Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: Заходи з удосконалення політики інформаційної безпеки сучасного підприємства

Виконавець: студентка IV курсу, групи КБ-42

_____ **Аліна РОГАЧОВА**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Яніна ШЕСТАК	

Нормоконтроль	Сергій ДАКОВ	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студентці **КБ-42** **Аліні Євгенівні Рогачовій**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Заходи з удосконалення політики інформаційної безпеки сучасного підприємства

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Розрахунок інформаційних ризиків, економічне обґрунтування доцільності витрат на інформаційну безпеку.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з теоретичними аспектами інформаційної безпеки на підприємстві, проаналізувати політику інформаційної безпеки на сучасному підприємстві, розробити систему інформаційної безпеки підприємства, побудувати модель структури системи інформаційної безпеки підприємства.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації дозволять підвищити ступень захисту інформації на підприємстві.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ (підпис) Яніна ШЕСТАК (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Аліна РОГАЧОВА (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 20.01.2023	*виконано*
2	Аналіз літератури	23.01.2023 – 10.02.2023	*виконано*
3	Обґрунтування вибору рішення	13.02.2023 – 17.02.2023	*виконано*
4	Огляд інформаційних джерел з тематикою, пов'язаною із інформаційною безпекою сучасного підприємства	20.02.2023 – 10.03.2023	*виконано*
5	Дослідження особливостей оцінки політики інформаційної безпеки на підприємстві	13.03.2023 – 24.03.2023	*виконано*
6	Планування заходів із вдосконалення політик інформаційної безпеки	27.03.2023 – 14.04.2023	*виконано*
7	Побудова моделі структури системи інформаційної безпеки підприємства	17.04.2023 – 12.05.2023	*виконано*
8	Оформлення пояснювальної записки	15.05.2023 – 26.05.2023	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	29.05.2023 – 12.06.2023	*виконано*

Завдання видав _____ (підпис) Яніна ШЕСТАК (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Аліна РОГАЧОВА (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 68 сторінок основного тексту, 9 таблиць, 7 рисунків та 4 формули. Список використаних джерел містить 34 найменування і займає 4 сторінки.

Методи дослідження кваліфікаційної роботи:

- теоретичні (класифікація, аналіз);
- практичні (вимірювання, порівняння);
- спеціальні методи (дослідницький, прогнозний аналіз даних);
- аналіз одержаних результатів шляхом статистичної обробки, узагальнення.

Об'єктом дослідження є процес інформаційної безпеки сучасного підприємства.

Предметом дослідження є методи та засоби по вдосконаленню політики інформаційної безпеки сучасного підприємства.

Практична цінність визначається тим, що її результати дозволяють підвищити ступінь захисту інформації на підприємствах шляхом використання запропонованих методів, алгоритмів та практичних процедур для формування системи інформаційної безпеки, спрямованої на зниження інформаційних ризиків.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПК	–	персональний комп’ютер
ПЗ	–	програмне забезпечення
КМ	–	комп’ютерна мережа
КІІ	–	критична інфраструктура
КЗ	–	контрольована зона
ДПКС	–	диспетчерський пункт компресорних станцій
КС	–	компресорна станція
СУБД	–	система управління базами даних
АРМ	–	автоматизовані робочі місця
ІБ	–	інформаційна безпека
КРІ	–	ключові показники ефективності
СЗІ	–	система захисту інформації
САК	–	система автоматичного керування

ЗМІСТ

ВСТУП

Актуальність. В останні роки все більш актуальною є проблема інформаційної безпеки в організаціях. Основне завдання інформаційної безпеки – це збереження персональної інформації, забезпечення захисту інформаційних даних, запобігання несанкціонованому доступу до різних інформаційних ресурсів, а також виявлення загроз та вразливостей. Ключовим інструментом забезпечення інформаційної безпеки у організаціях є політика інформаційної безпеки. Дотримуючись рекомендацій, які містяться у літературі з передової практики, сучасні організації часто впроваджують широкий спектр механізмів навчання та контролю, щоб мотивувати співробітників слідувати своїй політиці інформаційної безпеки.

Актуальність теми визначається загостренням проблем інформаційної безпеки (ІБ) навіть за умов інтенсивного вдосконалення технологій та інструментів захисту даних. Про це свідчить безпрецедентне зростання порушень інформаційної безпеки та тяжкість їх наслідків, що посилюється. Перелік загроз інформаційній безпеці, порушень, злочинів настільки великий, що потребує наукової систематизації та спеціального вивчення з метою оцінки пов'язаних з ними ризиків та розробки заходів щодо їх запобігання. Дослідження свідчать про те, що основною причиною проблем підприємств у галузі захисту інформації є відсутність продуманої та затвердженої політики забезпечення інформаційної безпеки, що базується на організаційних, технічних, економічних рішеннях з подальшим контролем їхньої реалізації та оцінкою ефективності.

