ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«РОЗРОБКА МОДЕЛІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Вікторії КИЦЮК

Виконав: здобувач(ка) вищої освіти групи БСДМ-62
КИЦЮК Вікторія
(ПРІЗВИЩЕ, Ім'я)

Керівник: ГАЙДУР Галина
д.т.н, професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кицюк Вікторії Максимівні
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Розробка моделі системи інформаційної безпеки на підприємстві»
керівник кваліфікаційної роботи: ГАЙДУР Галина, д.т.н., професор,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
інформаційна система організації;
Нормативно-правова основа захисту інформації на підприємстві ;
наукова та технічна література, експлуатаційна документація, нормативні методи захисту інформаційних ресурсів.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Теоретичні аспекти розробки моделі системи інформаційної безпеки на підприємстві
2. Аналіз роботи тов «перша українська газонафтова компанія» та виявлення загроз в її системі інформаційніої безпеки

3. Розробка моделі системи інформаційної безпеки на підприємстві

5. Перелік ілюстративного матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми управління систем інформаційної безпеки на підприємстві	19.10.2023 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	22.10.2023 р.	
3.	Аналіз роботи та виявлення загроз в її системі інформаційніої безпеки підприємства	27.10. 2023р.	
4.	Методи захисту інформаційних ресурсів	03.11.2023 р.	
5.	Розробка моделі системи інформаційної безпеки на підприємстві	15.11.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	26.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач(ка) вищої освіти _____ Вікторія КИЦЮК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Кицюк В.М. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Розробка моделі системи інформаційної безпеки на підприємстві».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач ***КИЦЮК Вікторія*** обрав тему роботи, метою якої було дослідити зміст технології контролю доступу до мережі організацій. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***КИЦЮК Вікторія*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***КИЦЮК Вікторія*** на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач(ка) ***КИЦЮК Вікторія .*** допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Кицюк Вікторія
на тему: «Розробка моделі системи інформаційної безпеки на підприємстві».

Актуальність:

Забезпечення безпеки інформації в Україні є одним з ключових факторів, що визначає здатність держави захистити свою територіальну цілісність та суверенітет. Інформаційна безпека має прямий вплив на політичний, економічний, оборонний стан України та інші складові національної безпеки, оскільки загрози цій сфері можуть призвести до значних наслідків для країни в цілому - у політичній, економічній, соціальній, екологічній, військовій тощо.

Позитивні сторони:

1. Оцінили стан забезпечення захисту інформаційних процесів на підприємстві.
2. Розроблена модель системи інформаційної безпеки на підприємстві.
3. Запропоновано модель системи інформаційної безпеки на підприємстві АС «Мотив».
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У кваліфікаційній роботі доцільно було б більш детально описати різні групи проблем що виникають при організації захисту в захищених АС.
2. Запропоновано нове вирішення наукового завдання щодо забезпечення інформаційної безпеки підприємства що сприятиме підвищенню ефективності захисту інформації та інформаційного продукту.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре»**, а здобувач **КИЦЮК Вікторія** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент:		Віктор ВИШНІВСЬКИЙ
д.т.н., професор	*підпис*	*Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи и на здобуття освітнього ступеня магістра: 76 сторінок, 6 рисунків, 2 таблиці, 42 джерел.

Об'єкт дослідження – є процес управління забезпеченням захисту інформаційних процесів на підприємстві.

Предмет дослідження – є теоретичні засади та прикладні аспекти проблеми захисту інформаційних процесів на підприємстві.

Мета роботи – розроблення даного проекту передбачає всебічний аналіз стану забезпечення ефективності системи інформаційної безпеки підприємства ТОВ «Перша українська газонафтова компанія», а також розробку пропозицій на формування управління забезпечення ефективності системи інформаційної безпеки та вироблення на їх основі рекомендацій, спрямованих на удосконалення захисту інформації на підприємстві.

Методи дослідження – що лежать в основі даного проекту, охоплюють широкий спектр сучасних філософських, загальнонаукових та спеціальних методів пізнання державно-правових процесів та явищ.

У даному проекті на базі загальнонаукових та спеціальних методів проводилось порівняння (у підпункті 1.2 при характеристиці загроз інформаційній безпеці), узагальнення (у підпункті 2.3 при обґрунтуванні оцінки інформаційної безпеки у місцевому органі державного управління), застосовувалися метод класифікації (у підпункті 3.1 для систематизації методів захисту інформації), аналізу та синтезу (у підпункті 2.2 при формуванні цілей і задач системи інформаційного безпеки органу державного управління) та інші загальноприйняті методи. В результаті було виділено наукову новизну, яка полягає в удосконаленні підходу до раціональної організації ефективності системи інформаційної безпеки підприємства, ТОВ «Перша українська газонафтова компанія».

Галузь використання – системи інформаційної безпеки на підприємстві.

СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ, СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, БАЗА ДАНИХ, МЕТОДИ ТА ЗАСОБИ, ГРИФ,

ABSTRACT

Text part of the master's qualification work:76 pages, 6 figures, 2 tables, 42 sources.

Object of research - it is the process of management of information processes security at the enterprise.

The purpose of the work is to develop this project, which involves a comprehensive analysis of the state of ensuring the effectiveness of the information security system of PrJSC "First Ukrainian Gas and Oil Company", as well as the development of proposals for the formation of management to ensure the efficiency of the information security system and the development of recommendations based on them aimed at improving information protection at the enterprise.

Research methods - which are the basis of this project, cover a wide range of modern philosophical, interdisciplinary and special methods of cognition of state-legal processes and phenomena.

In this project, comparison (in paragraph 1.2 when describing threats to information security), generalization (in paragraph 2.3 when justifying the assessment of information security in a local body of state administration), classification method was used (in paragraph 3.1 to systematize methods of information protection), analysis and synthesis method (in paragraph 2.2 when forming goals and tasks of an information security system of a state management body) and other generally accepted methods. As a result, scientific novelty was identified, which consists in improving the approach to rational organization of the information security system of PrJSC "First Ukrainian Gas and Oil Company".

Field of use - information security systems in the enterprise.

INFORMATION SECURITY SYSTEMS AT THE ENTERPRISE, INFORMATION PROTECTION SYSTEM, DATABASE, METHODS AND MEANS, CLASSIFIED DOCUMENTS

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – Програмне забезпечення;

НБ – Національна безпека

САД – Система автоматизації діловодства та документообігу

СЗІ – Система захисту інформації

СЗІБ – Система забезпечення інформаційної безпеки

СУІБ – Система управління інформаційною безпекою

ІС – Інформаційна система

ЗУ – Закон України

ЗМІ – Засоби масової інформації

ІТ – Інформаційні технології

ЗОТ – Засоби обчислювальної техніки

ЗІ – Захист інформації

ІАС – Інформаційно-аналітична система

БД – База даних

ТЗІ – Технічний захист інформації

ПЕОМ – Персональна електроно-обчислювальна машина.

ВСТУП

Актуальність дослідження. актуальність дослідження проблеми інформаційної безпеки визначається необхідністю забезпечення інформаційної безпеки держави в умовах сучасного інформаційного середовища та розвитку інформаційного суспільства. Здійснення реформ, пов'язаних з європейською інтеграцією, а також забезпечення сталого розвитку країни потребують ефективного управління усіма видами інформаційних ресурсів та елементами інформаційно-телекомунікаційної інфраструктури. Також, державна підтримка вітчизняного інформаційного виробництва, ринку інформаційних технологій, засобів, продуктів і послуг є чинником успіху розвитку держави в цілому.

Однак, розвиток інформаційних технологій призводить до появи нових форм загроз інформаційній безпеці. Тому необхідно проводити наукові дослідження, спрямовані на виявлення та аналіз таких загроз, розробку методів та засобів захисту інформації.

Забезпечення інформаційної безпеки - невід'ємна складова національної безпеки, оскільки загрози в цій сфері можуть мати серйозний вплив на всі складові національної безпеки України. Наприклад, кібератаки на системи енергетичного забезпечення, міжнародного фінансового сектору чи соціальних мереж можуть мати негативний вплив на стан економіки та фінансової стабільності країни.

У зв'язку з ринковим характером господарювання, комплексна інформаційна безпека є одним із провідних факторів успішного функціонування підприємств. Інформаційна безпека захищає від крадіжок комерційної та конфіденційної інформації, а також від порушень прав на інтелектуальну власність.

Тому для забезпечення інформаційної безпеки необхідний комплексний підхід до проблеми, що передбачає розробку та впровадження відповідної

стратегії, яка охоплювала б усі аспекти захисту інформації від втручань, викрадень та інших загроз. Також необхідно проводити наукові дослідження, спрямовані на моделювання та аналіз загроз інформаційній безпеці, що дозволить вчасно підготуватися до запобігання можливих негативних наслідків.

Об'єкт дослідження – є процес управління забезпеченням захисту інформаційних процесів на підприємстві.

Предмет дослідження – є теоретичні засади та прикладні аспекти проблеми захисту інформаційних процесів на підприємстві.*Мета роботи* – що лежать в основі даного проекту, охоплюють широкий спектр сучасних філософських, загальнонаукових та спеціальних методів пізнання державно-правових процесів та явищ.

Наукові завдання:

- дослідити поняття та зміст інформаційної безпеки, що дає можливість зрозуміти реальну ситуацію з інформаційною безпекою на підприємствах;
- розглянути характеристику загроз інформаційній безпеці підприємства;
- дослідити нормативно-правові аспекти захисту інформації на підприємстві; дослідити засоби забезпечення захисту інформації в автоматизованих інформаційних системах.

Методи дослідження – для дослідження державно-правових процесів та явищ застосовують різні методи, такі як описовий аналіз, порівняльний аналіз, статистичний аналіз, аналіз проблемного поля, логіко-смисловий аналіз тощо. Використання цих методів дозволяє отримати необхідну інформацію про об'єкти дослідження, їх властивості та особливості.

Практичне значення одержаних результатів. Одним з важливих аспектів науково-дослідної роботи є практичне застосування результатів дослідження. У даному випадку, розробка рекомендацій щодо вдосконалення управління системою інформаційної безпеки ТОВ "Перша українська газонфтова компанія"

дозволить покращити ефективність функціонування системи та забезпечити захист інформації від можливих загроз.

Апробація результатів. Результати дослідження, що стосуються організації діловодства в видавництві, були опубліковані в науковій статті "Управління забезпечення ефективності системи інформаційної безпеки підприємства" авторства І.А. Пухая та Л.М. Колєчкіної. Матеріали статті були включені до збірника наукових статей магістрів, який видав Інститут економіки, управління та інформаційних технологій.

1 ТЕОРЕТИЧНІ АСПЕКТИ РОЗРОБКИ МОДЕЛІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

1.1. Поняття та ознаки інформаційної безпеки

Сьогодні важко знайти свіжі або повністю точні дані щодо статистики кібербезпеки, єдиний надійний звіт датується 2003 роком. Дослідження школи Кларка при Університеті Меріленда, проведене в 2003 році, є одним із перших, в якому кількісно оцінюється майже постійний рівень атак хакерів. Дослідження показало, що кожен день відбувалося 2,244 напади, розпадається майже не одна кібератака кожні 39 секунд, і «груба сила» була найпоширенішою тактикою. За даними австралійського урядового агентства Австралійського центру кібербезпеки (ACSC), встановлено, що з липня 2019 по червень 2020 надійшло 59,806 XNUMX повідомлень про кіберзлочини (зареєстрованих злочинів, а не зламів), що в середньому становило 164 кіберзлочини на день або приблизно кожні 10 хвилин [1].

В умовах сьогодення статистика кібербезпеки змінюється щохвилини, кіберзагрози стають все більш небезпечними, більш складними та важкими для виявлення

За останній час зросла кількість атак шкідливих програм, які стали набирати оберти після їх спаду в 2018 році. За даними SonicWall, у 2023 році кількість таких атак склала 5,5 мільярда, що на 2% більше, ніж у попередньому році. Це значне зростання пояснюється інтенсивністю криптоджекінгу та шкідливого програмного забезпечення для Інтернету речей (IoT). Дослідження також показують, що людський фактор є причиною приблизно 88% всіх витоків даних. Особливо це стосується працівників, які працюють дистанційно. [1].

Враховуючи важливість інформаційної безпеки у діяльності підприємств, проведемо дослідження щодо сутності цієї дефініції. Вченими доведено, що трактування поняття «інформаційна безпека» на рівні підприємства досить неоднозначне. Це свідчить про те, що немає єдиного підходу до її визначення, оскільки сутність даної категорії залежить від багатьох обставин, якими характеризується інформаційна система підприємства Найбільш поширені визначення поняття «інформаційна безпека» представлені у таблиці. 1.1.

Таблиця 1.1

Зміст поняття «інформаційна безпека підприємства»

Автори	Визначення
Закон України «Про телекомунікації»	здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації [2]
Якименко Ю.М., Савченко В.А., Легомінова С.В.	стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держав [3]
Козачок В.А., Гайдур Г.І., Гахов С.О.	події, які шляхом потенційно можливого впливу на інформаційну систему прямо та/або опосередковано завдають збитку її власникам і користувачам [4]
Шульга В. І.	стан інформаційної системи, у якому вона може протистояти впливу внутрішніх і зовнішніх ризиків, не ініціюючи їхнє виникнення для елементів системи й зовнішнього середовища [5]
Забродський В.А.	кількісну і якісну характеристику властивостей фірми, що відбиває здатність «самовиживання» і розвитку в умовах виникнення зовнішньої і внутрішньої економічної загрози [6, с.35]
Камлика М.І.	це такий стан розвитку суб'єкта господарювання, який характеризується стабільністю економічного та фінансового розвитку, ефективністю нейтралізації негативних факторів і протидії їх впливу на всіх стадіях його діяльності [7, с. 9].
Гладченко Т.Н.	як захищеність життєво важливих інтересів підприємства від внутрішніх і зовнішніх загроз, організація якої здійснюється адміністрацією й колективом підприємства шляхом реалізації системи заходів правового, економічного, організаційного, інженерно-технічного й соціально-психологічного характеру[8, с.111-113]

Продовження табл. 1.1

Ніколаюк С.І., Никифорчук Д.Й.	як стан юридичних, виробничих відносин і організаційних зв'язків, матеріальних і інтелектуальних ресурсів, щодо яких гарантується стабільність функціонування, фінансово-комерційний успіх, прогресивний науково-технічний і соціальний розвиток [9, с. 15].
Могильний А.І., Безчастний В.М., Винокуров Ю.О.	забезпеченні стану життєдіяльності, при якому реалізуються його основні інтереси, воно захищено від внутрішніх та зовнішніх загроз і дестабілізуючих чинників [10, с.9].

Теоретичний аналіз доводить, що сутність поняття «інформаційна безпека» є неоднорідною та багатогранною в її трактуванні. На погляд авторів, «інформаційна безпека» - це стан інформаційного середовища господарюючого суб'єкта, при якому зберігаються властивості інформації й інформаційних потоків, та створюються умови протистояння впливу внутрішніх і зовнішніх загроз з метою досягнення бізнес-цілей підприємства.

У випадку із зовнішніми атаками здійснюється пошук вразливості в інформаційній структурі для доступу до основних вузлів, сховищ, персональних комп'ютерів співробітників, організаційної мережі тощо. Його використовують для завдання шкоди об'єктам копіювання, видозміни, шпигунства, відключення систем захисту, знищення тощо. До зовнішніх загроз відносять: шкідливе програмне забезпечення; спам; промислове шпигунство; мережеві вторгнення; крадіжка мобільних пристроїв та великого обладнання; таргетовані (цільові) атаки; злочинне шкідництво тощо.

До внутрішніх загроз можна віднести дії або бездіяльність співробітників, які свідомо чи несвідомо протидіють інтересам підприємства. Це може призвести до нанесення економічних збитків компанії, втрати інформаційних ресурсів, підриву ділового іміджу та створення проблем у відносинах з партнерами. Серед внутрішніх загроз можна виділити такі як: вразливість програмного забезпечення; випадкові витоки з вини співробітників; наміри викрадення інформації через співробітників; витік або неналежний обмін інформацією через мобільні пристрої; втрата мобільних пристроїв працівниками; шахрайство

співробітників. Важливо забезпечувати надійний захист від цих загроз, а також проводити постійний моніторинг інформаційної системи підприємства.

Класифікація загроз інформаційної безпеки за основними ознаками представлено на **рис 1.1**.

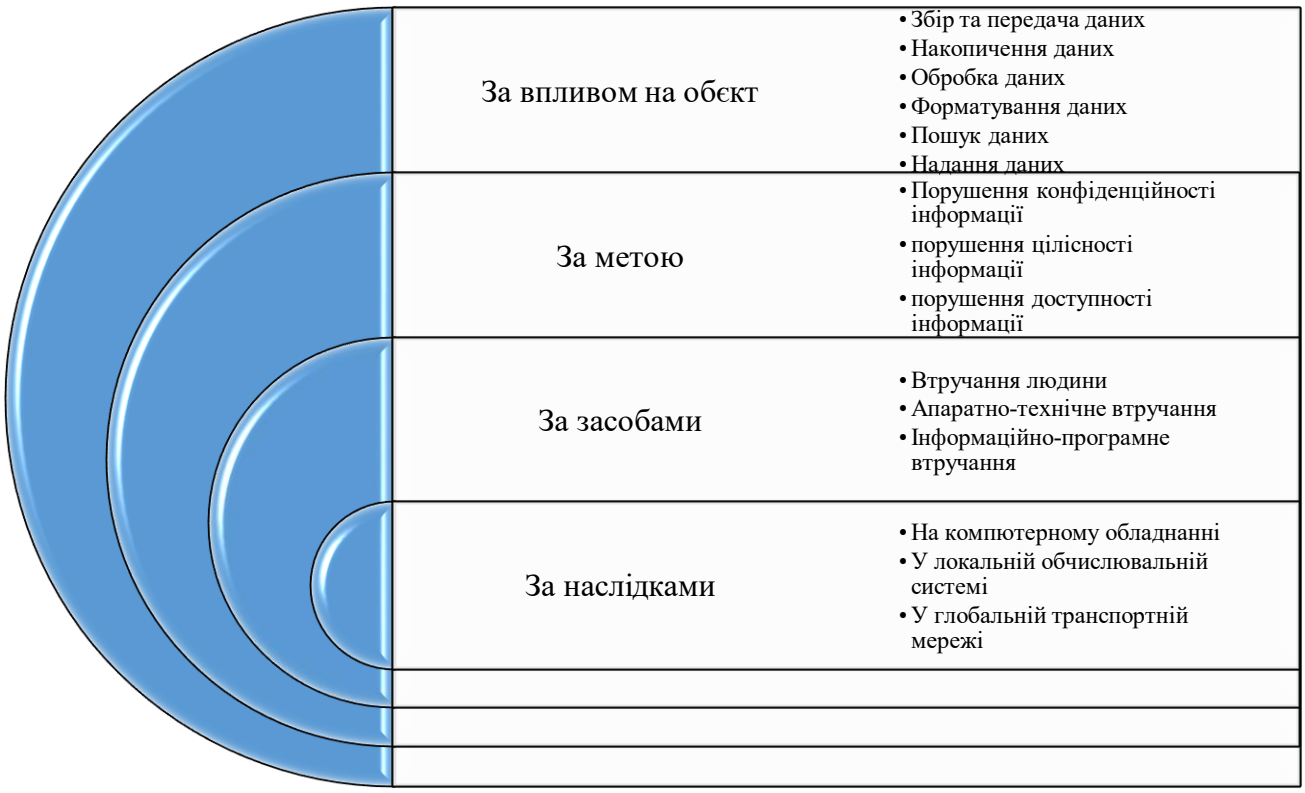

Рис. 1.1. Класифікація загроз інформаційної безпеки
Побудовано за джерелом [4]

Порушення інформаційної безпеки за результатами впливає на загрози, зокрема:

– даним підприємства в системі управління ним: втрата даних; викривлення даних; відмова у даних; порушення конфіденційності; крадіжка даних; атаки; хибні ідентифікації;

– обладнанню підприємства: відмови; вихід з ладу; завади; перегрів; електромагнітні наведення; волога.

