного з них. Складність задачі з проєктування та підтримки поданої ІКС полягає в тому, що вона водночас є виробничою, менеджерською системою, фінансовою та управлінською системою.

2.11 Модель інформаційних потоків в ІКС підприємства

В інформаційному середовищі ТОВ «Еліксир» постійно циркулюють наступні інформаційні потоки:

1. Інформація про клієнтів компанії;
2. Інформація про співробітників компанії;
3. Інформація про товари, які виробляє підприємство;
4. Інформація довідково-енциклопедичного характеру;
5. Науково-технічна інформація;
6. Фінансова інформація;
7. Податкова інформація;
8. Правова інформація;
9. Статистична інформація;
10. Соціологічна інформація;
11. Критична інформація про виробничі процеси.

Визначені інформаційні потоки наведено на схемі інформаційних потоків в ІКС ТОВ «Еліксир»:

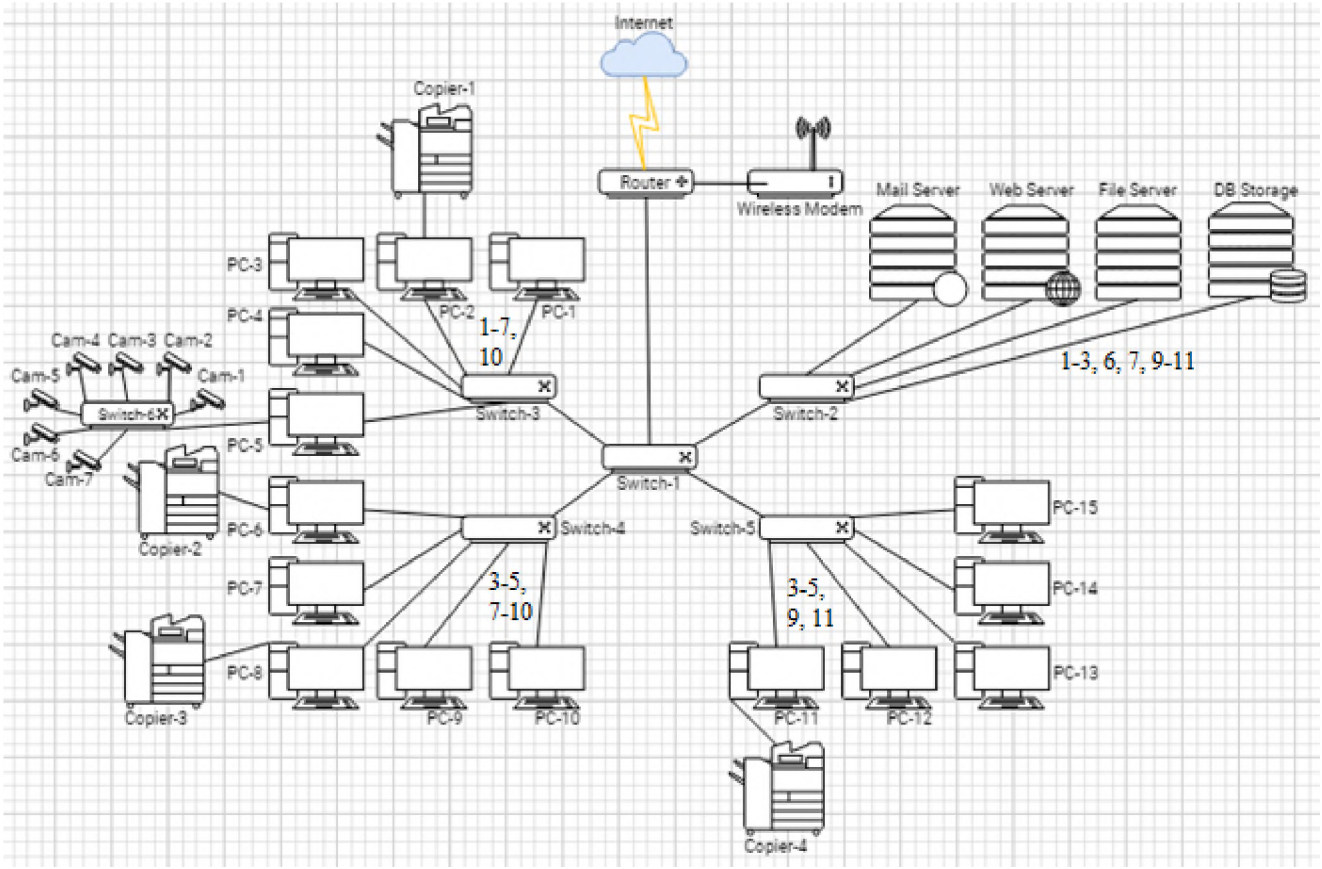

Рисунок 2.3 - Схема інформаційних потоків в ІКС ТОВ «Еліксир»

2.12 Ресурси ІКС ТОВ «Еліксир», на яких зберігається ІзОД підприємства

В ІКС ТОВ «Еліксир» ІзОД зберігається на корпоративному сервері баз даних, файл-сервері, поштовому сервері DELL T110 II (4x3.5) LFF. IP-адреса сервера: 192.168.1.15; MAC-адреса сервера: D6:3E:0B:C8:6F:E4.

Корпоративний сервер є основним вузлом комп'ютерної мережі компанії, тому забезпечення ІБ сервера, безперервності, безвідмовності його функціонування є пріоритетним напрямком роботи відділу системного адміністрування. Положення ПІБ обов'язково мають регулювати процес захисту сервера, оскільки його захист від кібератак, впливу шкідливого ПЗ та інших несприятливих факторів є критично важливим.

Інформація, що зберігається на серверах у процесі її обробки на підприємстві проходить через 6 комутаторів підприємства, Wi-Fi-маршрутизатор, а також може проходити через інші вузли комп'ютерної мережі. У політиці інформаційної безпеки необхідно врегулювати питання реагування на

кібератаки, спрямовані на перехоплення інформації та пакетів даних під час їх передавання комутаторами та маршрутизатором.

2.13 Модель загроз ІКС ТОВ «Еліксир»

Загроза безпеці інформації - це дія, спрямована проти об'єкта захисту, що виявляється в небезпеці спотворень і втрат інформації.

У визначенні загрози безпеці інформації йдеться не про всю інформацію, що циркулює в ІКС, а тільки про ту її частину, яка на думку її власника (користувача) має комерційну цінність (інформація як товар) або підлягає захисту в силу закону (конфіденційна інформація).

Загрози безпеці інформації, що циркулює в корпоративній мережі, за джерелом походження класифікуються на 3 основні групи:

1. Загрози, зумовлені діями суб'єктів (антропогенні загрози);

Антропогенні загрози можуть розподілятися за своїм походженням на внутрішні та зовнішні.

Зовнішніми антропогенними загрозами є кібератаки на конфіденційність, цілісність та доступність інформації, що циркулює в ІКС підприємства; атаки, спрямовані на безперервність функціонування ІКС. Атаки можуть вчинятися з мотивів промислового шпіонажу, перешкоджання роботі компанії з боку недобросовісних конкурентів, вандалізму.

Внутрішніми антропогенними загрозами зазвичай є ненавмисні дії працівників. У деяких випадках внутрішні загрози можуть супроводжуватися проникненням промислових шпигунів безпосередньо до штату співробітників компанії.

Протидія антропогенним загрозам інформаційній безпеці є головним завданням відділу системного адміністрування. Загрозам людської природи можна ефективно протидіяти при правильній роботі спеціалістів з інформаційної безпеки підприємства та керівництва компанії.

2. Загрози, зумовлені технічними засобами (техногенні загрози);

Основними техногенними загрозами є збої у роботі корпоративного ПЗ, вихід з ладу або руйнування технічних засобів обробки інформації, окремих компонентів ІКС, системи електроживлення та інші.