Інформаційна безпека на будь-якому рівні управління формується на основі фундаментальних принципів, які є вихідними положеннями, нормами і правилами поведінки, які диктують усім суб'єктам господарювання (рис. 1.2).

Рис. 1.2. Принципи забезпечення інформаційної безпеки

Побудовано за джерелом [11] Олійник О.В. Принципи забезпечення інформаційної безпеки України. Науковий вісник Ужгородського університету. 2012. Випуск 18. С.170-173

Принцип законності в контексті захисту інформаційної безпеки передбачає використання механізмів, що гарантують дотримання підприємствами правових норм та забезпечення відповідності чинного законодавства України в цій сфері. Також підприємствам важливо дотримуватися пріоритету міжнародних норм та

принципів, які стосуються захисту інформації, що може включати укладення міжнародних договорів та співпрацю з іноземними державами.

Принцип права власності в контексті захисту інформаційної безпеки передбачає забезпечення прав суб’єктів на інформацію, яка створена ними або належить їм на законних підставах. Важливо, щоб обмеження прав на таку інформацію були встановлені тільки чинним законодавством та не перевищували необхідних меж для забезпечення інформаційної безпеки підприємства. Один з аспектів проблеми захисту прав власності на об’єкти промислової власності полягає у зіткненні інтересів між створювачем такого об’єкту та суспільством в цілому, яке може мати претензії на певну частину вартості цього об’єкту. Необхідно знайти баланс між цими інтересами та гарантувати забезпечення прав власника на його об'єкт інтелектуальної власності. Другий аспект пов'язаний з умовами застосування патенту - обмеженої строком монополії на певне технічне рішення. При цьому важливо встановлювати чіткі підстави для видання патенту та не допускати зловживання монопольним становищем. Дотримання цих принципів дозволить запобігти обмеженням конкуренції та забезпечити ефективне функціонування антимонопольного законодавства.

Принцип економічної доцільності в системі забезпечення інформаційної безпеки передбачає оцінювання секретності та конфіденційності як ключових параметрів продукту та їх включення до загальної ціни продукту на підставі законодавства. Даний принцип передбачає необхідність всебічного аналізу можливої економічної шкоди для суб'єкта господарювання та врахування усіх негативних наслідків, пов'язаних з порушенням захисту інформації. Цей принцип має прямий вплив на фінансову діяльність підприємств, оскільки розмір економічної шкоди, пов'язаної з можливим порушенням захисту інформації, може бути значним. Це допомагає зменшити ризики, пов'язані з можливими порушеннями захисту інформації, та забезпечити стабільність фінансової діяльності підприємства.

Принцип комплексного підходу до організації забезпечення інформаційної безпеки передбачає створення взаємозв'язаної системи заходів, розроблених для забезпечення безпеки інформації на підприємстві. Цей принцип передбачає використання сил, засобів та методів, спрямованих на забезпечення захисту інформації підприємства, які повинні бути взаємодіючими та взаємозалежними.

Комплексний підхід у системі забезпечення інформаційної безпеки дозволяє створити єдину цілісну систему, яка включає у себе заходи з організації фізичної та технічної безпеки інформації, захисту від електронних атак, контролю доступу, а також забезпечення безпеки персоналу та кадрових рішень. Врахування принципу комплексного підходу до забезпечення інформаційної безпеки дозволяє підприємствам забезпечити єдність в рішеннях, пов'язаних з виробничою, комерційною та фінансовою діяльністю підприємства. Цей підхід допомагає забезпечити спільність підходів до забезпечення інформаційної безпеки та координацію роботи всіх підрозділів підприємства. Крім того, комплексний підхід сприятиме зменшенню можливих помилок, що виникають при взаємодії окремих елементів системи захисту інформації. В результаті, це створить умови до надійності та ефективності системи забезпечення інформаційної безпеки на підприємстві.

Принцип безперервності забезпечення інформаційної безпеки передбачає використання загальних та спеціальних засобів та методів для забезпечення безперебійного захисту інформації на всіх етапах її життєвого циклу. Врахування даного принципу у системі забезпечення інформаційної безпеки підприємства передбачає регулярне застосування активних, превентивних, ефективних та різноманітних заходів і спеціальних методів для забезпечення безпеки інформації.

Безперервність забезпечення інформаційної безпеки допоможе забезпечити безпеку інформації та її обігу в будь-який час та в будь-яких умовах. Цей принцип передбачає регулярне проведення аудитів та тестувань системи

забезпечення інформаційної безпеки з метою виявлення потенційних проблем та вдосконалення системи захисту. Врахування принципу безперервності забезпечення інформаційної безпеки дозволяє забезпечити надійний та стійкий захист інформації та зменшити ризики порушення її конфіденційності, цілісності та доступності. Цей принцип дозволяє підприємствам забезпечувати безпеку інформації в будь-який час та в будь-яких умовах, що сприяє забезпеченню континуїтету бізнесу та стійкості діяльності підприємства.

Принцип єдиноначальності передбачає, що відповідальність за забезпечення інформаційної безпеки покладається на керівників підприємств, які здійснюють діяльність, що пов'язана з захистом конфіденційної інформації. Даний принцип передбачає, що кожен суб’єкт господарювання несе відповідальність за забезпечення безпеки своєї інформації та покладає обов’язки інших суб’єктів у сфері захисту своєї інформації. Керівники організацій, де зберігається конфіденційна інформація, зобов'язані забезпечувати високий рівень захисту даних та приймати необхідні заходи для запобігання можливих загроз. Принцип єдиноначальності передбачає активну взаємодію між різними суб'єктами господарювання з метою обміну досвідом та координації дій. Це сприяє забезпеченню високого рівня захисту інформації в рамках всієї системи, а також зменшенню ризиків порушення конфіденційності, цілісності та доступності інформації.

1.2. Нормативно-правова основа захисту інформації на підприємстві

Українське законодавство регулює питання правового статусу підприємств в країні. Початковим етапом розвитку був Закон України "Про підприємства в Україні", який було прийнято в 1991 році, після здобуття державної незалежності.

Багато положень цього закону було враховано при розробці Господарського кодексу України, який набрав чинності з 2004 року. Згідно із законодавством, підприємства є самостійними юридичними особами, з правом володіння майном, здійснення підприємницької діяльності та участі у господарських відносинах. Крім того, підприємства мають обов'язок виконувати вимоги законодавства, забезпечувати охорону праці, дотримуватися правил конкуренції та регулювання цін. Важливо мати на увазі всі аспекти правового статусу підприємств для успішної діяльності в Україні.

Таким чином, підприємство є сукупністю нерухомих і рухомих речей, майнових та інших прав, що використовуються для здійснення підприємницької діяльності. Установчий документ підприємства та правовий режим майна визначається власниками майна або їх представниками. Крім того, підприємство має право вирішувати питання призначення керівника, реорганізації та ліквідації. Оскільки підприємство є самостійним суб'єктом господарювання, то воно має право на участь у всіх правовідносинах, пов'язаних зі здійсненням підприємницької діяльності.

Згідно з Цивільним кодексом України, підприємство є єдиним майновим комплексом, що використовується для здійснення підприємницької діяльності. Воно може бути об'єктом купівлі-продажу, застави, оренди та інших правочинів. Але Господарський кодекс (статті 62-72) визначає підприємство як самостійний суб'єкт господарювання, який безпосередньо бере участь у виробничій, науково-дослідницькій та комерційній діяльності, може функціонувати на будь-якій формі власності та має установчий документ.

Управління певними аспектами функціонування підприємства може бути здійснене лише за згодою власника майна, який має право на прийняття рішень щодо створення філій, представництв, випуску облігацій та інших фінансових операцій. Однак, деякі аспекти пов'язані з безпосереднім функціонуванням підприємства, такі як формування виробничої програми, наймання та звільнення

працівників, організація виробничого процесу, взаємовідносини з партнерами тощо, можуть бути вирішені самостійно керівництвом підприємства. Важливо мати на увазі, що управління підприємством повинно відбуватися в межах законодавства та з урахуванням інтересів всіх зацікавлених сторін, зокрема працівників, партнерів та споживачів продукції чи послуг.

Якщо підприємство має право господарського відання або користування виділеним майном, то воно має додаткові обов'язки, зокрема повинне виконувати вказівки власника або отримувати його згоду на питання діяльності у випадках, передбачених законом та статутом підприємства. Окрім цього, підприємство зобов'язане відраховувати визначену власником частину чистого прибутку, а також використовувати закріплене за ним майно лише в межах, встановлених законодавством та статутом підприємства.

Отже, визначення правового титулу майна та встановлення відповідних обов'язків для підприємства є важливими елементами управління підприємством в Україні. Дотримання встановлених вимог законодавства та статуту підприємства, а також співпраця з власником майна є необхідними умовами успішної діяльності підприємства.

Згідно з частиною 1 статті 55 Господарського кодексу України, суб'єктами господарювання вважаються учасники господарських відносин, які займаються підприємницькою діяльністю, мають окреме майно та несуть відповідальність за свої зобов'язання в межах цього майна. Однак, існують випадки, коли законодавством передбачено інші умови, що можуть бути визнані винятками. Наприклад, у певних сферах діяльності, таких як банківська діяльність або страхування, для отримання ліцензії на здійснення відповідної діяльності потрібні додаткові умови та вимоги. Важливо мати на увазі всі вимоги законодавства, які стосуються діяльності конкретного суб'єкта господарювання, та дотримуватися їх для успішного функціонування підприємства.

Стаття 56 Господарського кодексу України встановлює загальні принципи створення суб'єкта господарювання, зокрема, правові підстави для його формування та необхідність дотримання вимог чинного законодавства. Відповідно до цієї статті, суб'єкт господарювання може створюватися на основі різноманітних форм власності, включаючи державну, комунальну, приватну, кооперативну тощо. Крім того, створення суб'єкта господарювання повинно відповідати вимогам законодавства та належним чином зареєструватися у відповідних органах влади.

Таким чином, належне створення суб'єкта господарювання є необхідною умовою для успішної діяльності в господарському секторі України. Дотримання вимог законодавства та виконання усіх необхідних процедур є важливим елементом у процесі створення суб'єкта господарювання та забезпечення його правильної роботи.

Згідно з Господарським кодексом України, суб'єкт господарювання створюється та функціонує на підставі установчих документів, які повинні відповідати вимогам законодавства. Загальні вимоги до установчих документів визначені статтею 57 Господарського кодексу України, але для суб'єктів господарювання з особливим видом діяльності встановлюються спеціальні вимоги.

Наприклад, закон "Про банки і банківську діяльність" визначає вимоги до установчих документів банків щодо структури та мінімального розміру статутного капіталу. Крім того, цей закон встановлює процедуру реєстрації банків перед початком їх діяльності.

Закон "Про цінні папери та фондову біржу" встановлює порядок створення бірж та вимоги до їх статутів та правил торгівлі. Крім того, цей закон містить вимоги до установчих документів емітентів цінних паперів.

Закон "Про державне регулювання ринку цінних паперів в Україні" встановлює вимоги до установчих документів та статутів організаторів ринку цінних паперів та інших учасників ринку.

Отже, створення та функціонування суб'єктів господарювання базується на установчих документах, які повинні відповідати вимогам законодавства. Для окремих видів діяльності встановлюються спеціальні вимоги до установчих документів, які деталізують умови та процедури їх створення та реєстрації.

Українське законодавство містить низку положень, що регулюють питання фінансових послуг та інститутів, які займаються інвестуванням та страхуванням. Наприклад, "Про інститути спільного інвестування (пайові та корпоративні інвестиційні фонди)" (статті 9, 23-24) визначає правила збору та управління коштами інвесторів через спільний фонд, а також встановлює порядок проведення операцій з цими коштами. "Про страхування" (статті 2, 20, 31) містить правила реалізації страхової діяльності, встановлює порядок укладання договору про страхування, а також визначає права та обов'язки страховика та страхувальника. Важливо мати на увазі всі аспекти законодавства, які стосуються інвестування та страхування, для успішної діяльності в цих сферах та забезпечення прав та інтересів всіх сторін, що беруть участь у фінансових операціях.

Загальні вимоги щодо установчих документів стосуються:

- українське законодавство передбачає, що установчі документи є необхідною складовою процесу створення суб'єкта господарювання в Україні. Зокрема, рішення про утворення приймається при створенні господарської організації унітарного типу, а засновницький договір укладається у випадку заснування суб'єкта господарювання двома і більше особами. Статут є одним з найважливіших установчих документів і приймається у передбачених законом випадках: при створенні підприємства, господарських товариств, які належать до об'єднань капіталів та виробничого кооперативу. В статуті повинні бути

відображені всі права, обов'язки та відповідальність, які випливають з господарської діяльності суб'єкта господарювання. Для філій, представництв та інших відокремлених підрозділів господарських організацій зі статусом юридичної особи використовуються положення. Цей документ містить вимоги до організації та функціонування підрозділу, а також визначає його повноваження та відповідальність. Отже, установчі документи є ключовим елементом при створенні суб'єкта господарювання в Україні. Їх прийняття та належне оформлення є необхідною умовою для успішної діяльності суб'єкта господарювання та сприяє його правильному функціонуванню відповідно до вимог законодавства.

- установчі документи містять ключову інформацію про суб'єкт господарювання: найменування, місцезнаходження, мету та предмет діяльності. Також вказують склад органів управління та їх компетенцію, порядок прийняття рішень, умови формування майна та розподілу прибутків/збитків. Установчі документи також повинні включати умови реорганізації та ліквідації підприємства. Всі ці вимоги передбачені законодавством та важливі для успішного функціонування підприємства та його захисту;

- Установлені спеціальні вимоги до засновницького договору, статуту та положення суб'єкта господарювання. У засновницькому договорі вказуються умови щодо утворення суб'єкта господарювання, передачі майна, порядок розподілу прибутку та збитків, управління та участі в діяльності, а також процес виходу та приєднання нових засновників. Статут суб'єкта господарювання повинен містити відомості про назву та місцезнаходження, мету та предмет діяльності, розмір фондів, порядок розподілу прибутку та збитків, органи управління та контролю, умови реорганізації та ліквідації.

Положення визначає господарську компетенцію органів державної влади, місцевого самоврядування, окремих підрозділів зі статусом юридичної особи. Всі ці вимоги передбачені законодавством та важливі для належного функціонування

суб'єкта господарювання та його захисту. Регулюючи процес формування, діяльності та розподілу відповідальності, ці документи сприяють гармонійному розвитку бізнесу та допомагають запобігти можливим проблемам [12, с. 41].

Українські суб'єкти господарювання мають загальні права та обов'язки, які стосуються всіх видів діяльності.

Однак, кожен вид суб'єктів господарювання має свої спеціальні права та обов'язки, які властиві лише для даного виду діяльності.Загальні права та обов'язки суб'єктів господарювання охоплюють такі аспекти, як здійснення господарської діяльності в межах законодавства, дотримання правил конкуренції, оподаткування та бухгалтерського обліку. Крім того, всі суб'єкти господарювання повинні дотримуватися прав працівників, охорони довкілля та захисту прав споживачів.

Спеціальні права та обов'язки суб'єктів господарювання визначаються відповідними законами та нормативними актами і можуть стосуватися таких аспектів як спеціальні умови реєстрації, ліцензування чи сертифікації, ведення окремих видів діяльності, дотримання спеціальних правил та процедур. Наприклад, банки мають спеціальні права та обов'язки, пов'язані з організацією банківської діяльності та захистом депозитів клієнтів; фармацевтичні компанії – здійсненням контролю якості та безпеки лікарських засобів тощо.

Так, загальні права та обов'язки суб'єктів господарювання встановлені на законодавчому рівні і є однаковими для всіх видів діяльності. Але спеціальні права та обов'язки залежать від конкретного типу діяльності суб'єкта і можуть містити специфічні вимоги та процедури, пов'язані з цим видом діяльності. Кожен вид суб'єктів господарювання має свої особливості, які враховуються при встановленні спеціальних прав та обов'язків.

Спеціальні права є необхідними для суб'єктів господарювання з виключними видами діяльності, такими як банківські операції, страхування, спільне інвестування та біржові операції. Відповідні закони передбачають

спеціальні права для цих видів діяльності. Наприклад, Закон "Про банки і банківську діяльність" надає комерційним банкам право створювати та брати участь в банківських об'єднаннях (ст. 9) та здійснювати банківські операції на підставі банківської ліцензії (ст. 47). Закон "Про страхування" надає право страховикам здійснювати страхування, співстрахування та перестрахування на договірних засадах (ст. 10-11), створювати та брати участь в об'єднаннях страховиків (ст. 12) та здійснювати страхування через страхових посередників (стр. 14) [15, с. 87].

Норми, що регулюють процедуру припинення діяльності суб'єктів господарювання, визначені Господарським кодексом України (статті 59-Є1). Однак, для суб'єктів господарювання зі спеціальним (виключним) видом діяльності, законодавство передбачає спеціальні норми щодо їх правового статусу та процедури припинення діяльності. Такі норми можуть бути встановлені законами, що визначають особливості правового регулювання певного виду діяльності, наприклад, закони про банки, страхування, спільне інвестування тощо.

Захист інформації в автоматизованих системах має важливе значення у сучасних умовах, що підтверджується аналізом нормативно-правової бази. Створення систем технічного захисту інформації стало необхідною умовою для забезпечення цілісності та конфіденційності даних у процесі їх обробки та передачі.

У публічному праві України, система технічного захисту інформації (СТЗІ) розглядається як комплексний підхід до забезпечення безпеки та конфіденційності інформації. Це включає в себе сукупність суб’єктів, які працюють разом з метою захисту інформації за допомогою технічних заходів та використання нормативно-правової та матеріально-технічної бази. Важливо зберігати конфіденційність даних, що передаються через різні канали зв'язку.

Система технічного захисту інформації допомагає забезпечити це завдання та запобігти можливим наслідкам порушення безпеки даних.

До складу СТЗІ можуть входити різноманітні суб'єкти: органи державної влади, органи місцевого самоврядування, приватні компанії, наукові та освітні установи тощо. Вони об'єднують свої зусилля та використовують специфічні методи технічного захисту інформації залежно від типу діяльності та характеру обробки даних.

Нормативно-правова база СТЗІ складається з законодавчих актів та інших нормативних документів, які регулюють питання захисту інформації від несанкціонованого доступу, втрати або порушення конфіденційності даних. Матеріально-технічна база СТЗІ включає в себе технічні засоби захисту інформації, програмне забезпечення, засоби захисту мережі та інше обладнання.

Отже, система технічного захисту інформації є необхідною складовою сучасної інформаційної безпеки та утверджується як комплексний підхід до захисту інформації від будь-яких загроз. Нормативно-правова та матеріально-технічна база СТЗІ ґрунтовно регулюють питання захисту інформації в Україні та забезпечують відповідність процедур та методів технічного захисту інформації вимогам законодавства.

Система організації технічного захисту інформації є комплексом заходів, які визначаються нормативно-правовими актами та проводяться спеціальними суб'єктами з метою забезпечення цілісності, конфіденційності та доступності даних.

Матеріально-технічна база системи технічного захисту інформації є важливою складовою частиною, оскільки на неї покладено відповідальність за забезпечення правильної функціональності інженерних заходів. Відповідні суб'єкти, об'єднані загальними цілями, здійснюють заходи з встановлення й підтримки технічних засобів захисту інформації, програмного забезпечення, елементів мережі тощо.

Організація технічного захисту інформації передбачає також використання спеціальних протоколів та процедур, що регулюють обмін даними та забезпечують їх конфіденційність. Відповідні суб'єкти, які входять до складу системи технічного захисту інформації, здійснюють навчання персоналу щодо забезпечення безпеки даних та відповідних процедур взаємодії.

Технічний захист інформації є однією з ключових складових ефективної інформаційної політики, тому необхідно створити систему організації технічного захисту інформації, що буде оптимальною та відповідатиме потребам сучасного світу. Запровадження цієї системи дозволить забезпечити надійний захист конфіденційної інформації та запобігти можливим кібератакам та вторгненням на характерні для цього уразливі точки.

Система технічного захисту інформації є складною мережею інженерно-технічних засобів, які вибираються на основі доступної матеріально-технічної бази у суб'єктів, об'єднаних спільними цілями та завданнями захисту даних. Відповідні заходи та процедури регулюються нормативно-правовими документами, що визначають правила та порядок застосування системи ТЗІ.

Аналізуючи діюче законодавство та підзаконні нормативні акти, можна зробити висновок про існування національної системи правового регулювання захисту інформації в автоматизованих системах в Україні. Конституція України гарантує права та свободи людини і громадянина, зокрема право на конфіденційність персональних даних. Цей принцип також передбачений в багатьох інших законодавчих актах та підзаконних нормативних документах, які регулюють відносини щодо охорони інформації. Для забезпечення безпеки та конфіденційності інформації, існують різноманітні нормативні документи, сертифікаційна процедура технічних засобів захисту інформації, а також спеціальні установи та служби, які забезпечують функціонування національної системи захисту інформації.

Окрім цього, в Україні діють також окремі закони, які спеціально стосуються захисту інформації, наприклад Закон України "Про захист персональних даних", "Про інформацію", "Про охорону державної таємниці". Ці закони визначають правила та обов'язки щодо збору, обробки та зберігання інформації, а також встановлюють відповідальність за її порушення.

Отже, в Україні існує чітка система правового регулювання захисту інформації в автоматизованих системах, що базується на національних законодавчих актах та підзаконних нормативних документах. Ця система встановлює правила і процедури щодо забезпечення конфіденційності та безпеки даних, що є надзвичайно важливим у сучасному світі.

Концепція державної політики національної безпеки України має на меті захист суверенітету, територіальної цілісності та конституційного ладу країни. Інформаційна безпека є однією з ключових складових національної безпеки і регулюється законодавством України.

Нормативно-правові акти, такі як "Про інформацію", "Про захист інформації в автоматизованих системах", "Про державну таємницю", "Про науково-технічну інформацію" та інші, встановлюють правила збереження конфіденційності даних, захисту інформації від несанкціонованого доступу тощо.

Україна ратифікувала ряд міжнародних договорів, які регулюють питання забезпечення інформаційної безпеки в рамках міжнародних відносин. Державне регулювання інформаційної безпеки спрямоване на захист прав і свобод людини, боротьбу з кіберзлочинами та іншими загрозами для безпеки держави та її громадян. Надавання належної уваги інформаційній безпеці - ключова складова забезпечення сталого розвитку країни [19, с. 51].

З урахуванням вищезазначеного можна стверджувати, що проблема захисту інформації в автоматизованих системах являє собою актуальний напрям досліджень в Україні. На сьогоднішній день необхідно провести значну роботу з

наукового забезпечення даної проблематики, зокрема починаючи від систематизації понять та термінології, а також на рівні організаційно-правових аспектів.

Важливим етапом вирішення цієї проблеми є розробка наукових методів й алгоритмів, які дозволять оптимально реалізувати процеси захисту інформації в автоматизованих системах. Такі методики повинні враховувати особливості різних типів даних, форматування та обробки інформації, що передається в мережі.

Крім того, досягнення успіху в даному напрямку досліджень потребує тісного співробітництва між науковцями, фахівцями з інформаційних технологій та правниками. Тільки такий підхід дозволить створити повноцінну систему захисту інформації в автоматизованих системах, що буде відповідати вимогам національного та міжнародного законодавства.

З огляду на вищевказане, стає ясним, що необхідно формувати комплексну наукову дисципліну з теорії організації (технології) інформаційної безпеки, що складається з субінституту захисту інформації у автоматизованих системах. Це дозволить забезпечити всебічний підхід до захисту інформації із застосуванням сучасних методів та технологій, а також розробити ефективні механізми боротьби з кіберзагрозами та кіберзлочинами для забезпечення національної безпеки України [10, с. 16]

1.3. Етапи розробки моделі системи інформаційної безпеки на підприємстві

Система забезпечення інформаційної безпеки складається з різних компонентів, які взаємодіють між собою. Основними елементами системи є будівлі, приміщення та території, де розташовані автоматизовані інформаційні

системи, а також технічні засоби, які використовуються для їх функціонування - комп'ютерне обладнання, устаткування локальних мереж, кабельна та телекомунікаційна системи. Крім того, важливим елементом системи забезпечення інформаційної безпеки є інформація, яка зберігається та обробляється в автоматизованій інформаційній системі, а також автономні знімні носії інформації. Нарешті, важливу роль у забезпеченні безпеки даних відіграють співробітники організації, які мають доступ до автоматизованої інформаційної системи та можуть стати носіями інформації про захист системи.

Враховуючи складність та різноманітність складових елементів, забезпечення повноцінного функціонування системи забезпечення інформаційної безпеки вимагає високого рівня організації, контролю та підтримки. Тому, для забезпечення оптимальної роботи системи забезпечення інформаційної безпеки необхідно забезпечувати постійну підтримку технічних засобів, виявляти та запобігати можливим загрозам з боку зловмисників тощо.

Для досягнення оптимального рівня забезпечення інформаційної безпеки необхідно класифікувати рівні доступу до інформації та передбачити можливі загрози. Слід створити умови для мінімізації ймовірності реалізації загроз та появи збитків, а також оперативно реагувати на загрози інформаційної безпеки. Важливо приділяти увагу негативним тенденціям у функціонуванні організації та запобігати виникненню подій, які можуть загрожувати інформаційній безпеці.

Необхідно створювати умови для максимального відшкодування та локалізації шкоди, завданої неправомірними діями осіб, і послаблювати негативний вплив порушень інформаційної безпеки на досягнення стратегічних цілей організації. Забезпечення інформаційної безпеки є постійним процесом, який потребує системного підходу та активної участі всіх зацікавлених сторін. Ефективним є комплексна стратегія, яка включає профілактичні заходи,

планування ризиків, систему контролю та забезпечення безпеки інформації і оперативне реагування на можливі загрози.

Модель - це абстрактне відображення реальності у будь-якій формі, такій як математична, фізична, символьна, графічна або описова. Вона призначена для представлення певних аспектів цієї реальності, що допомагає знайти відповіді на запитання, що досліджуються. Крім того, моделі можуть бути використані для прогнозування поведінки системи, візуалізації складних процесів чи структур, аналізу можливих варіантів розвитку подій та прийняття рішень на основі отриманих даних і висновків. Важливо розуміти, що будь-яка модель не є повною копією реальності, а лише її окремим відображенням, яке може бути корисним для розуміння та аналізу складного світу навколо нас [10].

Для вивчення реальних систем та їх моделей необхідно враховувати багато різноманітних параметрів, які характеризують поведінку системи. Однак, для спрощення процесу дослідження, науковці виділяють чотири рівні моделей, кожна з яких враховує різну кількість і ступінь важливості властивостей та параметрів системи.

Починаючи з найбільш простого рівня, першим є функціональна модель, яка описує основний функціонал системи без урахування її внутрішньої будови та процесів. Ця модель дозволяє отримати загальне уявлення про систему та зрозуміти, як вона працює.

Принципова модель більш складна за функціональну, оскільки вона включає в себе опис процесів, що відбуваються всередині системи, а також враховує принципи її роботи. Ця модель дозволяє детальніше проаналізувати процеси, що відбуваються всередині системи.

Структурна модель дещо складніша за дві попередні, оскільки передбачає опис структури системи та взаємодію її компонентів. Ця модель дає можливість розібратися в будові системи та зрозуміти, як вона функціонує.

Останнім та найскладнішим рівнем моделювання є параметрична модель, яка включає в себе дослідження різних параметрів та їх впливу на систему. Ця модель дозволяє проводити докладний аналіз функціонування системи та виявляти можливі проблеми та шляхи їх вирішення.

Функціональна модель є однією з перших і найпростіших моделей, які використовуються для дослідження системи. Основна мета даної моделі полягає у вивченні функціонування системи та її призначення у взаємодії з іншими елементами - як внутрішніми, так і зовнішніми.

Функціональна модель дозволяє отримати загальне уявлення про принцип роботи системи, а саме, про те, як вона виконує свої основні завдання та функції. Ця модель описує, які результати повинна мати система на виході, які функції вона виконує та які параметри впливають на її роботу.

Однак, варто зазначити, що функціональна модель не враховує внутрішньої будови системи та процесів, що відбуваються в ній. Тому вона може бути неповною та не дає можливості провести докладний аналіз роботи системи.

Загалом, функціональна модель є початковим етапом вивчення системи та дозволяє отримати загальне уявлення про її роботу та взаємозв'язки з іншими елементами. Для більш детального дослідження необхідно використовувати більш складні моделі, такі як принципова, структурна та параметрична моделі.

Функція, яка відображає призначення системи та те, для чого вона потрібна, є найважливішою характеристикою будь-якої системи. Функціональні моделі систем також оперують з функціональними параметрами, які описують об'єкт дослідження та його функціонування.

Основним графічним представленням функціональних моделей систем є блок-схеми, які відображають послідовність дій, необхідних для досягнення бажаного результату (так звана “функціональна схема”).

Функціональна модель системи дозволяє отримати загальне уявлення про її функціонування та взаємозв'язки з іншими елементами. За допомогою функціональної моделі можна визначити основні функції системи та їх параметри, а також з'ясувати, як вона взаємодіє зі своїм середовищем.

Незважаючи на свою простоту, функціональна модель системи має свої обмеження. Вона не дає можливості дізнатися про внутрішню структуру системи та деталізувати процеси, що в ній відбуваються. Для більш детального дослідження системи необхідно використовувати більш складні моделі, такі як принципова, структурна та параметрична моделі.

Таким чином, функціональна модель системи є важливим етапом дослідження, що дозволяє отримати загальне уявлення про її функціонування та взаємодію з іншими елементами. Але для більш детального дослідження необхідно використовувати більш складні моделі та методи аналізу систем.

При описі подібних моделей дослідники намагаються зменшити кількість врахованих параметрів та характеристик системи, залишивши лише найбільш важливі з них. Такий підхід дозволяє зберегти прозорість моделі та уникнути трудомісткої роботи з нею, що може відволікти увагу від суті досліджуваних явищ.

Функціональні та фізичні характеристики процесів та явищ є основними складовими принципової моделі. Детальний опис цих параметрів дозволяє отримати більш докладну інформацію про функціонування системи та встановити зв'язки між різними її елементами. При створенні моделей необхідно забезпечувати баланс між збереженням достатньої точності та складності моделей, а також дотримуватися науково-обґрунтованого підходу до вибору інформації, що включається в модель. Розуміння принципів функціонування систем та використання моделей дозволяє зрозуміти природу явищ, що відбуваються в навколишньому середовищі та сприяє досягненню більш точних та об’єктивних результатів дослідження.

Ці моделі показують основні принципи та закономірності, які лежать в основі системи. Вони дозволяють проводити аналіз системи на більш глибокому рівні та виявляти можливі проблеми.

Отже, модель принципу дії є важливим етапом в системному аналізі та дозволяє зрозуміти принципові засади та властивості системи. Вона складається з основних функціональних та фізичних параметрів, які описують процеси та явища в системі, що дозволяє проводити більш детальний аналіз її роботи.

Принципові вихідні положення (методи, способи, напрямки тощо) покладено в основі будьякої діяльності або роботи.

Графічним представленням моделей принципу дії слугують:

- блок-схема,
- функціональна схема,
- принципова схема.

Інформація - ключове поняття в різних сферах діяльності людини, яке пояснюється її багатоаспектністю та наявністю у різних формах. Вона має важливе значення для прийняття рішень, ефективної комунікації та розвитку інноваційних технологій. Інформаційні технології стали одними з основних напрямів розвитку суспільства, тому знання про інформацію та її використання є необхідними для успішного функціонування будь-якої сучасної організації [11]. У визначенні поняття «інформація» в різні роки переважали три основні підходи:

- недетермінований,
- техноцентричний
- антропоцентричний.

Недетермінований підхід до визначення поняття інформації полягає у відмові від тлумачення її на підставі обмежень та неясностей, які можуть бути пов'язані з її визначенням. Один із засновників кібернетики - Норд Вінер - розглядав інформацію як позначення змісту, який ми одержуємо з зовнішнього

світу та адаптуємося до нього. Його погляд на інформацію полягав у тому, що це не матерія чи енергія, а самостійне, фундаментальне поняття.

З точки зору недетермінованого підходу, інформація є складним поняттям, яке не може бути точно визначене в рамках обмежень та лінійних описів. Інформація може бути представлена у різних формах та матеріалах, таких як текст, зображення, звук, відео тощо. Крім того, інформація може бути інтерпретована по-різному людьми залежно від їхніх знань, досвіду та контексту [11].

Інформація є основою всього існуючого та складовою всіх явищ та процесів. Технологічний підхід до цієї теорії полягає в тому, що інформацію ототожнюють з даними, які мають кількісний вимір, такий як обсяг, швидкість передачі чи пропускна здатність каналу. Однак, цей підхід не враховує всіх аспектів інформації, зокрема, її значення та контексту. Клод Шеннон у 60-х роках XX століття визначив поняття "інформації" як "упорядкованої субстанції, яку можна описати математично", що дозволяє застосовувати математичні методи для аналізу та обробки. Але інформація може мати як кількісний, так і якісний аспекти, що потребує використання різноманітних підходів для її аналізу та розуміння. Для повного розуміння поняття інформації, необхідно враховувати її різноманітність та соціально-культурний контекст функціонування [7].

Підхід, який зараз переважає в точних науках та інформаційній безпеці, є орієнтованим на фізичні параметри технічних засобів та математичні алгоритми їх роботи. Він широко використовується під час розробки та впровадження апаратно-програмних засобів для захисту інформації. Проте цей підхід не враховує змістовний аспект інформації, що унеможливлює його застосування в правовому регулюванні інформаційних відносин.

У свою чергу, антропоцентричний підхід базується на тому, що інформацію розглядають як знання, яке можна отримати та засвоїти. Такий підхід знайшов широке застосування в юридичній науці та законодавстві.

Зміст антропоцентричного підходу полягає в тому, що інформація має змістовне значення та пов'язана з людською діяльністю. Оскільки інформація може бути передана лише за допомогою мови або символів, то вона надає можливості для комунікації та взаємодії між людьми. Тому важливо враховувати не лише технічні параметри систем, що обробляють інформацію, але і змістовні аспекти, такі як конфіденційність, доступність, інтегритет та інші.

Цей підхід є основою для розробки законодавства та нормативних актів, що регулюють використання та захист інформації в суспільстві. Він дозволяє враховувати потреби та інтереси людей у процесі обробки та передачі інформації та забезпечує її належний рівень захисту.

Отже, антропоцентричний підхід до інформації забезпечує більш комплексний підхід до створення та використання інформаційних систем, що визнає значення їхнього змісту та соціальної важливості.

Узагальнена модель створюється з метою збереження та передачі інформації про специфічний об'єкт у вигляді уявного образу, знакового опису або матеріальної системи. Це дозволяє відображати властивості, характеристики та зв'язки об'єкта-оригіналу будь-якої природи, які є суттєвими для розв'язання задачі, вирішуваної суб'єктом. [12, с. 44].

В теорії прийняття рішень, для досягнення максимальної ефективності, використовуються моделі, які виражаються у формі слів, формул, алгоритмів та інших математичних засобів. Такі моделі дозволяють точно описати взаємозв'язки між об'єктами та параметрами, що є суттєвим для вирішення задачі прийняття рішень. Крім того, такі моделі можуть бути застосовані для

прогнозування подальшого розвитку подій та визначення оптимального шляху дій [1].