3. Загрози, зумовлені стихійними джерелами.

Стихійні загрози можуть мати природне та техногенне походження. Типовими стихійними загрозами є пожежі, повені, штормові погодні умови.

Модель загроз інформаційної безпеки підприємства є внутрішнім корпоративним документом, який встановлює можливі імовірні загрози (ризики) для інформаційної безпеки підприємства, джерела їх походження та можливі несприятливі наслідки для компанії у разі невжиття заходів щодо ліквідації, уникнення або зниження таких ризиків.

Існує велика кількість варіантів моделей загроз інформаційній безпеці корпоративної мережі підприємства. З цих моделей на місце опорної можна обирати будь-яку, але необхідно враховувати, що модель загроз має складатися з якомога більшої кількості можливих варіантів несприятливих подій та надзвичайних ситуацій (НС). При включенні певної загрози до моделі може аналізуватися також і ймовірність її виникнення, але кількісне значення такої ймовірності не впливає на якісний зміст моделі. Список загроз може поповнюватися, якщо певна загрозлива обставина має будь-яку ймовірність проявлення в роботі системі відмінну від нульової.

Модель загроз інформаційній безпеці є основним джерелом даних при проведенні аналізу ризиків інформаційній безпеці підприємства.

Модель загроз складається з:

- загального визначення кожної можливої загрози;
- наведених усіх можливих механізмів реалізації загрози;
- визначення потенційного джерела загрози;
- оцінки можливих наслідків реалізації загрози із визначенням.

Таблиця 2.10 - Модель загроз ІКС ТОВ «Еліксир»

№ з/п	Вид загрози	Можливий механізм реалізації	Джерело загрози	Наслідки	Ефективний рівень загрози
1	Катастрофа	Пожежа	Зовнішнє середовище	Ц, Д	Р1
2	Хакерські атаки	Злам системи	Порушник	К, Ц	Р2
3	Крадіжка носія інформації	Проникнення до офісу у неробочий час	Порушник, працівник	К, Д	Р3
4	Вірусне зараження	Завантаження комп'ютерних вірусів, черв'яків, троянів	Порушник, працівник	Ц, Д	Р4
5	Соціальна інженерія	Незаконне отримання ІзОД через промислове шпигунство з боку працівників	Порушник	К	Р3
6	Відмова в обслуговуванні	Виведення з ладу системи бухгалтерського обліку	Порушник, працівник	Ц, Д	Р4
7	Використання системи в корисних цілях	Копіювання коду ПЗ	Працівник	К	Р4
8	Компрометація інформації при передаванні	Підглядування за роботою секретаря	Порушник	К	Р2
9	Аварія обладнання	Стрибок напруги в мережі	Технічні засоби	Д	Р3
10	Переповнення ІС	Нестача зовнішніх носіїв інформації	Працівник, технічні засоби	Д	Р2
11	Віддалений шпіонаж	Встановлення закладних пристроїв, шпигунського ПЗ	Порушник	К	Р1
12	Підслуховування	Підслуховування нарад	Порушник, працівник	К	Р2
13	Крадіжка носіїв інформації або документів	Крадіжка жорсткого диску або SSD-накопичувача	Порушник, працівник	К, Д	Р4
14	Відновлення носіїв, які було використано або викинуто	Несанкціоноване використання програм відновлення даних, атаки типу «збір сміття»	Порушник, працівник	К	Р3
15	Фальсифікація прав	Несанкціоноване виготовлення та використання копії ЕЦП	Порушник, працівник	Д	Р2

Продовження таблиці 2.10

№ з/п	Вид загрози	Можливий механізм реалізації	Джерело загрози	Наслідки	Ефективний рівень загрози
16	Руйнування	Згорання технічних засобів обробки інформації в результаті пожежі на підприємстві	Зовнішнє середовище	Д	Р1
17	Підміна	Підміна прикладних програм схожим за інтерфейсом шкідливим ПЗ	Порушник	К, Д	Р2
18	Переривання	Порушення пропускної здатності каналів зв'язку, обсягів вільної оперативної пам'яті, дискового простору, електроживлення ІКС	Порушник, працівник, технічні засоби	Д	Р3
19	Помилки	Помилки під час інсталяції та експлуатації ПЗ, технічних засобів обробки інформації	Технічні засоби	Д	Р4
20	Несанкціоноване перехоплення інформації	Перехоплення інформації за рахунок ПЕМВ від технічних засобів, за рахунок наведень по лініях електроживлення, за рахунок наведень по сторонніх провідниках, акустичним каналом від засобів виведення, під час підключення до каналів передавання інформації	Порушник	К	Р2

Специфікація моделі загроз за рівнем реалізації загроз ІБ компанії:

- Р1 - низький;
- Р2 - нижчий за середній;
- Р3 - середній;
- Р4 - вищий за середній;
- Р5 - високий.

2.14 Модель порушника ІБ ТОВ «Еліксир»

Модель порушника інформаційної безпеки - це узагальнений опис суб'єктів, які можуть становити найбільш імовірну загрозу ІБ ІКС підприємства.

Модель порушника ІБ створюється з метою систематизації та аналізу антропогенних загроз ІБ підприємства, створення портрету можливого порушника ІБ, мотивації зловмисних дій порушника ІБ, доступних порушнику ІБ спеціалізованих знань, технічних засобів, відомостей про стан та порядок функціонування корпоративної ІКС, іншої ІзОД.

Навмисне порушення ІБ компанії може здійснюватися з метою:

- отримання НСД до обігових грошових коштів компанії;
- отримання НСД до ІзОД (комерційної таємниці);
- вчинення дій, спрямованих на завдання репутаційних втрат компанії;
- перешкоджання роботі компанії;
- вчинення хуліганських дій.

Також порушення ІБ компанії може бути здійснене ненавмисне некваліфікованими користувачами корпоративної ІКС або через помилки системного адміністратора.

Як антропогенні загрози ІБ компанії можуть бути внутрішніми та зовнішніми, так і порушники інформаційної безпеки поділяються на ці ж категорії. Внутрішніми порушниками ІБ підприємства можуть виступати користувачі або адміністратор ІКС, зовнішніми порушниками - особи, які вчиняють зловмисні дії відносно ІБ корпоративної ІКС з поза меж підприємства (хакери); найнятий зовнішній технічний персонал, що виконує роботи зі встановлення, налагодження та підтримки корпоративної ІКС, прокладання ліній електроживлення, зв'язку та кабельного інтернету, будівельні робітники; відвідувачі підприємства як імовірні промислові шпигуни або агенти впливу недобросовісних конкурентів; співробітники компанії, які не є користувачами ІКС.

Зовнішні порушники ІБ компанії можуть відрізнятися один від одного за рівнем знань, навичок та досвіду із отримання НСД до захищених ІКС,

доступним їм для вчинення зловмисних дій ПЗ та АЗ. Ступінь кваліфікації хакерів та інших потенційних порушників ІБ суттєво впливає на рівень загрози інформаційній безпеці компанії, який вони можуть становити.