Моделі можна поділити на такі види:

1) функціональні моделі – відображають прямі залежності між ендогенними та екзогенними змінними. Ендогенні змінні є такими змінними, значення яких визначаються в процесі діяльності компонентів або елементів системи, тобто "всередині" системи. Екзогенні змінні, натомість, визначаються або дослідником, або ззовні, тобто у будь-якому випадку вони діють на систему ззовні. Ці моделі дозволяють зрозуміти, як і чому змінюються показники системи за наявності певних умов, а також передбачити можливі наслідки різних сценаріїв дії [1];

2) моделі, виражені за допомогою систем рівнянь щодо ендогенних величин;

3) Моделі оптимізаційного типу складаються з системи рівнянь щодо ендогенних змінних. Головна мета таких моделей полягає у пошуку оптимального рішення для певного показника. Це можуть бути, наприклад, мінімальні витрати, максимальний прибуток або оптимальна кількість виробленої продукції. Моделі оптимізаційного типу дозволяють знайти найбільш ефективний спосіб використання ресурсів та максимізувати показники економічної діяльності системи. Вони широко використовуються у різних галузях, включаючи фінанси, логістику, менеджмент та інші;

4) імітаційні моделі – можуть дуже точно відображати досліджуване явище. Оскільки такі моделі базуються на симуляції реальних процесів, вони можуть ураховувати складні, нелінійні та стохастичні залежності. Математична формалізація імітаційних моделей може бути досить складною, оскільки потребує використання комп'ютерних програм та алгоритмів для генерації випадкових подій. Такі моделі широко застосовуються у багатьох областях,

включаючи економіку, фізику, соціологію та інші науки, оскільки дозволяють проводити дослідження без прямого втручання у реальні процеси.

Моделі можна розділити на дві основні категорії - керовані та прогнозні. Керовані моделі відповідають на запитання, пов'язані з досягненням певної мети або результату, яке потрібно отримати. Ці моделі включають три основні групи змінних:

змінні, які описують поточний стан об'єкта;

змінні-керування, які впливають на поточний стан об'єкта і можуть бути контрольовані та вибрані за певною метою;

вихідні дані і зовнішні впливи, такі як вхідні параметри, що задаються ззовні.

У прогнозних моделях керування не є центральним елементом. Ці моделі призначені для відповіді на запитання типу "Що буде, якщо нічого не зміниться?". Вони дозволяють прогнозувати майбутній стан об'єктів, ґрунтуючись на аналізі даних про їхній минулий стан та взаємозв'язки між ними. Прогнозні моделі допомагають аналізувати можливі наслідки різних сценаріїв без залучення активної участі користувача в процесі прийняття рішень.

Отже, різниця між керованими та прогнозними моделями полягає в тому, що керовані моделі спрямовані на досягнення конкретної мети, тоді як прогнозні моделі дозволяють прогнозувати майбутній стан об'єктів без активного керування. Обидва типи моделей використовуються в різних галузях, таких як наука, технології та бізнес, для аналізу та прийняття рішень.

Моделі можуть бути класифіковані на безперервні та дискретні в залежності від способу вимірювання часу. Якщо модель містить параметри, що змінюються з часом, то вона вважається динамічною. Найчастіше в моделях використовується дискретний час, оскільки інформація надходить дискретно,

наприклад у формі звітів, балансів та інших документів, що складаються періодично.

Дискретна модель передбачає, що час розбивається на певні інтервали, а змінні можуть змінюватися лише на кінець кожного інтервалу. Цей підхід є ефективним для більшості задач, оскільки дозволяє зберегти інформацію про стан об'єкту за певний період часу.

З іншого боку, безперервна модель використовує неперервну функцію часу для опису стану системи, що змінюється з плином часу. Вона дозволяє точніше визначити зміну значень змінних в будь-яку мить часу. Однак, вона може виявитися складнішою для вивчення, оскільки потребує більш складних математичних методів.

Таким чином, вибір між дискретною та безперервною моделлю залежить від природи досліджуваної системи та поставленої задачі. Обидва підходи можуть бути корисними для побудови ефективних та точних моделей, які можуть використовуватися для аналізу та прийняття рішень в різних галузях, таких як наука, технології та бізнес.

Імітаційне моделювання може бути застосовано для вивчення теорії дуополії, яка є моделлю конкуренції двох фірм. Одним із прикладів є модель дуополії, запропонована О. Курною, а новий поштовх надано в монографії Дж. Фон Неймана та О. Моргенштейна. Застосування імітаційного моделювання дозволяє оцінити ефективність стратегій та отримати рекомендації щодо оптимальних стратегій для кожної з фірм, покращуючи ефективність ринку.

Організація - багатогранна форма з різним вмістом, її можна описати як сукупність взаємопов'язаних компонентів, число яких визначено цілями управління. Організація може бути представлена деревом процесів, джерелами і каналами зв'язку, організаційною структурою та інфраструктурою. Кожен аспект є самостійним "проекцією" організації, що дає можливість досягти цілісного підходу до управління та аналізу. Описані компоненти дозволяють

побачити організацію як групу взаємопов'язаних елементів, які взаємодіють між собою для досягнення спільної мети.

Кожна організація створюється з метою створення доданої вартості та отримання прибутку, тому ключовою метою загального керівництва є представлення об'єкта у вигляді мережі процесів, які визначають його місію, називаючи такі процеси бізнес-процесами. Уявлення або моделювання об'єкта як набору бізнес-процесів визначає всі інші "проекції" організації. (див. рис.1).

Рисунок1 – Представлення різних моделей для об'єкта моделювання.

Реалізація систем автоматизації завжди передбачає проведення передпроектного обстеження діяльності організації. Це дає можливість отримати експертний висновок, у якому надаються рекомендації щодо усунення вразливостей управління діяльністю. До реалізації проекту впровадження системи автоматизації проводиться реорганізація бізнес-процесів на основі цього висновку.

Проведення комплексного обстеження організацій завжди є складним завданням, яке відрізняється від інших за метою та способами досягнення

результату. Важливим етапом є аналіз діяльності організації, що дозволяє виявити поточні проблеми та можливості для поліпшення. На підставі результатів аналізу формується експертний висновок з рекомендаціями щодо оптимізації процесів.

При моделюванні важливо враховувати адекватність, точність, універсальність і економічність моделей. Адекватність полягає у відповідності моделі реальній системі з урахуванням найважливіших якостей та характеристик. Точність передбачає ступінь збігу результатів моделювання з бажаними результатами. Універсальність дозволяє застосовувати модель до аналізу ряду однотипних систем в різних режимах. Економічність пов'язана з грамотним витрачанням ресурсів на моделювання, щоб досягти бажаних результатів.

Моделювання систем забезпечення інформаційної безпеки є важливим етапом у розробці та підтримці захисту інформації. Це дозволяє визначити необхідні та достатні умови для забезпечення її безпеки. Однак, організаційні аспекти також грають важливу роль у розробці технічних аспектів захисту інформації та окремих компонентів.

Розв'язання проблеми інформаційної безпеки залежить від двох основних завдань. По-перше, необхідно переконати користувачів у необхідності забезпечення інформаційної безпеки та досягти однозначного розуміння проблеми. По-друге, треба синтезувати систему забезпечення інформаційної безпеки з урахуванням можливих ризиків та обмежень.

Важливо пам'ятати, що абсолютна захищеність інформації неможлива. Тому при розробці системи забезпечення інформаційної безпеки необхідно оцінити ступінь ризику та планувати заходи з мінімізації наслідків можливого порушення безпеки інформації. Заходи забезпечення інформаційної безпеки повинні бути цілеспрямованими та ефективними, з урахуванням специфіки конкретної ситуації та потреб користувачів.

Крім того, під час переходу до експлуатації системи забезпечення інформаційної безпеки необхідно підтримувати заданий рівень її захищеності та проводити регулярну перевірку на предмет виявлення нових можливих загроз та вразливостей. Тільки так можна забезпечити оптимальний захист інформації та запобігти можливим нападам на неї.

Недостатня оцінка рівня захищеності інформації може призвести до проблем, пов'язаних зі зміною кадрів та невідповідністю розробленої схеми захисту реальним умовам. Саме тому необхідно періодично проводити оцінку рівня захищеності інформації.

У теорії захисту інформації ключовою фігурою є порушник - особа, яка намагається отримати несанкціонований доступ до інформації. Важливо враховувати його практичні та теоретичні можливості, наявність апріорних знань, час та місце дій, щоб ефективно захистити інформацію від можливих загроз. Підвищення свідомості користувачів щодо потенційних загроз та правильне використання методів захисту - важливий етап у забезпеченні безпеки інформації.

Основне зміст стандарту ISO/IEC 27001 полягає у встановленні процесів системи менеджменту інформаційної безпеки та вимог до їх розробки, впровадження, моніторингу та підтримки. Стандарт також надає визначення інформаційної безпеки, аби забезпечити збереження конфіденційності, цілісності та доступності інформації. Важливо регулярно оцінювати рівень захищеності інформації та правильно застосовувати методи захисту та підвищувати свідомість користувачів про потенційні загрози. Міжнародний стандарт ISO/IEC 27001, разом зі стандартами [15] та [16], може допомогти організаціям забезпечити безпеку інформації.

Основна користь впровадження системи управління інформаційною безпекою на основі стандарту ISO/IEC 27001 полягає у забезпеченні захисту інформаційних активів організації шляхом виявлення загроз та ризиків,

прийняття рішень на основі поставлених цілей, зменшення вартості підтримки системи та підвищення авторитету організації на внутрішньому та зовнішньому ринках. Крім того, система допомагає керувати інформаційною безпекою в критичних ситуаціях, легко інтегрується в бізнес-процеси та демонструє прихильність до інформаційної безпеки перед клієнтами, партнерами та власниками бізнесу.

Стандарт ISO/IEC 27001 включає елементи управління, такі як розробка політики безпеки, робота з персоналом, забезпечення безперервності виробничого процесу та відповідність юридичним вимогам. Ці вимоги мають загальний характер і можуть бути застосовані в різних секторах ринку, включаючи фінансовий, страховий, телекомунікаційний, комунальний, роздрібну торгівлю, виробництво, сервісні галузі, транспорт та органи влади.

Забезпечення інформаційної безпеки полягає в упровадженні комплексу елементів управління, таких як політики, процеси, процедури, організаційна структура, програмне та апаратне забезпечення. Для досягнення максимальної ефективності, ці елементи повинні бути розроблені, впроваджені, моніторені, переглянуті та вдосконалені за необхідності. Таким чином, можна підтвердити, що інформаційна безпека досягнута, а бізнес-цілі організації будуть досягнуті.

Створення інформаційної системи, що автоматизує інформаційні процеси організації, потребує аналізу функціональної взаємодії об'єктів автоматизації та їхньої взаємодії з довкіллям. За отриманою інформацією створюється функціональна модель, що описує основні функції системи та її компонентів.

Склад функціональної моделі залежить від контексту конкретної системи та може бути представлений у вигляді різноманітних документів. Наприклад, це можуть бути схеми баз даних, блок-схеми процесів, ілюстрації інтерфейсів користувачів, тощо. Важливо, щоб функціональна модель була

зрозумілою та доступною для всіх учасників процесу розробки та експлуатації системи інформаційної безпеки.

Таким чином, забезпечення інформаційної безпеки та створення інформаційних систем залежать від комплексу управлінських елементів та правильного аналізу функціональної взаємодії об'єктів автоматизації.

Функціональна модель інформаційної системи складається з кількох моделей, що описують процеси обробки інформації. Конструкції функціональної моделі включають структуру системи управління, технологічну схему процесу управління, комплекс характеристик управління, чинники, що впливають на ефективність управління, структуру інформації та взаємодію функцій управління. У дослідженні теорій управління також використовують комп'ютерні моделі з різною структурою та призначенням.

Моделювання є ефективним методом дослідження систем управління, але для досягнення позитивного результату необхідно використовувати широкий спектр інших методів. Моделювання стає найбільш ефективним, коли проблеми є добре структурованими, є достатня кількість інформації для оцінки ситуацій та проблем, а також наявна відпрацьована методологія роботи з моделями.

Незважаючи на багато переваг, використання моделей має свої труднощі. Однією з основних складнощів є висока вартість проведення досліджень. Крім того, можуть виникати труднощі з початковою недостовірною інформацією про об'єкт дослідження, необхідність надмірного спрощення характеристик об'єкта, помилки в методології моделювання та інші фактори.

Однак, з правильною підготовкою та використанням відповідних методів дослідження, застосування моделювання може допомогти вирішити багато проблем управління. Тому важливо забезпечити якість початкових даних та правильно вибрати методологію моделювання, щоб зменшити можливі помилки та зробити дослідження якомога ефективнішим.

В сучасному управлінні організації часто використовують традиційні методи концептуального моделювання, де інформаційні потоки між керівними ланками розглядаються окремо, а лише деякі з них можуть взаємодіяти, створюючи керівну інформаційну систему для прийняття рішень. Однак нові виклики та завдання з використання інформаційних систем дозволяють розгорнути процеси обробки транзакцій та забезпечити зв'язки між ними.

Моделювання також може бути використане для виявлення можливих проблем управління інформаційними процесами організації та для визначення шляхів покращення цих процесів. Застосування моделей дозволяє зрозуміти взаємодію між різними складовими системи та їх вплив на результативність діяльності організації. У свою чергу, це дає можливість підвищити ефективність управління інформаційними процесами та забезпечити успішну роботу організації в цілому.

При створенні моделей інформаційних систем часто відсутня формальна теоретична основа, що робить її схожою на інші методики. Це призводить до необхідності створення теоретичних рамкових принципів (англ. Framework) для того, щоб забезпечити пояснення та покращити якість концептуального моделювання. Оскільки теоретична основа є критично важливим аспектом у будівництві баз даних, недосконаліть її може значно вплинути на успішність проекту.

Організація можна порівняти з живим організмом, який складається з системи організованих інформаційних процесів, що надходять ззовні, циркулюють всередині та створюються як результат дій керівництва і працівників. Проте, не всі процеси формуються свідомо, багато з них обумовлені об'єктивною реальністю. Тому дуже важливо мати правильну теоретичну основу для ефективної роботи з інформаційними процесами та збереження цілісності даних.

Функціональна модель - це система пов'язаних систем, що включає багатоструктурні елементи, принципи і процеси, в тому числі й наслідки помилок управління, нерозуміння завдань співробітниками або необ'єктивне оцінювання результатів керівником. Важливим етапом при створенні інформаційної системи з метою автоматизації інформаційних процесів є аналіз функціональної взаємодії між об'єктами автоматизації. Цей аналіз дозволяє розробникам зрозуміти, які функції повинні бути виконані системою та як вони повинні бути побудовані для досягнення оптимального результату.

Після проведення аналізу, аналітики наводять результати у вигляді функціональної моделі, яка може бути представлена у формі текстової та графічної інформації. Склад функціональної моделі значно залежить від контексту конкретної системи, тож розробники повинні враховувати цей фактор у процесі її створення. Важливо мати чітку та зрозумілу функціональну модель, яка відповідає потребам організації та є оптимальною для виконання необхідних завдань.

Система управління інформаційною безпекою є системою документування всіх процесів, пов'язаних з інформаційною діяльністю та відносинами в організації. Ця система документації відповідає вимогам міжнародних стандартів серії ISO/IEC 27k, а також залежить від структури організації, виду та форми власності (приватна, державна) та сфери діяльності самої організації. На рисунку 2 представлена система, яка об'єднує 14 напрямків забезпечення інформаційної безпеки, названі так, щоб відображувати сутність функціонування системи менеджменту.

ІНФОРМАЦІЯ	A.5 Політики інформаційної безпеки
	A.6 Організація інформаційної безпеки
	A.7 Безпека, пов'язана з персоналом
	A.8 Управління активами
	A.9 Управління доступом
	A.10 Криптографія
	A.11 Фізична безпека і захист від навколишнього середовища
	A.12 Безпечна робота
	A.13 Безпека зв'язку
	A.14 Придбання, розробка та підтримка систем
	A.15 Взаємовідносини з постачальниками
	A.16 Інцидент-менеджмент інформаційної безпеки
	A.17 Аспекти інформаційної безпеки під час управління безперервністю бізнесу
	A.18 Відповідність вимогам

Рис. 2 – Модель «Система управління інформаційною безпекою»

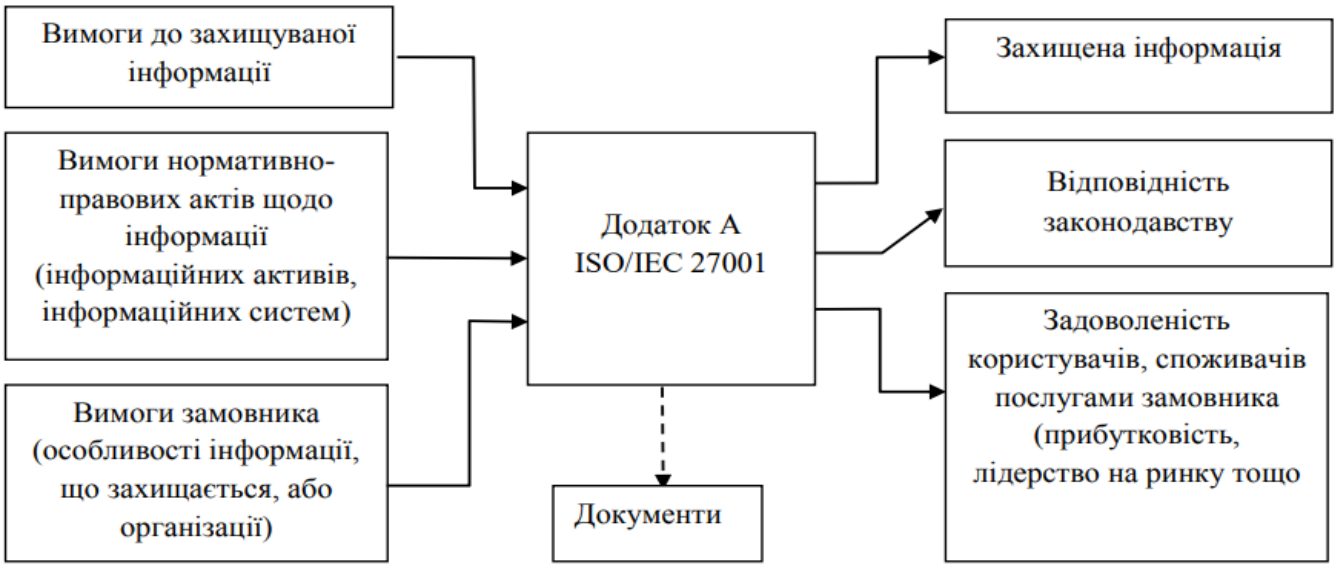

Рисунок 3 – Функціональна модель системи забезпечення інформаційною безпекою.

З урахуванням вищезазначеного можна зробити висновок, що проблематика захисту інформації в автоматизованих системах України перебуває на стадії активного розвитку та потребує наукового забезпечення, зокрема, систематизації на різних рівнях організаційно-правових аспектів. У зв'язку з цим, необхідно формування комплексної наукової дисципліни "теорії організації (технології) інформаційної безпеки", яка включатиме субінститут захисту інформації в автоматизованих системах.

Ця дисципліна має на меті вивчення методів та підходів до організації систем захисту інформації в автоматизованих системах, а також розробки відповідних правових норм та політик безпеки. Застосування тектології допоможе ефективно забезпечити захист інформації в автоматизованих системах та уникнути можливих загроз і ризиків для бізнесу і організацій. Крім того, комплексне підход до захисту інформації забезпечить стійкість автоматизованих систем до можливих вірусів та злому, що зменшить ризик викрадення конфіденційної інформації.