Таблиця 2.11 - Модель порушника ІБ ТОВ «Еліксир»

Посада (статус)	Мотив	Кваліфікація	Місце дії	Час дії	Ефективний рівень загрози
Внутрішні порушники інформаційної безпеки					
Директор	М3	К1	Д4	Ч1	Р4
Секретар	М3	К1	Д4	Ч3	Р4
Бухгалтер	М1, М3	К1	Д3	Ч3	Р4
Системний адміністратор	М3	К4	Д5	Ч3	Р5
Юрисконсульт	М2, М3	К1	Д3	Ч3	Р3
Менеджер	М1, М3	К1	Д3	Ч3	Р3
Хімік-технолог	М2, М3	К1	Д3	Ч3	Р3
Охоронець	М1, М3	К1	Д3	Ч2	Р4
Фасувальник	М3	К0	Д3	Ч2	Р2
Пакувальник	М3	К0	Д3	Ч2	Р2
Зовнішні порушники інформаційної безпеки					
Хакери	М1, М2	К6	Д1	Ч2, Ч3	Р2
Вандали	М2	К3	Д1	Ч2, Ч3	Р3
Зовнішній технічний персонал	М3	К5	Д4	Ч1, Ч2	Р3

Специфікація моделі порушника за професійним рівнем порушників:

- М1 - отримання НСД до обігових грошових коштів компанії або до інформації з обмеженим доступом;
- М2 - вчинення дій, спрямованих на завдання репутаційних втрат компанії, перешкоджання роботі компанії, вчинення хуліганських дій;
- М3 - помилка системного адміністратора, користувачів ІКС, робітників технічного обслуговування корпоративної ІКС.

Специфікація моделі порушника за професійним рівнем порушників:

- К0 - не має даних про функціональні особливості корпоративної ІКС;
- К1 - розуміє функціональні особливості системи, має досвід роботи з АЗ та ПЗ корпоративної ІКС;
- К2 - володіє високим рівнем знань та практичними навичками роботи з АЗ та ПЗ корпоративної ІКС та їх обслуговування;
- К3 - має високий рівень знань у галузі програмування та обчислювальної техніки, проєктування та особливостей експлуатації ІКС;
- К4 - має дані про функціональні можливості КЗЗ;
- К5 - має дані про вразливості вбудованих у ПЗ ІКС засобів захисту та про повний перелік його функціональних можливостей;
- К6 - є розробником системного програмного забезпечення або ПЗ комплексу засобів захисту ІКС.

Специфікація моделі порушника за місцем порушення ІБ компанії:

- Д1 - з-поза меж підприємства;
- Д2 - з приміщень підприємства;
- Д3 - з робочих станцій користувачів корпоративної ІКС;
- Д4 - з доступом до серверного обладнання та сховищ БД;
- Д5 - з зони керування КЗЗ ІКС підприємства.

Специфікація моделі порушника за часом порушення ІБ компанії:

- Ч1 - до впровадження КЗЗ корпоративної ІКС;
- Ч2 - під час припинення роботи засобів захисту ІКС;
- Ч3 - під час роботи ІКС та її комплексу засобів захисту.

Специфікація моделі порушника за рівнем реалізації загроз ІБ компанії:

- Р1 - низький;
- Р2 - нижчий за середній;
- Р3 - середній;
- Р4 - вищий за середній;

- Р5 - високий.

2.15 Розробка змісту документів політики інформаційної безпеки ТОВ «Еліксир»

Проаналізувавши розроблені модель загроз ІКС і модель порушника ІБ, з метою зниження ефективного рівня виявлених найбільш критичних загроз інформаційній безпеці підприємства, розроблено наступні п'ять документів політики інформаційної безпеки ТОВ «Еліксир»:

Політика автентифікації користувачів корпоративної ІКС ТОВ «Еліксир» з використанням особистих ключів і паролів

Мета: підвищити рівень ІБ ТОВ «Еліксир» встановленням єдиного зведення правил використання особистих ключів і паролів для підключення до вузлів або сегментів корпоративної ІКС.

Область дії: політика автентифікації користувачів корпоративної ІКС ТОВ «Еліксир» з використанням особистих ключів і паролів поширюється на корпоративну ІКС ТОВ «Еліксир», її користувачів та адміністратора і діє на території компанії, інформаційні потоки якої циркулюють в зазначеній ІКС.

Правила використання особистих ключів та паролів:

1. Паролі та особисті ключі користувачів ІКС мають бути унікальними;

2. Пароль для входу до елементу ІКС повинен складатися не менш ніж з 8 символів, серед яких обов'язково мають бути 1 велика літера, 1 мала літера, 1 цифра і 1 спеціальний символ. Для створення паролів використовуються літери англійської абетки;

3. Пароль не повинен складатися зі словникових слів, очевидних послідовностей символів, які легко підібрати або вгадати;

4. Пароль для входу до елементу ІКС розробляється спеціалістом з ІБ - системним адміністратором;

5. Забороняється передавати користувацькі паролі та особисті ключі стороннім особам;

6. Забороняється зберігати паролі на непристосованих носіях інформації, в незашифрованому вигляді (записувати на паперових носіях інформації, зберігати на жорсткому диску ПК та ін.);

7. Паролі та особисті ключі користувачів ІКС ТОВ «Еліксир» змінюються не рідше ніж 1 раз на рік та після кожного інциденту порушення ІБ підприємства.

Відповідальність:

Системний адміністратор несе дисциплінарну відповідальність за вжиття недостатніх заходів щодо забезпечення надійності особистих ключів та конфіденційності зберігання паролів. Користувачі ІКС ТОВ «Еліксир» несуть дисциплінарну відповідальність за зберігання особистих ключів та паролів на непристосованих носіях інформації в незашифрованому вигляді та за передавання своїх користувацьких паролів стороннім особам.

Порядок перегляду політики автентифікації користувачів корпоративної ІКС ТОВ «Еліксир» з використанням особистих ключів і паролів:

Політика автентифікації користувачів корпоративної ІКС ТОВ «Еліксир» з використанням особистих ключів і паролів може переглядатися за рішенням системного адміністратора або директора підприємства за потреби, у разі виникнення нових загроз ІБ ІКС ТОВ «Еліксир» або у випадку порушення ІБ корпоративної ІКС.

Політика безпеки корпоративних серверів ТОВ «Еліксир»

Мета: підвищити рівень ІБ ТОВ «Еліксир» встановленням єдиного зведення правил використання та обслуговування серверного обладнання та сховищ даних корпоративної ІКС.

Область дії: політика безпеки корпоративних серверів ТОВ «Еліксир» поширюється на сервери та сховища даних корпоративної ІКС ТОВ «Еліксир», їх користувачів та адміністратора і діє на території компанії, інформаційні потоки якої циркулюють в зазначеній ІКС.

Правила використання та обслуговування серверного обладнання та сховищ даних:

1. Процесом функціонування серверного обладнання та сховищ даних в ІКС керує системний адміністратор;

2. Системний адміністратор за дозволу директора підприємства має доступ до апаратної та програмної частин корпоративного серверного обладнання. Доступ до апаратної частини здійснюється при ремонті та обслуговування серверного устаткування, доступ до програмної частини здійснюється системним адміністратором з метою обслуговування серверів як через пряме підключення робочої станції до сервера, так і через віддалене робоче місце адміністратора сервера;

3. При введенні в дію політики безпеки корпоративних серверів ТОВ «Еліксир» у корпоративній ІКС функціонує 1 сервер: DELL T110 II (4x3.5) LFF. Даний сервер у корпоративній ІКС виконує функції комплексного вузла мережі, обслуговуючи 8 окремих інформаційних потоків, та складається з 4-х частин: поштовий сервер, файловий сервер, сховище БД та частково вебсервер;

4. Функції поштового сервера серверне обладнання виконує при обробці даних листів корпоративної електронної пошти з власним поштовим доменом @elixyr.com;

5. Функції файлового сервера серверне обладнання виконує як додатковий до пам'яті на робочих станціях обсяг пам'яті для зберігання файлів та обсяг пам'яті для резервного копіювання файлів, що здійснюється з метою мінімізації наслідків інцидентів ІБ;

6. Функції сховища БД серверне обладнання виконує як обсяг пам'яті для зберігання робочих баз даних різної галузевої спрямованості, зокрема й БД з обмеженим доступом, що містять комерційну таємницю;

7. Функції вебсервера серверне обладнання виконує як додаткове до хмарних сховищ місце зберігання даних та як ресурс для обробки даних вебсайту підприємства, зберігання відомостей з цього вебресурсу підприємства;

8. Забороняється доступ до серверного обладнання ТОВ «Еліксир» користувачами корпоративної ІКС без отримання на це письмового дозволу системного адміністратора.