Висновки. Розвиток сучасних технологій призвів до збільшення обсягів інформації, яку необхідно обробляти, зберігати та передавати в організаціях. Це стало причиною зростання потреби в ефективних методах та інструментах моделювання інформаційних процесів.

Використання різноманітних методологій моделювання дозволяє наочно продемонструвати складові інформаційного процесу в єдиній схемі функціонування організації. Такі методи дозволяють покращити стан забезпечення інформаційної безпеки та зменшити ризик втрати чутливої інформації.

Застосування стандартів серії ISO/IEC 27k є важливою складовою використання методів моделювання. Функціональна модель, яка базується на цих стандартах, дозволяє забезпечити повноту технологічного процесу та забезпечення інформаційної безпеки організації. Додаток А ISO/IEC 27001 є системоутворюючим чинником, який поєднує елементи системи забезпечення інформаційної безпеки організації.

Використання методів та інструментів моделювання інформаційних процесів є важливим кроком у забезпеченні ефективного захисту інформації та поліпшенні її безпеки в організаціях.

2. АНАЛІЗ РОБОТИ ТОВ «ПЕРША УКРАЇНСЬКА ГАЗОНАФТОВА КОМПАНІЯ» ТА ВИЯВЛЕННЯ ЗАГРОЗ В ЇЇ СИСТЕМІ ІНФОРМАЦІЙНІОЇ БЕЗПЕКИ

2.1. Характеристика діяльності ТОВ «Перша українська газонафтова компанія»

Перша українська газонафтова компанія (ПУГК) - це один з провідних недержавних нафтогазовидобувних підприємств України, яке було створене в 1991 році. Серед основних напрямків діяльності компанії є пошук, розвідка, видобуток та переробка нафти та газу.

Метою ПУГК є задоволення потреб ринку в продукції, роботах та послугах, збільшення їх асортименту та якості, забезпечення конкурентоспроможності на ринку, ефективне управління майном Товариства, отримання прибутку для його подальшого використання і/або розподілу для розвитку компанії. Наша мета полягає у задоволенні інтересів акціонерів Товариства, а також у забезпеченні економічних інтересів та соціальних потреб працівників. Ми прагнемо залишатися лідером в нашій галузі, надаючи якісні послуги, що відповідають найвищим стандартам і очікуванням наших клієнтів.

ПУГК прагне дотримуватися міжнародних етичних стандартів та забезпечувати повну відповідність вимогам охорони праці, навколишнього середовища та безпеки. Ми постійно використовуємо найсучасніші технології та методи, щоб забезпечити нашому бізнесу максимальну результативність та ефективність. Компанія прагне зробити свій внесок у досягнення енергетичної незалежності України, використовуючи передові розробки та інноваційні ідеї для оптимізації процесів та зменшення впливу на довкілля. Наша мета полягає в тому, щоб забезпечити найвищу якість продукту та послуг для задоволення потреб наших клієнтів, при цьому дотримуючись вимог етики та законодавства.

Одним із ключових завдань ПУГК є соціальна відповідальність, запровадження інноваційних технологій та передового досвіду у нафтогазовій галузі. Компанія постійно працює над вдосконаленням своїх процесів, щоб забезпечити оптимальну якість продукції та задовольнити потреби споживачів.

Предметом діяльності Першої української газонафтової компанії (ПУГК) є видобування нафти та газу. Крім цього, компанія займається проектуванням, будівництвом, реконструкцією та технічним переозброєнням електричних мереж, будівель, споруджень, машин та механізмів.

ПУГК є лідером серед недержавних нафтогазовидобувних підприємств України та працює з дотриманням міжнародних етичних стандартів та вимог охорони праці, навколишнього середовища та безпеки. Компанія використовує найсучасніші технології та методи для забезпечення оптимальної якості продукції та задоволення потреб споживачів.

Перша українська газонафтова компанія (ПУГК) є публічним акціонерним товариством, інформацію про яке можна знайти на веб-сайті "Спільне підприємство Перша Українська Газонафтова Компанія" для користувачів та акціонерів. На сайті розміщені установчі документи компанії, такі як статут, положення про загальні збори акціонерів, наглядову раду, керівництво, ревізійну комісію, а також про кожну з філій. Крім того, на сайті доступні протоколи загальних зборів, свідоцтво про державну реєстрацію випуску акцій та особлива інформація про компанію. ПУГК завжди відкрита для співпраці та готова надавати максимально можливу інформацію про свою діяльність.

2.2 Основні принципи та методи захисту інформаційних процесів в ТОВ «Перша українська газонафтова компанія»

У спільному підприємстві "Перша українська газонафтова компанія" існує окрема служба інформаційної безпеки, яка забезпечує захист інформаційних

процесів в компанії. Ця служба відокремлена від всіх відділів та груп, які займаються управлінням системою, програмуванням та іншими завданнями, щоб уникнути можливого зіткнення інтересів.

Комплексність підходів до інформаційної безпеки та пов'язаних з нею проблем є ключовим фактором успішного розвитку національних інформаційних систем. Особлива увага приділяється професійній освіті та наукових дослідженнях в галузі інформаційної діяльності, які визначені статтями 15 та 16 Закону України "Про інформацію".

Напрями забезпечення безпеки є важливими нормативно-правовими категоріями, які визначають комплексні заходи з захисту інтересів комерційних підприємств. Модель забезпечення інформаційної безпеки Першої української газонафтової компанії полягає в застосуванні сучасних методів та технологій захисту інформації, що дозволяє ефективно захищати конфіденційну інформацію та запобігати можливим загрозам безпеці. Крім того, ПУГК працює над постійним вдосконаленням своїх систем захисту інформації та розробляє нові стратегії для відповіді на загрози вірусів, хакерських атак та інших можливих загроз.

Також компанія забезпечує доступність інформації, використовуючи стійкі засоби резервного копіювання даних та гарантовану доступність інформації для користувачів, які мають на це право.

Модель забезпечення інформаційної безпеки Першої української газонафтової компанії передбачає взаємодію всіх підрозділів компанії з метою ефективного захисту інтересів підприємства.

ТОВ "Перша українська газонафтова компанія" як система має певні структурні ланки:

− органи управління підприємством;

− бухгалтерію;

− відділи – функціональні ланки підприємства;

− допоміжні служби;

− службу безпеки.

«Перша українська газонафтова компанія» є великим комерційним підприємством, яке займається видобутком та переробкою нафти і газу. Компанія приділяє велику увагу захисту інформації і має власну службу інформаційної безпеки.

Одним з напрямів забезпечення безпеки є забезпечення конфіденційності інформації. Для цього компанія використовує шифрування даних та контроль доступу для зменшення ризику несанкціонованого доступу до конфіденційної інформації.

Ще одним напрямом є забезпечення цілісності інформації. Компанія використовує технології захисту від зламу, вірусів та інших видів вторгнень, а також проводить регулярні аудити та оцінки ризиків для виявлення можливих порушень цілісності інформації.

Також компанія забезпечує доступність інформації, використовуючи стійкі засоби резервного копіювання даних та гарантовану доступність інформації для користувачів, які мають на це право.

Модель забезпечення інформаційної безпеки передбачає взаємодію всіх підрозділів компанії з метою ефективного захисту інтересів підприємства.

У загальному, «Перша українська газонафтова компанія» є успішним підприємством з високим рівнем професійної культури та дотриманням стандартів інформаційної безпеки.

ТОВ "Перша українська газонфтова компанія" має багаторівневу систему захисту інформації з ієрархічним доступом до неї, яка є прив'язана до специфіки підприємства та відкрита для регулярного оновлення. Комплексність системи забезпечується формуванням з різних елементів - правових, організаційних, технічних та програмно-математичних.

Крім технічних заходів, компанія надає велику увагу захисту конфіденційної інформації та включає елементи організаційного захисту інформації. У рамках цих заходів встановлюється система обмеження доступу персоналу до конфіденційної інформації, регламентується процес обробки та зберігання конфіденційних документів, формуються та регламентуються дії служби безпеки підприємства.

Успішне функціонування системи забезпечення інформаційної безпеки залежить від своєчасного та ефективного виконання відповідальними особами підприємства організаційних заходів з захисту інформації. Такий підхід дозволяє забезпечити надійний захист конфіденційної інформації та не створювати серйозних незручностей для співробітників підприємства в ході роботи.

"Перша українська газонфтова компанія" в своєму комплексному арсеналі захисту використовує елементи протипожежної охорони та засоби виявлення приладів і пристроїв технічної розвідки. Захист конфіденційної інформації забезпечується за допомогою організаційних, технічних та програмно-математичних заходів. Доступ до електронних документів регулюється персональними паролями та іншими методами захисту. Компанія також використовує спеціальні засоби та криптографічні методи захисту інформації у ПК та мережах для забезпечення безпеки своєї діяльності.

"Перша українська газонфтова компанія" використовує криптографію під час передачі тексту по звичайному та факсимільному зв'язку, а також під час листування поштою, щоб захистити конфіденційну інформацію. Елементи захисту можуть містити окремі складові, які забезпечують безпеку обробки, зберігання та передачі інформації. Компанія використовує математичні методи захисту, щоб запобігти можливим загрозам для своєї діяльності та зберегти безпеку конфіденційної інформації. Зовнішні загрози можуть бути випадковими або запланованими та мати різний рівень кваліфікації, серед них кримінальні

структури, потенційні злочинці і хакери, нечесні партнери та технічний персонал постачальників послуг.

Внутрішні джерела загроз в компанії зазвичай є кваліфікованими фахівцями з розробки та експлуатації програмного забезпечення і технічних засобів. Вони знають специфіку завдань, структуру і основні функції програмно-апаратних засобів захисту інформації та мають доступ до штатного устаткування та технічних засобів мережі.

До них відносяться:

− основний персонал (користувачі, програмісти, розробники);

− представники служби захисту інформації;

− допоміжний персонал (прибиральники, охорона);

− технічний персонал.

Технічні засоби, що є джерелами потенційних загроз безпеці інформації ТОВ «Перша українська газонафтова компанія», також можуть бути:

Таблиця 1.2.

Технічні засоби потенційних загроз.

Зовнішнішні	Внутрені
засоби зв’язку	неякісні технічні засоби обробки інформації
мережі інженерних комунікації	неякісні програмні засоби обробки інформації
транспорт	допоміжні технічні засоби (охорони, сигналізації, телефонії)
	інші технічні засоби, що застосовуються в установі

Також на інформаційну безпеку компанії можуть впливати різноманітні зовнішні фактори, такі як неправильне зберігання даних, крадіжка комп'ютерів і носіїв, форс-мажорні обставини. Організація повинна застосовувати відповідні заходи для захисту інформаційної безпеки, такі як правила доступу до комп'ютерної мережі, антивірусне програмне забезпечення та інші засоби, що зменшують ризики порушення інформаційної безпеки.

Наявність розвиненої системи інформаційної безпеки є однією з найважливіших умов конкурентоспроможності та життєздатності будь-якого підприємства, у тому числі і ПАТ "Перша українська газонафтова компанія". Для забезпечення інформаційної безпеки компанії використовуються такі засоби як ідентифікація та аутентифікація користувачів, шифрування даних, мережева безпека, контентна фільтрація, антивірусний захист тощо. Використання цих засобів дозволяє зменшити ризики порушення безпеки даних та зберегти конфіденційність інформації компанії.

Кожен з перелічених засобів може використовуватись як самостійно, так і в інтеграції з іншими системами. Це дозволяє створювати комплексні системи інформаційного захисту будь-якої складності та конфігурації, незалежно від використовуваних платформ. Використання різних засобів одночасно дозволяє комплексно захистити інформацію від можливих загроз. Також слід зазначити, що інтеграція з іншими системами може допомогти забезпечити більш ефективне функціонування системи захисту інформації та зменшити ризики порушення безпеки.

Висока ефективність заходів з захисту від втрати конфіденційної інформації є дуже важливою для будь-якої компанії. У ТОВ "Перша українська газонафтова компанія" використовуються різноманітні засоби захисту, серед яких можна виділити систему контролю вхідної та вихідної електронної пошти. Застосування правил перевірки дозволяє забезпечити безпеку компанії від судових позовів та захистити співробітників від спаму.

Основними принципами інформаційної безпеки в ТОВ «Перша українська газонафтова компанія» є:

− забезпечення цілісності і збереження даних, тобто надійне їх зберігання в неспотвореному вигляді;

− дотримання конфіденційності інформації (її недоступність для тих користувачів, які не мають відповідних прав);

− доступність інформації для всіх авторизованих користувачів за умови контролю за всіма процесами використання ними отриманої інформації;

− безперешкодний доступ до інформації в будь-який момент, коли вона може знадобитися підприємству [25, с. 34].

Ці принципи неможливо реалізувати без особливої інтегрованої системи інформаційної безпеки., що виконує наступні функції:

− вироблення політики інформаційної безпеки;

− аналіз ризиків (тобто ситуацій, в яких може бути порушена нормальна робота інформаційної системи, а також втрачені або розсекречені дані);

− планування заходів щодо забезпечення інформаційної безпеки;

− планування дій в надзвичайних ситуаціях;

− вибір технічних засобів забезпечення інформаційної безпеки [30, с. 34].

У ТОВ "Перша українська газонафтова компанія" етапи робіт із забезпечення інформаційної безпеки включають проведення обстеження підприємства для виявлення загроз несанкціонованого доступу до конфіденційної інформації, розробку політики безпеки та організаційних документів, проектування і розробку системи інформаційної безпеки, впровадження її в діючу структуру підприємства, навчання персоналу та атестацію системи. Дотримання цих етапів дозволяє забезпечити надійний захист конфіденційної інформації та запобігти можливим загрозам безпеці компанії.

Збереження безпеки інформаційної системи є важливим аспектом діяльності будь-якої компанії, зокрема ТОВ «Перша українська газонафтова компанія»". Основною метою комплексної інформаційної безпеки є захист інформаційних ресурсів підприємства від можливих загроз, таких як віруси, шпигунські програми, крадіжки даних тощо.

Проте сам термін "інформаційна безпека" є достатньо абстрактним та потребує узагальнення та конкретизації для ефективного використання його в реальному середовищі. Тому необхідні інструменти, які допоможуть систематизувати технології інформаційної безпеки та забезпечити захист інформаційного простору підприємства. Таким інструментом є політика інформаційної безпеки, яка охоплює встановлення правил та процедур з обмеження доступу до інформації, регулювання користування комп'ютерами та іншими пристроями, перевірку наявності бекапів та інших запобіжних заходів.

Використання політики інформаційної безпеки дозволяє забезпечити захист інформаційних ресурсів підприємства, гарантувати повноту та точність наданої інформації, а також мінімізувати можливі руйнування або модифікації інформації, якщо такі трапляються. В результаті, компанія може працювати з більшою ефективністю та успішністю, особливо на фоні постійно зростаючих загроз в сучасному цифровому світі.

2.3 Оцінка стану забезпечення захисту інформаційних процесів у ТОВ «Перша українська газонафтова компанія».

Існує кілька методик оцінки ризиків в інформаційній безпеці, але основними є метод оцінки на основі моделі загроз та вразливості та метод оцінки на основі моделі інформаційних потоків. Важливим етапом у процесі оцінки ризиків є визначення загроз для інформаційної системи та її вразливостей. Для цього можна використовувати метод оцінки ризиків на основі

моделі загроз та вразливості, який базується на вивченні потенційних загроз та вразливостей системи.

Також існує метод оцінки ризиків на основі моделі інформаційних потоків, який дозволяє визначити рівень ризику, аналізуючи потоки інформації в системі та ідентифікуючи можливі проблеми з конфіденційністю, цілісністю та доступністю.

Отже, для повного аналізу інформаційних ризиків необхідно побудувати повну модель інформаційної системи з точки зору її інформаційної безпеки. Це дозволить виявити потенційні загрози та вразливості, оцінити ризики та прийняти необхідні заходи для запобігання можливим інцидентам в майбутньому.

Для вирішення цього завдання можна скористатися програмою "Гриф", яка має простий та інтуїтивно зрозумілий інтерфейс. Вона використовує складний алгоритм, у якому міститься 54 параметри аналізу ризиків, що дозволяє отримати точну оцінку існуючих в інформаційній системі ризиків. Система "Гриф" враховує більше ста параметрів та аналізує особливості практичної реалізації інформаційної системи. Застосування такої програми дозволяє провести комплексний аналіз ризиків та забезпечити максимальний рівень захисту від можливих загроз.

Принцип роботи програми "Гриф" полягає в аналізі можливих загроз конфіденційності, цілісності та доступності інформації. В результаті, можна визначити можливі збитки через різноманітні загрози та встановити їх вартість. Згідно з принципом "мінімізації збитків", вартість можливих збитків повинна бути меншою чи дорівнювати вартості інформації. Таким чином, програма "Гриф" є ефективним інструментом для забезпечення інформаційної безпеки компаній та організацій, які мають значну кількість інформації, яку необхідно захистити від потенційних загроз.

Однією з основних мет системи "Гриф" є можливість для IT-менеджера самостійно оцінити рівень ризиків в інформаційній системі та ефективність застосованої практики щодо забезпечення безпеки компанії. Це дає можливість керівництву компанії бачити цифрові докази необхідності інвестування у сферу інформаційної безпеки, а також допомагає коштом оптимізувати систему захисту.

Система "Гриф" дозволяє провести детальний аналіз всіх складових інформаційної системи, виявити потенційні загрози та врахувати актуальні ризики. Крім того, вона надає можливість перевірити ефективність заходів з захисту та рекомендує шляхи поліпшення за результатами оцінки.

Завдяки цим функціональним можливостям, IT-менеджер може легко оцінити ризик за умовами конкретної інформаційної системи та розуміти, які заходи слід вживати для запобігання можливих загроз. Якщо ризики виявляться значними, система "Гриф" надає цифрові докази доцільності інвестицій у сферу інформаційної безпеки компанії, що допомагає правильно спрямувати ресурси компанії та підвищити рівень захисту. Таким чином, система "Гриф" є важливим інструментом для забезпечення інформаційної безпеки підприємств та організацій.

Комплексний засіб "Гриф" дозволяє проводити аналіз ризиків інформаційної безпеки шляхом побудови моделі інформаційної системи організації. При цьому враховується взаємозв'язок ресурсів з цінною інформацією, вплив прав доступу груп користувачів, та забезпечується аналіз захищеності кожного виду інформації. Методика оцінки ризиків на основі засобу "Гриф" дозволяє вибирати відповідні засоби захисту з урахуванням специфіки підприємства. Використання цієї методики не потребує значних затрат часу та коштів на навчання фахівців та структурування даних.

Оцінка рівня захищеності інформаційної системи ТОВ "Перша українська газонафтова компанія" може бути проведена з використанням даної методики.

Вона дає можливість визначити можливі загрози, що стосуються конфіденційності, цілісності та доступності інформації, а також порекомендувати ефективні заходи щодо її захисту.

Важливою перевагою цієї методики є можливість змінювати параметри інформаційних ресурсів відповідно до специфіки підприємства. Іншими словами, програма «Гриф» може бути адаптована для структурованих потреб ТОВ "Перша українська газонафтова компанія". Оцінка ризику інформаційної безпеки з використанням цієї методики дозволить компанії проактивно працювати над поліпшенням своєї захищеності та зменшенням можливих ризиків.

Після проведення дослідження стану інформаційної безпеки з використанням програми "Гриф", можна узагальнити, що рівень захищеності інформації в ТОВ "Перша українська газонафтова компанія" знаходиться на достатньо високому рівні. Проте, недоліками системи захисту є недостатня захищеність програмного забезпечення від хакерських атак, оскільки підприємство використовує застарілі версії програм для захисту своєї інформації.

Інформаційно-аналітична робота в ТОВ "Перша українська газонафтова компанія" є однією з основних внутрішньовиробничих функціональних складових безпеки підприємства. Її метою є забезпечення ефективного інформаційно-аналітичного забезпечення господарської діяльності ТОВ "Спільне підприємство «Перша українська газонафтова компанія»".

Служби ТОВ "Перша українська газонафтова компанія" виконують функції збору та аналізу інформації, прогнозування тенденцій у різних сферах, оцінки економічної безпеки, розробки рекомендацій для підвищення рівня безпеки. Ці функції допомагають забезпечити захист інформаційних активів від зовнішніх загроз та ризиків. У ТОВ "Спільне підприємство «Перша українська газонафтова компанія»" постійно надходять потоки інформації, які можна

розділити на відкриту офіційну, вірогідну нетаємну отриману через неформальні контакти працівників з носіями такої інформації.

Для ефективного розроблення структури служби інформаційної безпеки на ТОВ «Перша українська газонафтова компанія» необхідно провести детальний аналіз політики безпеки, визначити ймовірні загрози та можливі втрати у разі їх реалізації, оцінити ефективність існуючої системи захисту інформації та фінансові витрати на заходи з її покращення. Тільки після такого аналізу керівництво підприємства зможе обґрунтовано прийняти рішення щодо створення необхідної структури служби інформаційної безпеки, яка має відповідну складову та належне оснащення засобами безпеки. Розробка та впровадження такої структури є важливим етапом у забезпеченні захисту інформаційних активів підприємства та виконанні завдань ефективного функціонування в сучасному цифровому середовищі.

Політика верхнього рівня в ТОВ "Перша українська газонафтова компанія" залежить від цілей, які формулюються організаціями в сфері інформаційної безпеки. Зазвичай такі цілі описують цілісність, доступність та конфіденційність. Якщо компанія підтримує критично важливі бази даних, то на першому плані може стояти зменшення втрат, пошкоджень або спотворень даних. Для компаній, що надають послуги, може бути важливо мати актуальну інформацію про ціни та доступність послуг для максимального числа потенційних клієнтів. Режимні організації зосереджуються на захисті від несанкціонованого доступу та забезпеченні конфіденційності інформації. Враховуючи ці цілі, ТОВ "Перша українська газонафтова компанія" може визначити свою політику безпеки і відповідні заходи для захисту своїх інформаційних активів від різних загроз та ризиків.

провадження політики інформаційної безпеки на верхньому рівні в ТОВ "Перша українська газонафтова компанія" повинне відповідати державних законам та нормативним актам. Для забезпечення точного та відповідального

виконання цієї політики персонал підприємства може бути заохочений або покараний, якщо необхідно. Однак, на верхній рівень слід виносити лише найбільш важливі питання з інформаційної безпеки, щоб забезпечити ефективність та простоту в управлінні цими питаннями. На середній рівень можуть бути виділені окремі аспекти інформаційної безпеки, які є важливими для різних систем, які використовує організація. Впровадження цієї структури допоможе забезпечити ефективне функціонування інформаційної безпеки в ТОВ "Перша українська газонафтова компанія" та дозволить підвищити рівень захисту її інформаційних активів.

У ТОВ "Перша українська газонафтова компанія" політика середнього рівня щодо кожного аспекту інформаційної безпеки передбачає розроблення відповідного управлінського рішення, яке містить детальний опис аспекту та його застосування. Для прикладу, якщо користувачі використовують неофіційне програмне забезпечення, то про це повинна бути обов'язкова інформація в цьому документі, оскільки таке програмне забезпечення не схвалене та не закуплене на рівні організації. Крім того, слід чітко визначити область застосування даної політики інформаційної безпеки, де, коли, як і по відношенню до кого і чого вона буде застосовуватися. Важливо мати чіткий розподіл ролей та відповідальності для проведення політики безпеки в життя. У "політичний" документ необхідно включити інформацію про посадових осіб, які відповідають за забезпечення інформаційної безпеки. Крім цього, механізм забезпечення законності повинен бути введений у дію, щоб переконатися в тому, що політика відповідає всім державним законам та нормам. Розробка та впровадження такого рішення є важливим етапом у забезпеченні ефективного функціонування інформаційної безпеки в ТОВ "Перша українська газонафтова компанія".

У ТОВ "Перша українська газонафтова компанія" політика безпеки нижнього рівня належить до конкретних сервісів, які включають всього два

аспекти: мету та правила їх досягнення. Це може часто викликати складнощі при окремому визначенні такої політики від питань реалізації, особливо при наданні послуг з інформаційного забезпечення. У порівнянні з двома верхніми рівнями, політика на нижньому рівні може бути набагато більш детальною. Оскільки окремі сервіси можуть мати свої власні специфічні питання, які не можна регулювати єдиним чином в рамках всієї організації.

Часто ці питання стосуються контролю доступу до даних, захисту від злому та вірусів, а також збереження конфіденційності інформації. Рішення, пов'язані з цими питаннями, повинні бути прийняті на управлінському, а не технічному рівні, оскільки вони настільки важливі для забезпечення режиму безпеки. Враховуючи велику кількість специфічних питань, організація повинна створювати детальний план дій для кожного сервісу та відповідно запроваджувати політику безпеки, що буде покривати всі можливі ризики і загрози.

Така політика безпеки нижнього рівня допоможе забезпечити захист інформаційних активів підприємства на всіх рівнях доступу до даних. Крім того, вона дозволяє підприємству оперативно та ефективно реагувати на потенційні загрози та ризики, що можуть виникнути в процесі надання послуг з інформаційного забезпечення.

У другому розділі було проведено детальний аналіз діяльності ТОВ "Перша українська газонафтова компанія" з визначенням основних принципів та методів забезпечення інформаційної безпеки на підприємстві, а також оцінено стан забезпечення інформаційної безпеки. Важливим кроком є формулювання конкретних цілей та правил безпеки, щоб запобігти неправильному використанню інформації та зберегти її конфіденційність, цілісність та доступність.

Політика безпеки повинна розвиватися та оновлюватися залежно від потреб і викликів часу. Наприклад, якщо мова йде про систему оплати праці,

можна поставити мету, що лише працівникам відділу кадрів та бухгалтерії дозволяється вводити та змінювати інформацію. Завдяки конкретним цілям встановлюються правила безпеки, що допомагають захистити інформаційні активи від зовнішніх загроз та ризиків.

Отже, для ефективної організації політики безпеки у ТОВ "Перша українська газонафтова компанія", керівництву необхідно знайти оптимальний компроміс, який забезпечить належний рівень інформаційної безпеки, при цьому маючи врахувати фінансові можливості підприємства.

3. УДОСКОНАЛЕННЯ МЕТОДІВ ТА РОЗРОБКА МОДЕЛІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

3.1. Принципи захисних заходів від несанкціонованого доступу в автоматизованих системах.

Управління електронним документообігом базується на зрозумілих для користувачів електронних документах, які містять вказівки щодо роботи з ними. Електронний документообіг покликаний стати одним з основних інструментів управління документами, які представлені в електронному форматі, допомагаючи впроваджувати концепцію "безпаперового" офісу. [42, с. 145].

Системи електронного документообігу представляють собою складний комплекс технічних і організаційних рішень, які допомагають зберігати та раціонально використовувати людські ресурси, а також підвищувати ефективність управління потоками корпоративних документів та інформації. Ці системи дозволяють автоматизувати процеси обробки документів та забезпечують швидкий доступ до необхідної інформації, що сприяє оптимізації робочих процесів та підвищенню продуктивності працівників. Такий підхід дозволяє керівництву організації більш ефективно використовувати свої ресурси та значно покращити якість роботи всього колективу. [38, с. 12].

Використання систем електронного документообігу в ТОВ "Перша українська газонафтова компанія" має безліч переваг, таких як збільшення продуктивності праці персоналу на 20-25%, зниження вартості архівного збереження електронних документів на 80% порівняно із збереженням паперових архівів та звільнення фізичного місця для їх зберігання. Також це дозволяє зменшити витрати на копіювання і доставку документів у паперовому форматі, покращити контроль за виконанням документів та підвищити безпеку

інформації завдяки повноваженням доступу до неї. Крім того, колективна робота над документами стає можливою, що дозволяє більш ефективно співпрацювати. Застосування СЕД прискорює пошук і вибірку документів залежно від різних атрибутів, що економить час на обробку документів та поліпшує документальну підтримку роботи з клієнтами і діловими партнерами.

Перед впровадженням системи електронного документообігу (СЕД) в ТОВ "Перша українська газонафтова компанія", необхідно ретельно оцінити готовність всіх суб'єктів до нових інформаційних технологій. СЕД забезпечує автоматизацію традиційних діловодних процесів та підтримує безпеку і автентичну ідентифікацію при роботі з документами, повнотекстовий пошук, архівацію та історію змін документів. Проте, впровадження СЕД може стикнутися зі складнощами через те, що ці системи пропонують рішення менш очевидних і більш комплексних задач. Величезна складність задачі може недооцінюватися керівництвом компанії, а також її вартість може збільшуватися через складне програмне забезпечення. Це може призвести до того, що покупці систем можуть віддалятися від впровадження СЕД через відсутність готовності до такого рівня складності. Отже, перед впровадженням СЕД необхідно виважено оцінювати готовність та здатність компанії до адаптації нових технологій, а також розуміти, що впровадження СЕД може відображатися на всіх рівнях управління компанії.

Для успішного впровадження платформи комплексної автоматизації документообігу в ТОВ "Перша українська газонафтова компанія" потрібно сформувати принципи: 1) повне усвідомлення необхідності вирішення задач в області автоматизації документообігу для покращення керованості організації; 2) наявність волі керівництва та розуміння тривалості та складнощів впровадження системи; 3) наявність кваліфікованих кадрів для координації розробки та впровадження програм. Автоматизація паперового документообігу є лише проміжним рішенням, а електронний документообіг та комплексна

автоматизація забезпечують швидку та точну обробку документів та допомагають уникнути помилок та зменшити час на їх обробку. Впровадження нової системи може бути складним та тривалим процесом, але це необхідно для подальшого розвитку та успіху компанії.

Автоматизація документообігу є важливим питанням для будь-якої організації та залежить від багатьох факторів, таких як характер комерційної діяльності, інфраструктура та адміністративна організація. У ТОВ "Перша українська газонафтова компанія" вже використовується система оперативного управління підприємством "Мотив", яку використовують більше 1200 компаній для ведення електронного архіву, управління проектами та взаємодії з клієнтами.

Система "Мотив" містить в собі автоматизовану систему контролю виконання доручень, яка є однією з ключових компонентів цього програмного продукту. Вона входить до складу Web-орієнтованих додатків та може бути дуже потужним інструментом управління для будь-якої організації. Цей продукт поєднує в собі можливості ефективної організації спільної роботи співробітників (workflow) та управлінні електронними документами. Завдяки такому підходу, можна значно поліпшити керування організацією та забезпечити швидку та точну обробку документів.

Проте слід мати на увазі, що впровадження нових систем може бути складним та тривалим процесом. Необхідно ураховувати особливості конкретної організації та забезпечувати необхідний рівень навчання працівників. Однак, впровадження нових технологій є необхідним для подальшого розвитку та успіху компанії в майбутньому, оскільки забезпечує більш ефективне функціонування та зменшення витрат на обробку документів та їх архівацію [27].

Система "Мотив" автоматизує створення доручень і завдань, контролює їх виконання та надає звіти про діяльність співробітників, підрозділу або компанії.

Її можна інтегрувати з електронною поштою та корпоративним порталом, автоматично сортує завдання за відповідальними співробітниками і має розсилку email-оповіщень та SMS. Інтерфейс системи простий у розумінні, не потребує великих витрат на навчання персоналу та дозволяє проводити роботу з документами та завданнями у більш точному та ефективному режимі. Впровадження системи "Мотив" підвищує ефективність та точність роботи з документами та дорученнями, знижує витрати часу та зусиль на їх обробку, поліпшує керування діяльністю окремих співробітників та всього підрозділу. [37].

Автоматизована система "Мотив" дозволяє керівному складу організувати строгу структуру підпорядкованості персоналу, контролювати своєчасне виконання завдань та створювати робочі групи для вирішення окремих завдань. Збір статистики за діяльністю співробітників допомагає керівництву оперативно реагувати на труднощі, що виникають під час вирішення поставлених завдань, що в свою чергу забезпечує високий рівень управління і тактичного планування, необхідний для отримання виробничого прибутку та подальшого розвитку компанії.

Автоматизована система "Мотив" є значним придбанням для ТОВ "Перша українська газонафтова компанія". Вона має безліч переваг, таких як відсутність серверної ліцензії та прихованих платежів, дешева безстрокова ліцензія COMPLETE, максимальний комплект поставки для кожної ліцензії, можливість поєднання функціональності кількох систем в одному продукті, швидке та недороге впровадження, інтуїтивно зрозумілий інтерфейс, можливість самостійного впровадження та подальшої підтримки в зручному графічному інтерфейсі та легке адміністрування.

При цьому впровадження АС "Мотив" спроможна значно прискорити та контролювати процес виконання завдань, впливати на підготовку, узгодження і виконання документів. Крім того, для 100 активних користувачів достатньо

мати лише штатного системного адміністратора, що дозволяє знизити витрати на обслуговування системи.

Незважаючи на всі переваги, слід мати на увазі, що впровадження нової системи може бути складним процесом, тому необхідно провести детальний аналіз потреб компанії та забезпечити необхідний рівень навчання працівників. Проте, попри ці труднощі, впровадження автоматизованої системи "Мотив" є ключовим чинником розвитку та успіху організації в майбутньому.

В ТОВ "Перша українська газонафтова компанія" захист від несанкціонованого доступу до документів є ключовим фактором. Адміністратор системи захисту інформації розрізняє пасивні об'єкти (файли, програми, термінали) від активних суб'єктів, які можуть виконувати операції над ними. Захист об'єктів здійснюється за допомогою контролю за виконанням правил, які регламентують операції.

Автоматизована система "Мотив" містить політику безпеки, яка включає в себе політику мережевої безпеки і безпеки паролів. Адміністратор задає фільтри для контролю доступу до системи користувачів з різних ділянок мережі. Доступ до системи визначається відповідно до параметрів, заданих для довірених вузлів, заборонених вузлів та інших вузлів на мережі.

Якщо параметри входу користувача потрапляють під параметри, зазначені в списку заборонених вузлів або в інших вузлах встановлено заборону для всіх користувачів - доступ до системи заборонено. Якщо параметри входу користувача потрапляють під параметри, зазначені в списку довірених вузлів або в інших вузлах встановлено дозвіл для всіх користувачів - доступ до системи дозволений.

Застосування автоматизованої системи "Мотив" дозволяє забезпечити безпеку даних та документів, що зберігаються в системі, і контролювати доступ до них. Це особливо важливо для ТОВ "Перша українська газонафтова

компанія", оскільки такий підхід до захисту даних та документів дозволяє запобігти несанкціонованому доступу до конфіденційної інформації.

У разі, коли параметри входу користувача потрапляють одночасно і в заборонені, і дозволені, то доступ до системи визначається параметрами Інших вузлів. Така система контролю доступу допомагає забезпечити безпеку ресурсів операційної системи "Мотив" в ТОВ "Перша українська газонафтова компанія".

Доступ до ресурсів обмежується за допомогою паролів, які можуть бути використані як ключ для шифрування-дешифрування інформації в користувацьких файлах. Паролі зберігаються в зашифрованому вигляді, що ускладнює їх виявлення та використання зловмисниками. Користувачі можуть змінювати свої паролі самостійно або за допомогою адміністратора системи. Крім того, сама система може вимагати зміни пароля через встановлений інтервал часу.

Загалом, АС "Мотив" в ТОВ "Перша українська газонафтова компанія" має чітке розмежування доступу користувачів до системи, щоб запобігти несанкціонованому доступу до важливих даних та документів, що містяться в системі. Така система контролю доступу сприяє забезпеченню безпеки та конфіденційності даних у підприємстві.

3.2 Засоби забезпечення захисту інформації в автоматизованих інформаційних

У автоматизованих інформаційних системах ТОВ "Перша українська газонафтова компанія" використовуються стандартне та спеціалізоване обладнання та програмне забезпечення для захисту інформації. Ці функції включають захист цілісності і конфіденційності даних, а також обмеження доступу до них за допомогою спеціальних компонентів системи.

Автоматизована інформаційна система є об'єктом інформаційної безпеки, тому в процесі її функціонування не можна дозволяти появу нових функцій. Для забезпечення цього необхідно забезпечити цілісність системи в момент запуску та в процесі її роботи.

Особлива увага приділяється аутентифікації користувача. Система ідентифікує користувача, перевіряє його повноваження та виконує запит на обробку інформації. Надійність захисту інформації в АІС визначається переліком і властивостями функцій, методами, які використовуються у функціях, та способом їх реалізації.

При оцінці конкретної системи слід звернути увагу на методи і спосіб реалізації ключових функцій, таких як аутентифікація та перевірка цілісності системи. Важливо забезпечити надійний захист інформації в АІС шляхом використання спеціалізованого обладнання та програмного забезпечення, що відповідає класу захищеності системи. [24, с. 43].

У ТОВ "Перша українська газонафтова компанія" більшість функцій сучасних комп'ютерних систем реалізовані у вигляді програм, що може створювати проблеми з їх цілісністю в процесі запуску та функціонування. Без додаткового обладнання можлива атака на програмне забезпечення, оскільки багато користувачів вміє програмувати та має розуміння операційних систем і помилок, які в них виникають.

Перевірка цілісності програм не може бути надійною, якщо вона здійснюється програмним шляхом за допомогою інших програм, оскільки результатами перевірки неможливо довіряти, якщо самі програми та їх перевірка знаходяться на одному носії. Чисто програмним способом неможливо забезпечити надійну цілісність системи, тому необхідно підходити до програмних систем захисту від НСД з особливою обережністю.