Відповідальність:

Системний адміністратор несе дисциплінарну відповідальність за вжиття недостатніх заходів щодо забезпечення безпеки корпоративних серверів та сховищ даних ТОВ «Еліксир». Користувачі ІКС ТОВ «Еліксир» несуть дисциплінарну відповідальність за передавання будь-яких даних або їх частини стороннім особам.

Порядок перегляду політики безпеки корпоративних серверів та сховищ даних ТОВ «Еліксир»:

Політика безпеки корпоративних серверів та сховищ даних ТОВ «Еліксир» може переглядатися за рішенням системного адміністратора або директора підприємства за потреби, у разі виникнення нових загроз ІБ ІКС ТОВ «Еліксир» або у випадку порушення ІБ корпоративної ІКС або її серверного обладнання.

Політика використання систем виявлення вторгнень та організації антивірусного захисту ІКС ТОВ «Еліксир»

Мета: підвищити рівень ІБ ТОВ «Еліксир» встановленням єдиного зведення правил використання систем виявлення вторгнень та організації антивірусного захисту корпоративної ІКС.

Область дії: політика використання систем виявлення вторгнень та організації антивірусного захисту ІКС ТОВ «Еліксир» поширюється на корпоративну ІКС ТОВ «Еліксир», її користувачів та адміністратора і діє на території компанії, інформаційні потоки якої циркулюють в зазначеній ІКС.

Правила використання систем виявлення вторгнень та організації антивірусного захисту

1. Керівну роль у забезпеченні антивірусного захисту вузлів корпоративної комп'ютерної мережі, в управлінні системою виявлення вторгнень до ІКС (IDS), системою попередження вторгнень до ІКС (IPS) має системний адміністратор;

2. Програмні засоби захисту від негативного впливу шкідливого ПЗ на роботу ІКС ТОВ «Еліксир» встановлюються на вузли або сегменти комп'ютерної

мережі і налаштовуються в автоматичний режим роботи заздалегідь до початку роботи з робочими станціями та іншими складовими мережі;

3. При кожному запуску робочої станції, її пам'ять має перевірятися антивірусним ПЗ на наявність вірусів, черв'яків, троянів та іншого шкідливого ПЗ за його сигнатурами в автоматичному режимі;

4. Вся інформація з потоків, що входять у локальну корпоративну комп'ютерну мережу (зокрема файли, які пропонується завантажити зі змісту листування електронною поштою їх відправниками, а також підозрілі файли, що завантажуються з мережі Internet) має перевірятися на наявність шкідливого ПЗ;

5. На підприємстві серед персоналу, який у своїй роботі використовує корпоративну ІКС, проводиться навчальна та роз'яснювальна робота щодо профілактики завантаження вірусних програм до системи, щодо правил поводження з підозрілими посиланнями та файлами невідомого змісту, щодо методів соціальної інженерії, які можуть застосовуватися з боку кіберзлочинців або недобросовісних конкурентів (спаму, фішингу та ін.);

6. Один раз на квартал на підприємстві проводяться повні планові перевірки робочих станцій, серверного обладнання та інших вузлів комп'ютерної мережі на наявність шкідливого ПЗ, слідів вторгнень до ІКС компанії;

7. З метою зниження ризику зараження робочих станцій співробітників комп'ютерними вірусами користувачам забороняється відкривати посилання сумнівного змісту, надіслані від невідомих користувачів файли без попередньої перевірки їх вмісту адміністратором системи.

Відповідальність:

Системний адміністратор несе дисциплінарну відповідальність за вжиття недостатніх заходів щодо забезпечення захищеності ІКС підприємства від негативного впливу шкідливого ПЗ. Системний адміністратор несе дисциплінарну відповідальність за несвоєчасне реагування на вторгнення до ІКС.

Порядок перегляду політики автентифікації користувачів корпоративної ІКС ТОВ «Еліксир» з використанням особистих ключів і паролів:

Політика використання систем виявлення вторгнень та організації антивірусного захисту ІКС ТОВ «Еліксир» може переглядатися за рішенням системного адміністратора або директора підприємства за потреби, у разі виникнення нових загроз ІБ ІКС ТОВ «Еліксир» або у випадку порушення ІБ корпоративної ІКС.

Політика організації доступу до конфіденційної інформації в інформаційному середовищі ТОВ «Еліксир»

Мета: підвищити рівень ІБ ТОВ «Еліксир» встановленням єдиного зведення правил надання та отримання доступу до конфіденційної інформації, що обробляється в ІКС ТОВ «Еліксир».

Область дії: політика організації доступу до конфіденційної інформації в інформаційному середовищі ТОВ «Еліксир» поширюється на корпоративну ІКС ТОВ «Еліксир», її користувачів та адміністратора і діє на території компанії, інформаційні потоки якої циркулюють в зазначеній ІКС.

Правила надання та отримання доступу до конфіденційної інформації, що обробляється в корпоративній ІКС ТОВ «Еліксир»

1. В ІКС ТОВ «Еліксир» конфіденційною інформацією, що обробляється у системі, є комерційна таємниця;

2. Допуск до роботи з конфіденційною інформацією, що обробляється на підприємстві, надає директор підприємства;

3. Якщо конфіденційна інформація пов'язана з рецептурами лікарських засобів та біологічно активних речовин, надання допуску до роботи з нею надається колегіальним рішенням директора підприємства, головного хіміка-технолога і завідувача лабораторією;

4. Допуск до роботи з конфіденційною інформацією, що обробляється у компанії, є документом, реквізити якого реєструються в електронному журналі видачі допусків до роботи з конфіденційною інформацією секретарем;

5. Допуск до роботи з конфіденційною інформацією, що обробляється на підприємстві видається директором підприємства на термін не більше 30 днів;

6. При звільненні співробітника з підприємства його допуск до роботи з конфіденційною інформацією, що обробляється на підприємстві негайно вилучається;

7. Звільнення співробітника, який в межах здійснення своєї діяльності мав доступ до комерційної таємниці, є підставою для позапланової зміни паролів та особистих ключів доступу до вузлів та сегментів корпоративної мережі ТОВ «Еліксир»;

8. Забороняється надавати доступ до роботи з конфіденційною інформацією, що обробляється в ІКС ТОВ «Еліксир», співробітникам підприємства, які не отримали допуску до роботи з конфіденційною інформацією від директора підприємства.

Відповідальність:

Директор підприємства несе відповідальність за наслідки вжиття недостатніх заходів щодо забезпечення захищеності підприємства від несанкціонованого доступу до комерційної таємниці. Порушники порядку доступу до конфіденційної інформації несуть дисциплінарну або кримінальну відповідальність згідно чинного законодавства України в залежності від тяжкості спричинених порушенням правил отримання доступу до роботи з конфіденційною інформацією негативних наслідків для підприємства.

Порядок перегляду політики автентифікації користувачів корпоративної ІКС ТОВ «Еліксир» з використанням особистих ключів і паролів:

Політика організації доступу до конфіденційної інформації в інформаційному середовищі ТОВ «Еліксир» може переглядатися за рішенням директора підприємства за потреби, у разі виникнення нових загроз ІБ ІКС ТОВ «Еліксир» або у випадку порушення ІБ корпоративної ІКС.