Тому в ТОВ "Перша українська газонафтова компанія" необхідно дотримуватися правильної політики безпеки програмного забезпечення, такої як

перевірка походження та цілісності програм, використання підписів та шифрування для забезпечення конфіденційності, тестування на безпеку перед використанням, а також швидко виправляти виявлені вразливості. Тільки таким чином можна забезпечити високий рівень захисту від НСД в комп'ютерних

Для забезпечення криптографічного захисту в ТОВ "Перша українська газонафтова компанія" використовують плати серії "Криптон", які забезпечують захист ключів шифрування та електронного цифрового підпису, а також забезпечують незмінність алгоритму шифрування та електронного цифрового підпису. Електронний цифровий підпис використовується для підтвердження цілісності та ідентифікації підписувача, а накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Таким чином, в ТОВ "Перша українська газонафтова компанія" використовуються найсучасніші апаратні та програмні засоби для забезпечення безпеки та цілісності системи, що дозволяє захищати важливу інформацію від несанкціонованого доступу та забезпечувати надійну роботу комп'ютерної системи в цілому. [28, с. 1].

Криптографічний захист інформації є важливим елементом політики безпеки комп'ютерної системи в ТОВ "Перша українська газонафтова компанія". Особистий ключ є параметром криптографічного алгоритму формування електронного цифрового підпису, до якого має доступ тільки підписувач. Відкритий ключ же є параметром криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису.

В сучасному світі безпека даних та інформації є вельми важливою темою, тому захист від несанкціонованого доступу до комп'ютерних систем є ключовим фактором. Щоб забезпечити безпеку, можна використовувати криптографічний захист інформації при побудові політики безпеки

комп'ютерної системи. Однак, важливо мати належно розроблену та безпечну систему розподілу криптографічних ключів.

У таких системах ключі можуть бути зашифровані в майстер-ключі та зберігатися на зовнішньому носії в зашифрованому вигляді. При цьому ключі розшифровуються лише всередині плати, що дозволяє забезпечити їх безпеку. Також можна використовувати функції доступу на персональний комп'ютер, що виконуються до завантаження операційної системи, та апаратні функції блокування портів ПК для частково контрольованих систем.

Криптографічні методи захисту інформації полягають в шифруванні даних та є ефективним засобом захисту від несанкціонованого доступу до конфіденційної інформації. Важливо розуміти, що захист від несанкціонованого доступу до комп'ютерних систем - це постійний процес, який потребує регулярного оновлення та підтримки.

Основна мета шифрування (кодування) інформації полягає у захисті її від несанкціонованого доступу та читання. Системи криптографічного захисту (системи шифрування інформації) для онлайн-банківських систем можуть бути розподілені за різними ознаками.

По-перше, вони можуть бути вбудованими у систему або додатковим механізмом, який може бути відключений. По-друге, системи криптографічного захисту можуть бути реалізовані апаратно, програмно або програмно-апаратно. По-третє, системи можуть використовувати загальні чи спеціальні криптографічні алгоритми.

По-четверте, системи криптографічного захисту можуть мати різноманітні цілі захисту, наприклад, забезпечення конфіденційності інформації (шифрування), захист повідомлень та даних від модифікації, контроль доступу та привілеїв користувачів тощо. Нарешті, системи можуть використовувати різні методи розподілу криптографічних ключів, такі як базові/сеансові ключі, відкриті ключі та інші.

Вбудовані механізми криптографічного захисту входять до складу системи та розробляються одночасно з системою. Такі механізми можуть бути окремими компонентами системи або розподілятися між іншими компонентами системи, залежно від їх призначення та функціональності. [31].

Додаткові механізми криптозахисту - це додаткові програмні або апаратні засоби, які не входять до складу системи. Це надає значну гнучкість та можливість швидкої заміни. Для більш ефективного захисту інформації рекомендується використовувати комбінацію додаткових і вбудованих механізмів криптографічного захисту.

Забезпечення криптографічного захисту є важливою складовою безпеки даних та інформації. В залежності від способу реалізації, криптографічний захист можна здійснювати різними способами: апаратним, програмним або програмно-апаратним.

Апаратна реалізація криптографічного захисту є найбільш надійним, оскільки забезпечує захист ключів від перехоплення та підробки інформації під час передачі. Однак, цей спосіб є найбільш дорогим.

Програмна реалізація криптографічного захисту є більш доступною та гнучкою в реалізації, але виникають питання щодо захисту криптографічних ключів від перехоплення під час роботи програми та після її завершення. Також потрібно вживати заходів для забезпечення повного звільнення пам'яті від криптографічних ключів, наприклад, через "збирання сміття".

Комбінування апаратних і програмних механізмів криптографічного захисту є одним з найбільш поширених способів. Програмна реалізація криптоалгоритмів з апаратним зберіганням ключів є досить надійним і не надто дорогим методом. Однак, при використанні апаратних засобів для зберігання криптографічних ключів, необхідно пам'ятати про захист від перехоплення ключів під час їх зчитування з носія та використання в програмі.

Криптографічний алгоритм - це математична функція, яка використовується для шифрування повідомлень та іншої зрозумілої інформації. Криптоалгоритми можна розділити на дві групи: загальні та спеціальні.

Спеціальні криптоалгоритми характеризуються таємним алгоритмом шифрування, що ускладнює їх злам. Ці алгоритми часто використовуються в апаратних засобах криптозахисту.

Загальні криптоалгоритми мають відкритий алгоритм, при цьому їх криптостійкість залежить від ключів шифрування. Такі алгоритми стають стандартами шифрування, якщо їхня криптостійкість доведена. Зазвичай ключі генеруються методом випадкових чисел та не можуть повторюватись протягом певного часу. Криптостійкість загальних алгоритмів збільшується зі збільшенням довжини ключа.

Захист від несанкціонованого доступу до криптографічних ключів є важливим елементом криптозахисту. Ключі можуть бути зашифровані та зберігатися на зовнішньому носії в зашифрованому вигляді. При цьому ключі можуть бути розшифровані лише всередині плати, що забезпечує їх безпеку.

Існують дві великі групи загальних криптоалгоритмів: симетричні та асиметричні. Симетричні криптографічні алгоритми використовують один і той самий ключ для шифрування та розшифрування повідомлення, що забезпечує досить високу швидкість обробки як для апаратної, так і для програмної реалізації. Однак недоліком цих алгоритмів є складнощі, пов'язані з безпечним розподілом ключів між користувачами системи.

До асиметричних криптоалгоритмів належать ті, для яких шифрування та розшифрування виконуються за допомогою різних ключів. Це означає, що маючи один ключ, неможливо визначити парний до нього ключ. Такі алгоритми можуть потребувати значно більше часу для обробки, проте не створюють складнощів під час розподілу ключів, оскільки відкритий розподіл одного з

ключів не зменшує криптостійкості алгоритму та не дає можливості відновлення парного ключа.

Криптографічні алгоритми можна використовувати з різними цілями, включаючи шифрування повідомлень для приховування змісту та забезпечення захисту даних від модифікації.

Шифрування даних є важливою складовою криптографічного захисту інформації. Серед найпоширеніших методів шифрування можна виділити симетричні алгоритми, такі як DES та ГОСТ 28147-89, що використовують один ключ для шифрування та розшифрування повідомлення. Для підвищення ступеня захисту може використовуватись алгоритм Потрійний DES, який запропонований як альтернатива DES та передбачає триразове шифрування даних трьома різними закритими ключами.

До інших симетричних алгоритмів можна віднести RC2, RC4 та RC5, що забезпечують швидке шифрування великих обсягів інформації та можуть підвищувати ступінь захисту через вибір.

Асиметричні алгоритми, такі як RSA та Ель-Гамаль, використовують різні ключі для шифрування та розшифрування повідомлення та не створюють складнощів з безпечним розподілом ключів. Однак, вони можуть потребувати значно більше часу для обробки, що може ускладнювати роботу з великими об'ємами даних.

Вибір методу шифрування залежить від конкретних вимог до захисту інформації, а також від доступних ресурсів та можливостей системи. Криптографічний захист може бути забезпечений як програмним, так і апаратним шляхом, а також комбінованою реалізацією засобів захисту. В будь-якому випадку, важливо дотримуватись всіх необхідних вимог до безпеки при роботі з конфіденційною інформацією.

Для шифрування повідомлень можна використовувати різні криптографічні алгоритми, такі як IDEA, DES, або ГОСТ 28147-89. Деякі

алгоритми (наприклад, RSA) можуть виконувати шифрування даних у різних режимах, за допомогою таємного ключа відправника, відкритого ключа отримувача, або комбінації цих ключів.

Крім шифрування повідомлень, криптографічні методи можуть використовуватись для захисту інформації від модифікації, викривлення або підробки. Для цього можна використовувати код автентифікації для симетричних алгоритмів та електронний цифровий підпис для асиметричних алгоритмів. Обидва методи використовують спеціальні алгоритми для формування та перевірки інформації, що дозволяє однозначно довести її невідомість або незмінність після передачі по мережі.

Захист конфіденційної інформації та ресурсів систем став вельми актуальним у сучасному інтернеті. З цією метою, компанії все частіше використовують електронний цифровий підпис. Для забезпечення надійного захисту систем інформації від криптографічних атак, необхідний безпечний розподіл ключів між всіма учасниками системи.

Два основних методи розподілу ключів - метод базових/сеансових ключів та метод відкритих ключів. Перший метод використовується для розподілу ключів симетричних алгоритмів шифрування. Для його введення потрібна ієрархія ключів, де головний ключ і ключ шифрування даних є основними елементами. Другий метод може використовуватись як для симетричного, так і для асиметричного шифрування і забезпечує актуальний розподіл ключів між учасниками системи.

Під час використання електронного цифрового підпису потрібно створити відкритий та особистий ключі, а після генерації ключової пари розповсюдити відкритий ключ респондентам. Найнадійнішим способом розповсюдження є через сертифікаційні центри, де цифровий сертифікат може підтвердити справжність особи користувача та зберігатись як електронне підтвердження відкритих ключів.

Отже, щоб ефективно захистити автоматизовані системи від несанкціонованого доступу, в «Перша українська газонафтова компанія» потрібні не лише програмні, але й апаратні засоби криптозахисту. Таким чином, використання електронного цифрового підпису та правильний розподіл ключів є важливими елементами захисту від будь-яких криптографічних алгоритмів.

3.3 Методи захисту електронної корпоративної інформації в «Перша українська газонафтова компанія»

Сучасні підприємства дуже чутливі до захисту своєї електронної корпоративної інформації. Отже, безпека електронних систем необхідна для їх захисту від можливих збитків для власників та користувачів у разі навмисного або ненавмисного завдання шкоди. Різноманітні впливи на систему наведені на рисунку 3.1.

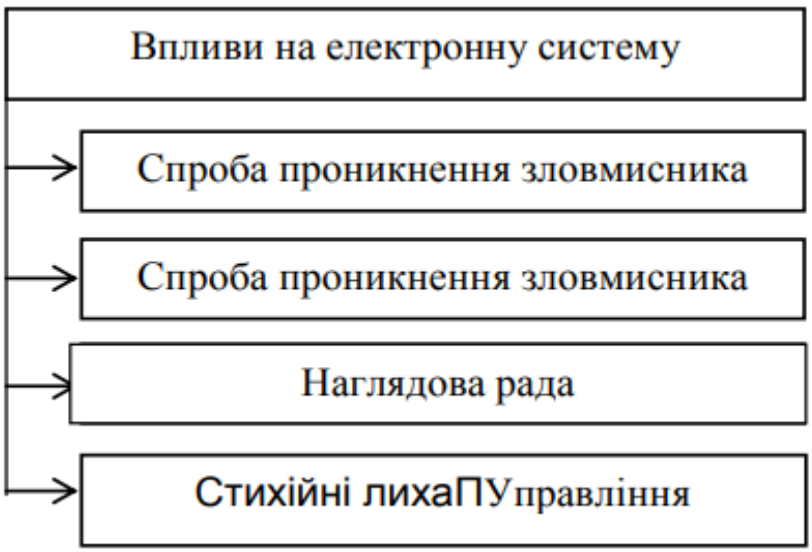

Рисунок 3.1 – Основні види впливів на електронну систему в ТОВ «Перша українська газонафтова компанія»

ТОВ "Перша українська газонафтова компанія" вкладає значні зусилля у забезпечення як внутрішньої, так і зовнішньої безпеки їх електронної системи. Внутрішня безпека передбачає захист від стихійного лиха, можливого проникнення зловмисника, неправомірного доступу до носіїв інформації та можливих збоїв системи. Основним завданням внутрішньої безпеки є забезпечення надійної та правильної роботи електронної системи, а також збереження цілісності програм та даних.

Проведений аналіз показує, що на даному підприємстві використовуються два основних підходи до забезпечення безпеки електронної системи. Перший полягає в проведенні систематичних перевірок та контрольних механізмів для запобігання можливих загроз зсередини системи. Другий підхід передбачає встановлення спеціальної програмної та апаратної захисту для забезпечення надійної оборони від зовнішніх загроз. Обидва підходи використовуються для забезпечення гарантії безпеки електронної системи на підприємстві.

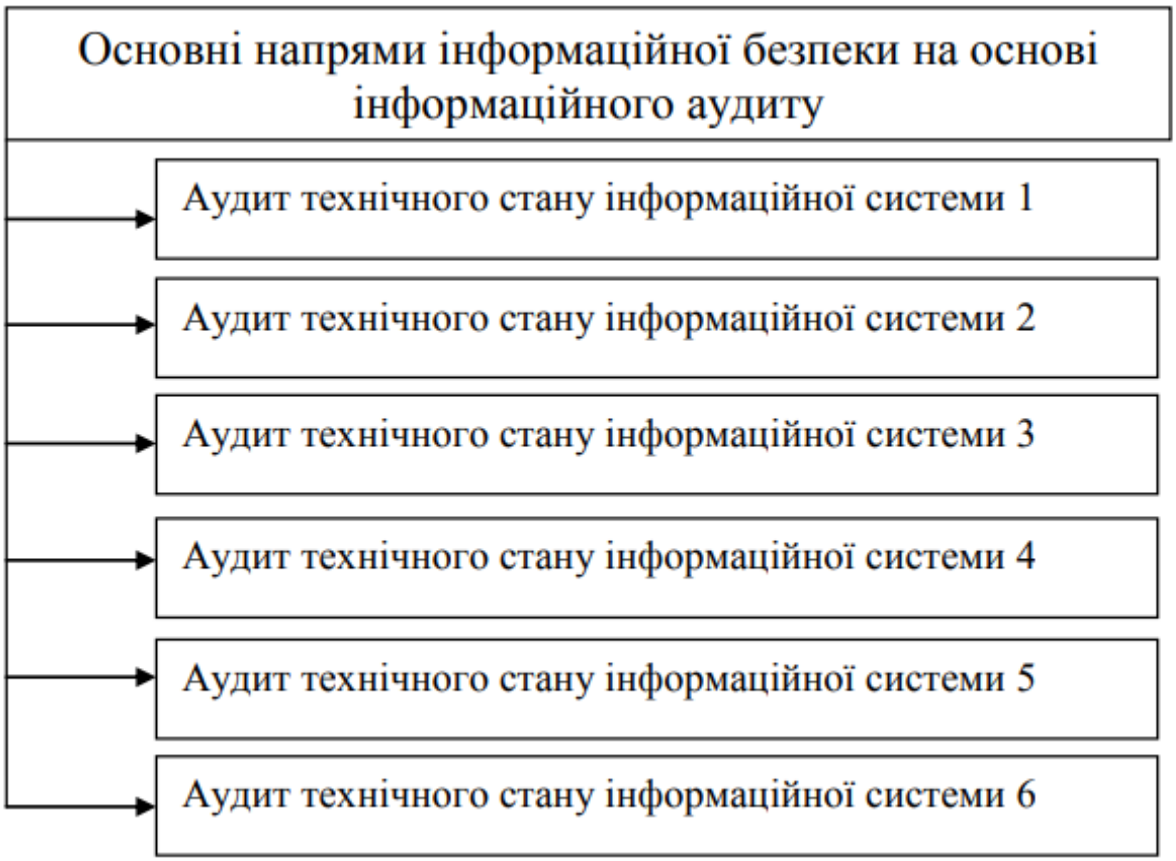

Рисунок 3.2 – Основні підходи до гарантування безпеки електронних систем в ТОВ «Перша українська газонафтова компанія» [складено автором за (23, с. 207)

В ТОВ "Перша українська газонафтова компанія" використовується комплексний підхід до захисту великих електронних систем. Хоча програмні засоби, такі як АС "Мотив" та 1С мають вбудовані засоби захисту інформації, це не досить для гарантування безпеки системи. Організаційні та технічні заходи повинні включати контроль за персоналом з високим рівнем повноважень, проведення резервного копіювання критично важливої інформації, заходи відновлення працездатності системи у разі непередбачуваних ситуацій, управління доступом до приміщень з обчислювальною технікою та фізичний захист приміщень.

Аналізуючи ситуацію в світі щодо стандартизації інформаційної безпеки протягом років розвитку індустрії ІБ, можна виділити такі періоди: поява стандартів (198-1995 роки), випробування практикою (1996-2000 роки) та "виживання сильних" (від 2001 року й дотепер). Перші етапи характеризувалися природним розвитком інформаційних технологій і формуванням понятійного апарату та основних підходів у сфері ІБ. Поява великої кількості різноманітних стандартів відбувалася як в окремих компаніях, так і в авторитетних інститутах, як NIST та ISO. Сучасний етап "виживання сильних" полягає в постійному вдосконаленні заходів захисту від загроз та атак на електронні системи.

ТОВ "Перша українська газонафтова компанія" використовує комплексний підхід до захисту своїх електронних систем, але зазначається, що стандартизація в сфері інформаційної безпеки досить обмежена та має природні недоліки. Для другого та третього етапів розвитку стандартизації характерним було вже практичне застосування стандартів та їх природний відбір, що сприяло визнанню основоположних стандартів, таких як ISO 15408 та ISO 27001/17799, міжнародними. Однак, існує розщеплення на дві географічно незалежні з огляду на стандартизацію зони: Європа та Азія визнають стандарти ISO, тоді як США вважає за краще використовувати стандарти NIST.

Зазначається, що найбільш відомі стандарти ISO мають свою основу у BSI. В 1985 році Національний центр комп'ютерної безпеки Міністерства оборони США опублікував "Помаранчеву книгу", де було систематизовано підходи до гарантування безпеки інформаційних систем та методів захисту від загроз безпеці інформаційних систем. Ця книга стала еталоном для безпеки інформаційних систем.