Політика організації роботи відділу системного адміністрування ТОВ «Еліксир»

Мета: підвищити рівень ІБ ТОВ «Еліксир» встановленням обов'язків, правил, основних напрямків і принципів роботи співробітників відділу системного адміністрування.

Область дії: політика організації роботи відділу системного адміністрування ТОВ «Еліксир» поширюється на співробітників відділу системного адміністрування і діє на території компанії.

Правила, основні напрямки і принципи роботи відділу системного адміністрування ТОВ «Еліксир»

1. Відділ системного адміністрування ТОВ «Еліксир» є відокремленим підрозділом компанії на чолі з системним адміністратором;

2. Співробітники відділу системного адміністрування підпорядковуються директору підприємства. Директор підприємства організовує роботу відділу системного адміністрування, забезпечує відділ системного адміністрування сучасним АЗ та виділяє грошові кошти на закупівлі необхідних для робочого процесу відділу системного адміністрування та ІКС ТОВ «Еліксир» програмних продуктів;

3. Системний адміністратор несе відповідальність за стан ІБ ІКС підприємства;

4. Відділ системного адміністрування:

- встановлює та налаштовує на вузли або сегменти ІКС необхідне ПЗ;
- встановлює, налагоджує, ремонтує і замінює АЗ корпоративної ІКС;
- забезпечує безперервність роботи ІКС підприємства;
- керує КЗЗ ІКС ТОВ «Еліксир»;
- проєктує і налагоджує корпоративну комп'ютерну мережу ТОВ «Еліксир».

5. Співробітники відділу системного адміністрування можуть мати допуск до роботи з конфіденційною інформацією.

6. Співробітники відділу системного адміністрування ТОВ «Еліксир» у своїй роботі повинні неухильно дотримуватися вимог ПІБ ТОВ «Еліксир».

Відповідальність:

Системний адміністратор та директор підприємства несуть матеріальну відповідальність за стан збереження АЗ ІКС ТОВ «Еліксир». Системний адміністратор несе дисциплінарну відповідальність за вжиття недостатніх

заходів щодо забезпечення захищеності ІКС підприємства від негативного впливу шкідливого ПЗ, від негативних наслідків некоректної роботи АЗ ІКС. Системний адміністратор несе дисциплінарну відповідальність за несвоєчасне реагування на вторгнення до ІКС та інші інциденти ІБ в ІКС ТОВ «Еліксир».

Порядок перегляду політики організації роботи відділу системного адміністрування ТОВ «Еліксир»:

Політика організації роботи відділу системного адміністрування ТОВ «Еліксир» може переглядатися за рішенням директора підприємства за потреби, у разі виникнення нових загроз ІБ ІКС ТОВ «Еліксир» або у випадку порушення ІБ корпоративної ІКС.

2.16 Модель загроз ІКС ТОВ «Еліксир» після впровадження політики інформаційної безпеки ТОВ «Еліксир»

Впровадження у робочий процес підприємства фармацевтичної галузі ТОВ «Еліксир» розробленої політики інформаційної безпеки прямо покращить стан захищеності корпоративної ІКС. Слідування правилам розроблених документів ПІБ безпосередньо знизить імовірність реалізації загроз корпоративній ІКС. Зменшити ризики настання загроз інформаційній безпеці підприємства покликані розроблені п’ять документів ПІБ ТОВ «Еліксир», а саме:

- політика автентифікації користувачів корпоративної ІКС ТОВ «Еліксир» з використанням особистих ключів і паролів;
- політика безпеки корпоративних серверів ТОВ «Еліксир»;
- політика використання систем виявлення вторгнень та організації антивірусного захисту ІКС ТОВ «Еліксир»;
- політика організації доступу до конфіденційної інформації в інформаційному середовищі ТОВ «Еліксир»;
- політика організації роботи відділу системного адміністрування ТОВ «Еліксир».

Після впровадження ПІБ у робочий процес підприємства, для того, щоб проаналізувати її ефективність, необхідно розробити оновлену модель загроз

ІКС ТОВ «Еліксир», у якій при оцінці рівня реалізації загроз ІБ компанії буде враховано позитивний вплив дотримання політики інформаційної безпеки на ефективний рівень реалізації загроз інформаційній безпеці.

Таблиця 2.12 - Модель загроз ІКС ТОВ «Еліксир» після впровадження у робочий процес підприємства розробленої політики інформаційної безпеки

№ з/п	Вид загрози	Можливий механізм реалізації	Джерело загрози	Наслідки	Ефективний рівень загрози
1	Катастрофа	Пожежа	Зовнішнє середовище	Ц, Д	Р1
2	Хакерські атаки	Злам системи	Порушник	К, Ц	Р1 (-1)
3	Крадіжка носія інформації	Проникнення до офісу у неробочий час	Порушник, працівник	К, Д	Р2 (-1)
4	Вірусне зараження	Завантаження комп'ютерних вірусів, черв'яків, троянів	Порушник, працівник	Ц, Д	Р2 (-2)
5	Соціальна інженерія	Незаконне отримання ІзОД через промислове шпигунство з боку працівників	Порушник	К	Р2 (-1)
6	Відмова в обслуговуванні	Виведення з ладу системи бухгалтерського обліку	Порушник, працівник	Ц, Д	Р3 (-1)
7	Використання системи в корисних цілях	Копіювання коду ПЗ	Працівник	К	Р2 (-2)
8	Компрометація інформації при передаванні	Підглядування за роботою секретаря	Порушник	К	Р2
9	Аварія обладнання	Стрибок напруги в мережі	Технічні засоби	Д	Р3
10	Переповнення ІС	Нестача зовнішніх носіїв інформації	Працівник, технічні засоби	Д	Р2
11	Віддалений шпіонаж	Встановлення закладних пристроїв, шпигунського ПЗ	Порушник	К	Р1
12	Підслуховування	Підслуховування нарад	Порушник, працівник	К	Р2
13	Крадіжка носіїв інформації або документів	Крадіжка жорсткого диску або SSD-накопичувача	Порушник, працівник	К, Д	Р2 (-2)

Продовження таблиці 2.12

№ з/п	Вид загрози	Можливий механізм реалізації	Джерело загрози	Наслідки	Ефективний рівень загрози
14	Відновлення носіїв, які було використано або викинуто	Несанкціоноване використання програм відновлення даних, атаки типу «збір сміття»	Порушник, працівник	К	Р2 (-1)
15	Фальсифікація прав	Несанкціоноване виготовлення та використання копії ЕЦП	Порушник, працівник	Д	Р1 (-1)
16	Руйнування	Згорання технічних засобів обробки інформації в результаті пожежі на підприємстві	Зовнішнє середовище	Д	Р1
17	Підміна	Підміна прикладних програм схожим за інтерфейсом шкідливим ПЗ	Порушник	К, Д	Р1 (-1)
18	Переривання	Порушення пропускної здатності каналів зв’язку, обсягів вільної оперативної пам’яті, дискового простору, електроживлення ІКС	Порушник, працівник, технічні засоби	Д	Р2 (-1)
19	Помилки	Помилки під час інсталяції та експлуатації ПЗ, технічних засобів обробки інформації	Технічні засоби	Д	Р4
20	Несанкціоноване перехоплення інформації	Перехоплення інформації за рахунок ПЕМВ від технічних засобів, за рахунок наведень по лініях електроживлення, за рахунок наведень по сторонніх провідниках, акустичним каналом від засобів виведення, під час підключення до каналів передавання інформації	Порушник	К	Р2

Специфікація моделі загроз за рівнем реалізації загроз ІБ компанії:

- Р1 - низький;
- Р2 - нижчий за середній;
- Р3 - середній;
- Р4 - вищий за середній;
- Р5 - високий.

2.17 Висновок зі спеціальної частини

У другому розділі, спираючись на проаналізовану інформацію про діяльність фармацевтичної компанії ТОВ «Еліксир», про середовище користувачів та інформаційне середовище підприємства, було обрано стандартний функціональний профіль захищеності корпоративної ІКС, розроблено модель загроз ІКС ТОВ «Еліксир» і модель порушника ІБ ТОВ «Еліксир». За створеними моделлю загроз і моделлю порушника, були розроблені документи політики інформаційної безпеки ТОВ «Еліксир», спрямовані на підвищення рівня ІБ ТОВ «Еліксир» встановленням єдиних зведень Правил використання особистих ключів і паролів для підключення до вузлів або сегментів корпоративної ІКС, Правил використання та обслуговування серверного обладнання та сховищ даних корпоративної ІКС, Правил використання систем виявлення вторгнень та організації антивірусного захисту, Правил надання та отримання доступу до конфіденційної інформації, що обробляється в корпоративній ІКС ТОВ «Еліксир», Правил роботи відділу системного адміністрування ТОВ «Еліксир».

У спеціальному розділі було доведено необхідність розробки політики інформаційної безпеки ТОВ «Еліксир» з метою вдосконалення процесу забезпечення безпеки на підприємстві, що виробляє стратегічно важливу фармацевтичну продукцію.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Розробка політики інформаційної безпеки підприємства фармацевтичної галузі ТОВ «Еліксир» є необхідною умовою для забезпечення стабільної роботи компанії, для скорочення загроз ІБ корпоративної ІКС.

Розробка ПІБ є економічно доцільною, тому що річний обіг грошових коштів на підприємства складає 22,5 млн грн, відповідно, місячний обіг коштів дорівнює 1875 тис. грн. Усі витрати на розробку та впровадження ПІБ значно менші за розмір можливих фінансових втрат підприємства у разі порушення ІБ.

3.1 Розрахунок капітальних (фіксованих) витрат

3.1.1 Визначення трудомісткості розробки корпоративної ПІБ

Трудомісткістю розробки ПІБ є тривалість кожної дії, яку необхідно виконати для створення політики безпеки. Трудомісткість визначається за формулою:

$$t=t_{тз}+t_в+t_а+t_{вз}+t_{озб}+t_{овр}+t_д, год., \quad (3.1)$$

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 відновлюваних робіт і забезпечення неперервного функціонування організації;

$t_д$- тривалість документального оформлення політики безпеки.

За формулою (3.1), трудомісткість розробки ПІБ складатиме:

$$t = 24+8+16+24+16+32+32 = 152 \text{ год.}$$

3.1.2 Розрахунок витрат на розробку ПІБ

Витрати на розробку ПІБ $К_{рп}$ вираховуються за формулою:

$$К_{рп}=З_{зп}+З_{мч.}, \quad (3.2)$$

де $З_{зп}$ - витрати на заробітну плату системного адміністратора - спеціаліста з ІБ;

$З_{зп}$ - вартість витрат необхідного для розробки ПІБ машинного часу.

За формулою (3.2), витрати на розробку ПІБ складатимуть:

$$К_{рп} = 25840+957,6 = 26797,6 \text{ грн.}$$

Заробітна плата виконавця робіт вираховується за формулою:

$$З_{зп}=t\cdot З_{іб}, \quad (3.3)$$

де t - загальна тривалість розробки ПІБ;

$З_{іб}$ - середньогодинна заробітна плата системного адміністратора - спеціаліста з інформаційної безпеки з нарахуваннями, грн/год.

За формулою (3.3), заробітна плата виконавця робіт складатиме:

$$З_{зп} = 152\cdot 170 = 25840 \text{ грн.}$$

Вартість машинного часу, необхідного для розробки корпоративної ПІБ визначається за формулою:

$$З_{мч}=t \cdot С_{мч}, \quad (3.4)$$

де t - трудомісткість розробки ПІБ, годин;

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

За формулою (3.4), вартість машинного часу, необхідного для розробки корпоративної ПІБ складатиме:

$$З_{мч} = 152 \cdot 6,3 = 957,6 \text{ грн.}$$

Вартість 1 години машинного часу вираховується за формулою:

$$Смч = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_a}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p}, \quad \text{грн,} \quad (3.5)$$

де Р - встановлена потужність ПК, кВт;

$t_{нал}$ - кількість задіяних робочих станцій при написанні ПІБ;

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

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

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

$Н_{апз}$ - річна норма амортизації на ліцензійне ПЗ, частки одиниці;

$К_{лпз}$ - вартість ліцензійного ПЗ, грн.;

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

За формулою (3.5), вартість 1 години машинного часу складатиме:

$$Смч = 1 \cdot 1 \cdot 4,32 \cdot \frac{8999 \cdot 0,3}{1920} + \frac{2000 \cdot 0,05}{1920} = 6,3 \text{ грн.}$$

Таким чином, капітальні (фіксовані) витрати К на розробку ПІБ можна підсумувати за формулою:

$$К = К_{пр} + К_{лпз} + К_{рп} + К_{аз} + К_{навч} + К_{н}, \quad (3.6)$$

де $К_{пр}$ - вартість розробки проєкту ПІБ і залучення зовнішніх консультантів;

$К_{лпз}$ - вартість закупівлі ліцензійного і додаткового ПЗ;

$К_{рп}$ - вартість розробки ПІБ;

$К_{аз}$ - вартість закупівлі АЗ;

$К_{навч}$ - вартість навчання персоналу;

$К_{н}$ - витрати на встановлення обладнання і налагодження системи ІБ.

Вартість розробки проєкту ПІБ і залучення зовнішніх консультантів $К_{пр}$ вираховується як добуток загальної тривалості розробки проєкту ПІБ (8 годин, тобто 1 робочий день) та середньогодиної заробітної плати системного адміністратора - спеціаліста з інформаційної безпеки з нарахуваннями (170 грн/год):

$$К_{пр} = 8 \cdot 170 = 1360 \text{ грн.}$$

Вартість закупівлі ліцензійного і додаткового ПЗ $К_{лпз}$ дорівнює вартості закупівлі ліцензійної ОС Windows 10 PRO 64-bit для однієї робочої станції системного адміністратора (2000 грн). Вартість закупівлі корпоративної ліцензії на ОС Windows 10 PRO 64-bit наведено у таблиці вартості ліцензійного ПЗ корпоративної ІКС (Таблиця 3.1).

Вартість закупівлі АЗ $К_{аз}$ дорівнює вартості закупівлі однієї робочої станції системного адміністратора (8999 грн). Вартість закупівлі однієї робочої станції наведено в інвентаризаційному списку АЗ ІКС ТОВ «Еліксир» (Таблиця 2.5).

Вартість навчання персоналу $К_{навч}$ становить 500 грн. Стільки коштують 2 академічні години робочого часу системного адміністратора, середньогодинна заробітна плата якого складає 170 грн/год.

Витрати на встановлення обладнання і налагодження системи ІБ $К_н$ обчислюються як добуток необхідного для цього часу системного адміністратора у годинах (24 години, тобто 3 робочих дні) та середньогодиної заробітної плати системного адміністратора - спеціаліста з інформаційної безпеки з нарахуваннями (170 грн/год):

$$К_{пр} = 24 \cdot 170 = 4080 \text{ грн.}$$

За формулою (3.6), капітальні (фіксовані) витрати К на розробку ПІБ складатимуть:

$$К = 1360 + 2000 + 26797,6 + 8999 + 500 + 4080 = 43736,60 \text{ грн.}$$

3.2 Розрахунок річних поточних (експлуатаційних) витрат

Експлуатаційні витрати вираховуються за формулою:

$$С = С_а + С_з + С_е + С_{лпз} \text{ грн.}, \quad (3.7)$$

де $С_а$ - річний фонд амортизаційних відрахувань;

$С_з$ - річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему ІБ;

$С_е$ - вартість електроенергії, що споживається апаратурою системи ІБ протягом року;

$С_{лпз}$ - річні витрати на поновлення ліцензії ПЗ.