Отже, можна зробити висновок, що стандартизація в сфері інформаційної безпеки є складним та постійно розвиваючимся процесом, і визнання основних підходів та стандартів є важливим кроком до забезпечення безпеки електронних систем.

У 1985 році "Помаранчева книга", яку опублікував Національний центр комп'ютерної безпеки Міністерства оборони США, внесла у стандарти поняття "політика безпеки". Це поняття стало загальноприйнятим та застосовується для опрацювання, зберігання та розподілу критичної інформації всередині інформаційної системи. Політика безпеки не обмежується апаратно-програмним комплексом, а також включає обслуговуючий персонал.

Формування політики безпеки базується на аналізі поточного стану та можливих загроз для інформаційної системи. Такий аналіз допомагає визначити мету, завдання та пріоритети системи безпеки, галузь дії окремих підсистем, гарантований мінімальний рівень захисту, обов'язки персоналу щодо забезпечення захисту та санкції за порушення захисту. Якщо політика безпеки не проводиться повністю або непослідовно, то збільшується ймовірність порушення захисту інформації.

Для формування політики безпеки необхідно провести аналіз ризиків, що допомагає підвищити рівень поінформованості про слабкі та сильні сторони захисту, створити базу для підготовки та прийняття рішень та оптимізувати розмір витрат на захист. Аналіз ризиків завершується підготовкою плану захисту, який включає поточний стан, вибір основних засобів захисту, відповідальність, розклад та перегляд положень, які потрібно періодично переглядати. У загальній системі гарантування безпеки захист інформації відіграє значну роль, а виділяють такі підходи до організації захисту: фізичні, законодавчі, управління доступом та криптографічне закриття.

Політика безпеки - це важливий аспект діяльності будь-якої організації, яка працює з конфіденційною інформацією. Вона передбачає застосування різноманітних методів та технологій для захисту даних від несанкціонованого доступу. Фізичний захист полягає у створенні перешкод для зловмисників, які намагаються отримати доступ до приміщення з апаратурою або носіями інформації. Однак цей підхід не захищає інформацію від внутрішніх загроз,

таких як порушення правил користування інформацією співробітниками організації.

Законодавчий захист передбачає встановлення законів, що регулюють використання та опрацювання інформації з обмеженим доступом, а також встановлюють міру відповідальності за порушення цих правил. Управління доступом - це система регулювання доступу до ресурсів системи, що включає технічні та програмні елементи баз даних. Регламентуються порядок роботи користувачів і персоналу, а також права доступу до окремих файлів в базах даних.

Усі напрями організації захисту інформації (фізичні, законодавчі, управління доступом, криптографічне закриття) повинні реалізовуватися механізмами безпеки на всіх рівнях еталонної моделі. Це дає змогу забезпечити максимальний рівень захисту інформації від всіх можливих загроз.

Однак, найважливішим фактором успішного захисту інформації є свідомість та дисципліна працівників. Правильна підготовка та навчання персоналу допоможуть уникнути більшості порушень та недбалості, що можуть призвести до компрометації даних. Тому культура безпеки має бути вбудована в кожен елемент діяльності організації, щоб забезпечити безпеку інформації та гарантувати успішну роботу.

Протоколи информационного обмена делятся на две группы: виртуального соединения и дейтаграммные. В соответствии с этими протоколами сети подразделяются на виртуальные и дейтаграммные. В виртуальных сетях информация между абонентами передается виртуальным каналом, проходя три этапа: создание (установление) виртуального канала, передача виртуального канала и уничтожение виртуального канала (разъединение). При этом сообщение разбивается на блоки (пакеты), которые передаются в порядке их расположения в сообщении.

В дейтаграммных сетях блоки сообщений передаются от отправителя к получателю независимо друг от друга и по различным маршрутам, поэтому порядок доставки блоков может не совпадать с порядком их расположения в сообщении.

Для защиты электронной корпоративной информации в ТОВ "Перша українська газонафтова компанія" следует использовать методы криптографического закрытия информации в компьютерных системах. Это наиболее эффективный способ защиты информации с высоким уровнем безопасности. Методы шифрования обеспечивают конфиденциальность информации и используются другими сервисными службами. Для использования механизмов криптографического закрытия информации в локальной вычислительной сети необходимо организовать специальную службу генерации ключей и их распределения между абонентами.

Рекомендуется использовать метод DEC (Data Encryption Standard), разработанный фирмой IBM и рекомендованный для использования Агентством национальной безопасности США. Алгоритм криптографической защиты известен и опубликован. Российский стандарт шифрования данных ГОСТ 28147-89 является единственным алгоритмом криптографического преобразования данных для больших информационных систем и не накладывает ограничений на степень секретности информации.

Для формальної моделі статусу захисту в операційній системі використовують матрицю доступу, яка містить m рядків (за кількістю суб'єктів) і n стовпців (за кількістю об'єктів). Кожен елемент матриці відповідає конкретному суб'єкту та об'єкту і містить інформацію про права доступу даного суб'єкта до цього об'єкту. Це може бути список операцій (читання, запис, виконання тощо), які суб'єкт може виконувати над об'єктом або значення, що вказують на рівень доступу (наприклад, "читання заборонено", "виконання дозволено").

Матриця доступу дозволяє оперативно контролювати та регулювати доступ до об'єктів в системі. Управління правами доступу до об'єктів здійснюється через надання користувачам різного рівня доступу до окремих об'єктів або групи об'єктів. Для цього встановлюються правила, які визначають, які суб'єкти можуть виконувати певні операції над об'єктами, та які об'єкти доступні для кожного суб'єкта.

Застосування матриці доступу в операційній системі дозволяє забезпечити захист об'єктів в системі, уникнути несанкціонованого доступу або внесення змін до об'єктів. При цьому, важливим є постійне оновлення матриці доступу та перегляд прав доступу до об'єктів в залежності від потреб користувачів та безпекових вимог. [31].

Для забезпечення ефективного захисту інформації у ТОВ «Перша українська газонафтова компанія» необхідно визначити політику безпеки, яка повинна бути повною та послідовною. При цьому, важливим є проведення аналізу ризику, який дозволить оцінити потенційні загрози та слабкі сторони захисту інформації.

Оптимальна політика безпеки має за мету зниження ризику порушення безпеки до прийнятного рівня. Для цього можуть бути використані різноманітні засоби та методи захисту, такі як комплексне застосування різних засобів і методів, створення структури захисту з кількома рівнями та їх постійне удосконалення.

При застосуванні паролів для обмеження доступу до ресурсів операційної системи важливо забезпечити їх збереження у зашифрованому вигляді, що утруднює їх виявлення і використання зловмисниками. Крім того, необхідно регулярно змінювати паролі та контролювати доступ користувачів до окремих об'єктів.

У межах програми захисту інформації важливим є також формування кола безпеки, яке характеризується своїм унікальним номером та дозволяє розмежовувати доступ до захищених об'єктів.

Отже, успішна реалізація політики безпеки в компанії залежить від збалансованої та налагодженої взаємодії захисту операційних систем і гарантування безпеки баз даних, а також від постійного оновлення заходів захисту та контролю за їх виконанням.

ВИСНОВКИ

В рамках проведеного дослідження у ТОВ "Перша українська газонафтова компанія" було запропоновано нове рішення щодо забезпечення інформаційної безпеки підприємства. Отримані результати теоретичних узагальнень та практичних досліджень сприятимуть підвищенню ефективності захисту інформації та інформаційного продукту компанії.

У першому розділі дослідження було визначено, що система інформаційної безпеки для підприємства полягає у заходах з виявлення, усунення та нейтралізації негативних джерел, причин та умов, які можуть впливати на інформацію. Поняття "інформаційна безпека" відображає стан інформаційного захисту суб'єкта, від якого залежить можливість дії загроз.

Зокрема, акцентувалась увага на основних видів загроз, які можуть виникати у контексті інформаційної безпеки підприємства, таких як компрометація даних, розголошення конфіденційної інформації, помилкове використання інформаційних ресурсів, відмова в обслуговуванні, несанкціонований обмін інформацією, відмова від інформації та несанкціоноване використання ресурсів локальної мережі. Для більш ефективного захисту інформації та визначення найбільш економічних та ефективних засобів забезпечення безпеки, необхідне детальне знання можливих загроз та вразливих місць системи захисту.

Аналіз актуальних способів та методів несанкціонованого доступу до інформації та мереж показав, що порушення захисту інформації можуть відбуватись через застосування технічних та програмних засобів, використання недоліків мов програмування та операційних систем, крадіжки носіїв інформації, отримання захищених даних за допомогою запитів дозволу, реквізитів розмежування доступу та таємних паролів. Результати дослідження дають можливість розробити ефективні заходи забезпечення інформаційної безпеки.

Отже, результати дослідження вказують на необхідність введення нових заходів та методів.

В другому розділі дослідження було проведено аналіз діяльності ТОВ «Перша українська газонафтова компанія» та з'ясовано, що результати його роботи важливі для всіх сфер життя Київщини. Дослідження також показало, що діловодство має провідне місце у роботі апарату підприємства, оскільки впорядковує роботу з документами та носіями інформації, що забезпечує економію ресурсів управлінської ланки.

В ТОВ "Перша українська газонафтова компанія" було проведено дослідження основних принципів та методів забезпечення інформаційної безпеки. За результатами дослідження можна стверджувати, що компанія має достатню кількість захисних засобів для забезпечення інформаційної безпеки, таких як ідентифікація та аутентифікація користувачів, шифрування інформації, антивірусний захист та контентна фільтрація.

Для оцінки стану забезпечення інформаційної безпеки в ТОВ "Перша українська газонафтова компанія" було використано програму "Гриф", загальний рейтинг інформаційної безпеки склав 7,9 бала, що свідчить про достатній рівень захисту. Однак, під час дослідження було виявлено недоліки в системі захисту інформації, зокрема, недостатня захищеність програмного забезпечення від хакерських атак через використання застарілих версій програм захисту інформації.

Отже, на основі проведеного дослідження можна зробити висновок про доцільність введення нових заходів та методів забезпечення інформаційної безпеки в ТОВ "Перша українська газонафтова компанія" для підвищення рівня захисту від потенційних загроз. Компанія повинна приділяти належну увагу підвищенню свого рівня інформаційної безпеки та відповідно покращувати свої захисні заходи.

В третьому розділі дослідження було виявлено, що в АС "Мотив" захист від несанкціонованого доступу до документів забезпечується адміністратором системи захисту інформації, який належним чином розмежовує доступ користувачів до системи. Для ефективного захисту інформації можна використовувати комбінацію апаратних та програмних механізмів криптографічного захисту, включаючи програмну реалізацію криптоалгоритмів й апаратне зберігання ключів. Однак, слід пам'ятати про захист від перехоплення ключів при їх зчитуванні з носія та використанні в програмі.

У ТОВ "Перша українська газонафтова компанія" існують два основні підходи до захисту електронних систем: фрагментарний та комплексний. Компанія переважно використовує комплексний підхід для захисту великих систем, які містять вмонтовані програмні засоби захисту інформації (наприклад, АС "Мотив", 1С тощо). Однак, це не завжди є достатнім для повноцінного захисту інформації, тому необхідні додаткові організаційні заходи з контролю за персоналом, зокрема програмістами та адміністраторами баз даних, а також з резервування критично важливої інформації та відновлення працездатності системи в разі непередбачуваних ситуацій. Такі заходи допоможуть підвищити рівень захисту інформації в компанії та запобігти потенційним загрозам.

Отже, на основі проведеного дослідження можна зробити висновок, що для ефективного захисту інформації необхідно використовувати комплексний підхід, включаючи комбінацію апаратних і програмних механізмів криптографічного захисту та додаткові організаційні заходи з контролю за персоналом та резервування критично важливої інформації.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Топ 20 приголомшливих статистичних фактів пов'язаних з витоками даних у 2023 році. Режим доступу: http://surl.li/meqsk
2. Закон України «Про телекомунікації» № 1089-IX від 16.12.2020. ВВР 2020.
3. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с.
4. Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів. Київ: ДУТ ННІЗІ, 2020.167 с.
5. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. Ефективна економіка № 4, 2015. Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=5514
6. Забродський В.А., Кізім Н. А., Янов Л.І. Сучасні методи організації та управління промисловим виробництвом. Харків: АТ «Бізнес-Інформ», 1997. 64.
7. Камлик, М.І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект [Текст] : навч. посіб. К. : Атіка, 2005. 432 с
8. Гладченко Т.М. Індикатори економічної безпеки підприємницької діяльності. Донецьк: ДонДАУ. *Менеджер*. 2000. №12. С.111-113.
9. Ніколаюк, С.І., Никифорчук Д.Й. Безпека суб'єктів підприємницької діяльності [Текст] курс лекцій К. : КНТ, 2005. 320с.
10. Могильний А.І., Безчастний В.М., Винокуров Ю.О. Основи безпеки бізнесу. Донецьк: Регіон, 2000. 130 с.
11. Олійник О.В. Принципи забезпечення інформаційної безпеки України. *Науковий вісник Ужгородського університету.* 2012. Випуск 18. С.170-173.
12. Про електронні документи та електронний документообіг: Закон України : прийнятий ВРУ 22.05.2003 р. № 851–IV // Відомості Верховної Ради України. -2003 р. - №44. – С.1175-1176.
13. Інформація та документація. Базові поняття. Терміни та визначення: ДСТУ 2398–94. / [Чинний від 1995–02–01]. – К. : Держспоживстандарт України, 1995. – І, 45 с. – (Національний стандарт України).

14. Про Основні засади розвитку інформаційного суспільства в Україні на 2007– 2015 роки: Закон України: прийнятий ВРУ 09.01.2007 р. № 537–V // Відомості Верховної Ради України. - 2007 р. - №125. – С.1120-1124.
15. Інформація і документація. Словник термінів (ISO 5127:2001, IDT): ДСТУ ISO 5127:2007 / [Чинний від 2007–14–12]. – К. : Держспоживстандарт України, 2007. – III, 389 с. – (Національний стандарт України).
16. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України: прийнятий ВРУ 05.07.1994 р. № 81/94-ВР // Відомості Верховної Ради України. - 1994 р. - №31. – С.1115-1158.
17. Про захист персональних даних: Закон України: прийнятий ВРУ 01.06.2014 р. № 2297-VI // Відомості Верховної Ради України. - 2010 р. - №34. – С.1105-1150.
18. Про електронні документи та електронний документообіг: Закон України : прийнятий ВРУ 22.05.2003 р. № 851–IV // Відомості Верховної Ради України. - 2003 р. - №44. – С.1175-1176.
19. Про основи національної безпеки України: : [Електронний ресурс] : Закон України : № 964-IV від 19.06.2003 р.
20. Комплектування фонду документів. Бібліографування. Каталогізація. Терміни і визначення: ГОСТ 7.76 – 96. / [Чинний від 1998– 01–01]. – Минск.: Изд– во стандартов, 1997. – 52 с. – (Система стандартів з інформації, бібліотечної та видавничої справи
21. Уніфіковані системи документації. Основні положення: ГОСТ 6.10.1–88/ [Чинний від 1995–18–03]. – К. : Держспоживстандарт України, 1995. – III, 360 с. – (Національний стандарт України)
22. Про інформацію [Електронний ресурс] : Закон України № 2657-XII (2657-12) від 2.10.1992 р. – Режим доступу : http://zakon2.rada.gov.ua/laws/show.
23. Андрєєва В. І. Діловодство: практичний посібник / В.І. Андрєєва. – М.: ТОВ «Управління персоналом», 2005. – 234 с.
24. Баранов О. А. Інформаційний суверенітет або інформаційна безпека? / О. А. Баранов // Національна безпека та оборона. – 2001. – № 1. – С. 70-76
25. Барсуков В. С. Безпека: технології, засоби, послуги / В. С. Борсуков. – М.: 2001 – 496 с.
26. Батюк А. Є. Інформаційні системи в менеджменті / А. Є. Батюк, З. П. Двуліт, К. М. Обельовська та ін. – Львів: Інтелект-Захід, 2004. – С. 343–384.

27. Бурячок В. Л. Метод визначення найбільш значимих загроз із «генеральної сукупності» загроз інформаційним ресурсам на підставі їх якісних та кількісних показників / В. Л. Бурячок, Я. В. Невойт // Сучасний захист інформації. – 2014. – № 3. – С. 18-21.
28. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015.– 288 с.
29. Зубок М. І. Інформаційна безпека / М. І. Зубок – К.: КНТЕУ, 2005. – 93 с.
30. Зубок М. І. Правове регулювання безпеки підприємницької діяльності / М. І. Зубок. – К.: КНТЕУ, 2005. – 76 с.
31. Інформаційне законодавство: збірник законодавчих актів / Ред. Ю. С. Шемшученко, К. С. Чиж. – Т. 5: Міжнародно-правові акти в інформаційній сфері. – К.: Юридична думка, 2005. – 328 с
32. . Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві [Електронний ресурс] / Ю. О. Коваленко. – Електронні дані. – Режим доступу: http://www.econindustry.org/arhiv/html/2010/st_51_18.pdf.
33. Коваленко Ю. О. Організація систем інформаційної безпеки підприємств [Електронний ресурс] / Ю. О. Коваленко. – Електронні дані. – Режим доступу: http://fullref.ru/job_05dc6b4cd1d240ca816e0bf9a1e0c2d4.html.
34. Кримінальний Кодекс України [Електронний ресурс]. – Електронні дані. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/2341-14.
35. Кузьменко Б. В. Захист інформації. Організаційно-правові засоби забезпечення інформаційної безпеки: навч. посібник / Б. В. Кузьменко, О. А. Чайковська. – К.: Ліра, 2009. – Ч.1. – 83 с
36. Малюк А. А . Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие / А. А. Малюк. – М.: Горячая линия – Телеком, 2004. – 280 с.
37. Матвієнко О. В. Основи організації електронного документообігу: навч. посібник для студ. ВНЗ / О. В. Матвієнко, М. Н. Цивін. – К.: Центр навчальної літератури, 2008. – 112 с.
38. Низенко Е. І. Забезпечення інформаційної безпеки підприємництва: навч. посібик / Е. І. Низенко, В. П. Каленяк. – К.: МАУП, 2006. – 154 с.

39. Про основи національної безпеки України: [Закон України: прийнятий ВРУ 19 червня 2003 р. № 964-IV] // Відомості Верховної Ради України. – 2003. – № 39. – С. 351
40. Про Стратегію національної безпеки України: [Указ Президента України: затв. ВРУ 12 лютого 2007 р. № 105/200] // Офіційний вісник України. – 2007. – № 11. – 389 с
41. Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні: [Постанова Верховної Ради України 01 грудня 2005 р.] // Відомості Верховної Ради України. – 2006. – № 15. – 131 с.
42. Юдін О. К. Захист інформації в мережах передачі даних: підручник / О. К. Юдін, О. Г. Корченко, Г. Ф. Конахович. – К.: Інтерсервіс, 2009. – 716 с.