Річний фонд амортизаційних відрахувань $С_а$ визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ).

Мінімально допустимий строк корисного використання активів, що належать до груп 4 і 5, а саме: ЕОМ, ПЗ, засоби обробки інформації, вартість яких перевищує 2500 грн, авторські та ліцензійні права на ПЗ, складає 2 роки. Для

визначення річного амортизаційного фонду необхідно скласти 50% вартості ліцензійного ПЗ та 50% вартості АЗ системи ІБ. Таким чином, річний фонд амортизаційних відрахувань $С_а$ вираховуватиметься за формулою:

$$С_а = (К_{аз} + К_{лпз})/2 \quad (3.8)$$

За формулою (3.8), річний фонд амортизаційних відрахувань $С_а$ складатиме:

$$С_а = (8999 + 2000)/2 = 10999/2 = 5499{,}5 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу (ІТП), що обслуговує систему ІБ вираховується за формулою:

$$С_з = З_{осн} + З_{дод}, \quad (3.9)$$

де $З_{осн}$ - основна заробітна плата ІТП на рік, грн./рік;

$З_{дод}$ - додаткова заробітна плата ІТП на рік, грн./рік.

За формулою (3.9), річний фонд заробітної плати ІТП, що обслуговує систему ІБ (на підприємстві, що розглядається - 1 співробітник), складатиме:

$$С_з = 240000 + 24000 = 264000 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системи ІБ протягом року вираховується за формулою:

$$С_е = Р \cdot F_р \cdot Ц_е, \quad (3.10)$$

де Р - встановлена потужність апаратури ІБ, кВт;

$F_р$ - річний фонд робочого часу системи ІБ;

$Ц_е$ - тариф на електроенергію, грн/кВт·годин;

За формулою (3.10), вартість електроенергії, що споживається апаратурою системи ІБ протягом року становитиме:

$$C_e = 7 \cdot 8760 \cdot 4.32 = 264902,4 \text{ грн.}$$

Річний фонд робочого часу системи ІБ визначається виходячи з режиму роботи системи ІБ. У приміщеннях підприємства цілодобово працює система відеонагляду. Враховуючи це, річний фонд робочого часу системи ІБ становитиме:

$$F_p = 24 \cdot 365 = 8760 \text{ годин.}$$

Річні витрати на поновлення ліцензії ПЗ $C_{лпз}$ розраховуються як сума витрат на ліцензію для кожного корпоративного програмного продукту.

Таблиця 3.1 - Вартість ліцензійного ПЗ корпоративної ІКС

Назва	**Вартість ліцензії на 1 рік, грн.**
Windows 10 PRO 64-bit	2000
Windows Server 2016 Essentials	4000
Microsoft Office 2013	400
Microsoft Teams	800
Adobe Photoshop	400
Microsoft SQL Server	400
Дебет Плюс	200

$$C_{лпз} = 2000 + 4000 + 400 + 800 + 400 + 400 + 200 = 8200 \text{ грн.}$$

Таким чином, за формулою (3.7) визначаються річні експлуатаційні (поточні) витрати:

$$C = 5499,5 + 264000 + 264902,4 + 8200 = 542601,90 \text{ грн.}$$

Сума капітальних (фіксованих) витрат на розробку ПІБ і річних експлуатаційних (поточних) витрат на виконання ПІБ $\sum_C$ обчислюється за формулою:

$$\sum_C = K + C, \tag{3.11}$$

де К - капітальні (фіксовані) витрати на розробку ПІБ;

С - річні експлуатаційні (поточні) витрати на виконання ПІБ.

$$\sum_C = 43736,6 + 542601,9 = 586338,50 \text{ грн.}$$

3.3 Визначення річного економічного ефекту від впровадження ПІБ. Оцінка можливого збитку від атаки (злому) на вузол або сегмент корпоративної мережі

Якщо загрози ІБ ТОВ «Еліксир» будуть реалізовані, компанія ризикує втратити капітал на суму 22,5 млн грн - обсяг річних обігових грошових коштів.

Збитки від реалізації загроз ІБ підприємства вираховуються за формулою:

$$U = П_п + П_в + V \text{ грн}, \tag{3.12}$$

де $П_п$ - оплачувані втрати робочого часу та простою 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.

За формулою (3.11), збитки від реалізації загроз ІБ підприємства складатимуть:

$$U = 18181,81 + 54545,43 + 17307,69 = 90034,93 \text{ грн.}$$

Вартість оплати непродуктивної праці співробітників підприємства за час простою внаслідок атаки вираховується за формулою:

$$П_{п} = \frac{\sum З_{с}}{F} \cdot t_{п} \text{ грн,} \quad (3.13)$$

де F - місячний фонд оплати робочого часу (при 40-годинному робочому тижні становить 176 годин).

За формулою (3.12), вартість оплати непродуктивної праці співробітників підприємства за час простою $П_{п}$ складатиме:

$$П_{п} = \frac{400000}{176} \cdot 8 = 18181,81 \text{ грн.}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі складаються з декількох статей витрат і вираховуються за формулою:

$$П_{в} = П_{ви} + П_{пв} + П_{зч} \text{ грн,} \quad (3.14)$$

де $П_{ви}$ - витрати на повторне введення інформації, грн;

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

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

За формулою (3.13), витрати на відновлення працездатності вузла або сегмента корпоративної мережі складатимуть:

$$П_{в} = 18181,81 + 18181,81 + 18181,81 = 54545,43 \text{ грн.}$$

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 $t_{ви}$ за формулою:

$$П_{ви} = \frac{\sum З_с}{F} \cdot t_{ви} \text{ грн}, \quad (3.15)$$

За формулою (3.14), витрати на повторне введення інформації $П_{ви}$ складатимуть:

$$П_{ви} = \frac{400000}{176} \cdot 8 = 18181{,}81 \text{ грн}.$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{вп}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів) за формулою:

$$П_{пв} = \frac{\sum З_о}{F} \cdot t_в \text{ грн}, \quad (3.16)$$

За формулою (3.15), витрати на відновлення вузла або сегмента корпоративної мережі $П_{вп}$ складатимуть:

$$П_{пв} = \frac{400000}{176} \cdot 8 = 18181{,}81 \text{ грн}.$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи з середньогодинного обсягу продажів і сумарного часу атакованого вузла або сегмента корпоративної мережі за формулою:

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви}) \text{ грн}, \quad (3.17)$$

де $F_г$ - річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить 2080 годин.

За формулою (3.16), втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі складатимуть:

$$V = \frac{1500000}{2080} \cdot 24 = 17307{,}69 \text{ грн.}$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі складе:

$$В = \sum_i \cdot \sum_n \cdot U, \text{ грн}, \quad (3.18)$$

де $\sum_i$ - кількість атакованих вузлів або сегментів корпоративної мережі;

$\sum_n$ - середня кількість атак на рік.

За формулою (3.17), загальний збиток від атаки на вузол або сегмент корпоративної мережі В дорівнюватиме:

$$В = 1 \cdot 12 \cdot 90034{,}93 = 1080419{,}16 \text{ грн.}$$

Загальний ефект від впровадження системи ІБ визначається з урахуванням ризиків порушення ІБ компанії за формулою:

$$Е = В \cdot R - С \text{ тис. грн}, \quad (3.19)$$

де В - загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R - очікувана ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

С - щорічні витрати на експлуатацію системи ІБ.

За формулою (3.18), загальний ефект від впровадження системи ІБ становитиме:

$$E = 1080,42 \cdot 0,15 - 0,54 = 161,523 \text{ тис. грн.}$$

3.4 Визначення та аналіз показників економічної ефективності системи ІБ

Економічну ефективність системи захисту інформації оцінюють на основі визначення та аналізу наступних показників:

- сукупна вартість володіння (ТСО);
- коефіцієнт повернення інвестицій (ROI). В галузі ІБ цьому коефіцієнту відповідає показник ROSI (Return of Investment for Security);
- термін окупності капітальних інвестицій T_o.

Показник сукупної вартості володіння (ТСО) використовується, якщо величину відверненого збитку від атаки на вузол або сегмент корпоративної мережі важко або неможливо визначити у вартісній формі.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку (для системи ІБ - запобігання можливих втрат) приносить одна гривня капітальних інвестицій на впровадження системи ІБ.

Коефіцієнт повернення інвестицій ROSI вираховується за формулою:

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \qquad (3.20)$$

де Е - загальний ефект від впровадження системи ІБ;

К - капітальні інвестиції за варіантами, що забезпечили цей ефект.

За формулою (3.19), коефіцієнт повернення інвестицій ROSI дорівнюватиме:

$$ROSI = \frac{161523}{43736,6} = 3,69.$$

Отримане значення коефіцієнта повернення інвестицій ROSI = 3,69 означає, що кожна гривня, що витрачена на розробку ПІБ ТОВ «Еліксир» принесе підприємству 3,69 грн. прибутку. Це означає, що розробка ПІБ для ТОВ «Еліксир» є економічно доцільною.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи ІБ і визначається за формулою:

$$T_o = \frac{К}{Е} = \frac{1}{ROSI}, \quad (3.21)$$

За формулою (3.20), термін окупності капітальних інвестицій T_o дорівнюватиме:

$$T_o = \frac{43736,6}{161523} = 0,27.$$

Отримане значення терміну окупності капітальних інвестицій T_o показує, що капітальні інвестиції окупляться за термін 99 днів.

3.5 Висновок з економічного розділу

У третьому розділі було визначено: обсяг капітальних (фіксованих) витрат на розробку (К = 43736,60 грн.) та річних експлуатаційних витрат на підтримку виконання ПІБ підприємства ($\sum_C$ = 586338,50 грн.), можливу величину збитку від атаки (зламу) на вузол або сегмент корпоративної ІКС (U = 90034,93 грн.),

загальний ефект від впровадження системи ІБ (Е = 161,523 тис. грн.), показники економічної ефективності впровадження ПІБ та проаналізовано їх (коефіцієнт повернення інвестицій ROSI = 3,69), термін окупності капітальних інвестицій у розробку та впровадження ПІБ (99 днів).

За результатами аналізу фінансових витрат було доведено, що впровадження політики інформаційної безпеки у робочий процес підприємства є економічно доцільним.

ВИСНОВКИ

Інформаційна безпека робочого процесу будь-якої компанії, як стан захищеності інформації, що обробляється на підприємстві, є необхідною умовою для її стабільного функціонування. Забезпечення інформаційної безпеки є особливо важливою діяльністю для підприємств, які виробляють стратегічно важливу продукцію. Продукція підприємства фармацевтичної галузі ТОВ «Еліксир» є стратегічно важливою для населення, тому що від якості випущеної продукції може залежати стан здоров'я громадян.

В інформаційно-комунікаційній системі ТОВ «Еліксир» обробляється інформація з обмеженим доступом. За Законом, ІзОД захищається в обов'язковому порядку, а вимоги до організації організаційного та технічного захисту ІзОД встановлюються Законами України та нормативними документами технічного захисту інформації.

Для систематизації організації роботи із підтримки інформаційної безпеки на підприємстві фармацевтичної галузі необхідно впровадити політику інформаційної безпеки - сукупність загальних принципів та правил, якими керується об'єкт інформаційної діяльності.

У ході виконання кваліфікаційної роботи бакалавра було обґрунтовано необхідність впровадження політики інформаційної безпеки у робочий процес підприємства фармацевтичної галузі ТОВ «Еліксир», проведено обстеження середовища користувачів та інформаційного середовища приватної фармацевтичної компанії, розроблено модель загроз ІКС ТОВ «Еліксир» і модель порушника ІБ ТОВ «Еліксир», розроблено зміст документів політики інформаційної безпеки. Було доведено економічну доцільність розробки та впровадження корпоративної політики інформаційної безпеки ТОВ «Еліксир».

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про інформацію», Відомості Верховної Ради України (ВВР), 1992, № 48, ст. 650.

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р.

3. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 р.

4. Закон України «Про захист персональних даних» від 01.06.2010 р.

5. Закон України «Про державну таємницю» від 21.01.1994 р.

6. Постанова Кабінету Міністрів України «Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19.06.2019 р.

7. Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» від 29.03.2006 р.

8. Постанова КМУ № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» від 23 грудня 2020 р.

9. НД ТЗІ 1.1-003-99 Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

10. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

11. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

12. ДСТУ ISO/IEC 27000:2022 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник.

13. ДСТУ ISO/IEC 27005:2015 Інформаційні технології Методи захисту. Управління ризиками інформаційної безпеки.

14. Матвієнко О. В. , Цивін М. Н. Основи менеджменту інформаційних систем: Навч.посібник.-К.:Центр навчальної літератури, 2005.- 176 с.

15. Компьютерные сети : Нисходящий подход / Джеймс Куроуз, Кит Росс. - 6-е изд. - Москва : Издательство "Э", 2016. - 912 с. - (Мировой компьютерный бестселлер).

16. Енциклопедія сучасної України / ред. кол.: І. М. Дзюба [та ін.] ; НАН України, НТШ. — К. : Інститут енциклопедичних досліджень НАН України, 2011. — Т. 11 : Зор — Как. — 710 с. — ISBN 978-966-02-6092-4.

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

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	1 Розділ	9	
6	А4	2 Розділ	45	
7	А4	3 Розділ	14	
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	1	

ДОДАТОК Б. Перелік документів на оптичному носії

Пояснювальна записка КРБ Бойчук.docx

Презентація КРБ Бойчук.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу

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

Керівник розділу _____ доц. Пілова Д. П.

(підпис) (ім'я, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Розробка політики безпеки підприємства
фармацевтичної галузі ТОВ «Еліксир»
студента групи 125-20-2
Бойчука Миколи Олексійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 81 сторінці та містить 3 рисунки, 13 таблиць, 17 джерел та 4 додатка.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: проаналізовано теоретичні основи процесу розробки ПІБ корпоративної ІКС, досліджено інформаційне середовище ТОВ «Еліксир», розроблено модель загроз, модель порушника та проведено оцінку ризиків інформації, що можуть призвести до завдання збитків підприємству. Згідно з проведеним аналізом, були розроблені та запропоновані до впровадження елементи політики безпеки захисту інформації ТОВ «Еліксир».

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні рівня захищеності властивостей інформації з обмеженим доступом в інформаційно-комунікаційній системі ТОВ «Еліксир».

До недоліків кваліфікаційної роботи потрібно віднести незначні відхилення від стандартів оформлення. В цілому робота написана грамотною мовою, відповідає вимогам положення про систему запобігання та виявлення плагіату у Національному технічному університеті «Дніпровська політехніка». Містить необхідний ілюстрований матеріал, автор добре знає проблему, уміє формулювати практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а її автор заслуговує на оцінку «90 / відмінно».

Керівник кваліфікаційної роботи проф. Магро В. І.

Керівник спеціального розділу ас. Мілінчук Ю. А.