Аналіз джерел. Теоретичним надбанням дослідження стали праці вчених, які ґрунтовно вивчали питання правових режимів інформації (зокрема, інформації з обмеженим доступом), правового регулювання захисту інформації, зокрема: Б.А. Кормича, В.А. Ліпкана, Р.А. Калюжного, О.В. Олійника, В.Ю. Баскакова, І.С. Чижа, М.Я. Швеця, М.О. Шиліна, І.В. Арістової, О.О. Кулініча, А.Б. Стоцького, А.І. Марущака, М.І. Дімчогло, М.П. Стрельбицького, В.М. Панченко, А.М. Гуза та інших учених.

Незважаючи на достатню кількість праць, присвячених праву на доступ до інформації з обмеженим доступом, найбільш дискусійними є ті, що спрямовані на формування понятійного апарату, але вдосконаленню політики інформаційної безпеки сучасного підприємства приділено недостатньо уваги, що й визначає актуальність цієї роботи.

Мета роботи полягає у удосконаленні політики інформаційної безпеки сучасного підприємства.

Реалізація поставленої мети передбачає розв'язання низки наступних **завдань:**

- вивчити поняття інформаційної безпеки;
- розглянути сутність і проблеми забезпечення інформаційної безпеки на підприємстві;
- визначити методи і засоби захисту інформації на сучасному підприємстві;
- дослідити політику інформаційної безпеки сучасного підприємства;
- розробити планування заходів із вдосконалення політики інформаційної безпеки;
- розробити систему інформаційної безпеки підприємства;
- побудувати модель структури системи інформаційної безпеки підприємства.

Об'єктом дослідження є процес інформаційної безпеки сучасного підприємства.

Предмет дослідження є методи та засоби по вдосконаленню політики інформаційної безпеки сучасного підприємства.

Написання роботи включало **такі методи дослідження**: теоретичні (класифікація, синтез, аналіз), практичні (вимірювання, порівняння), спеціальні методи (інтелектуальний, дослідницький, прогнозний аналіз даних), а також аналіз одержаних результатів шляхом статистичної обробки, узагальнення.

Практична цінність визначається тим, що її результати дозволяють підвищити ступінь захисту інформації на підприємствах шляхом використання запропонованих методів, алгоритмів та практичних процедур для формування системи інформаційної безпеки, спрямованої на зниження інформаційних ризиків.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

1.1 Поняття інформаційної безпеки

Сьогодні все більше шириться вплив інформаційних технологій, ресурсів та важливості зібраної інформації для суб'єктів підприємництва. Як наслідок, безпека інформації стає важливим аспектом економічної безпеки компанії, який має фундаментальне значення.

Забезпечення інформаційної безпеки підприємства передбачає активну діяльність керівних органів та посадових осіб компанії з використанням відповідних ресурсів і зусиль для досягнення безпечного інформаційного середовища, необхідного для нормального функціонування та прогресивного розвитку організації.

Інший підхід до визначення інформаційної безпеки ґрунтується на виділенні системних параметрів та функціональному блоці.

Існує два основних аспекти, на яких базується сутність інформаційної безпеки:

1. Безпосередня інформаційна безпека – стан захищеності інформаційного середовища.

2. Забезпечення захисту інформації - діяльність, спрямована на запобігання витоку захисту. інформації, недопущення несанкціонованих та ненавмисних впливів на захист інформацію.

Системними параметрами виступають сама інформація та інфраструктура, під якою слід розуміти всі системи забезпечення, починаючи від електропостачання, закінчуючи обслуговуючим персоналом.

Функціональний блок - це загрози інформаційній системі та збитки, яким не можна знехтувати внаслідок порушення стану інформаційної безпеки.

Забезпечення інформаційної безпеки загалом веде до значної економії витрат, коштів та ресурсів підприємства, тоді як збитки, завдані внаслідок навмисних дій та ненавмисних помилок, що призводить до значних матеріальних втрат. Наприклад, якщо особливі умови технологічних процесів стають відомими конкурентам через

розкриття інформації, це може призвести до створення аналогічних продуктів, що конкурують з власними. У результаті порушення інформаційної безпеки підприємство може втратити частину ринку, а, отже, зменшити свої прибутки і виторг. Якщо ж інформаційні активи є ключовим чинником конкурентоспроможності підприємства, порушення інформаційної безпеки веде до катастрофічних наслідків для компанії.

Специфіка забезпечення інформаційної безпеки компанії проявляється у трьох базових ознаках: конфіденційності, цілісності та доступності інформації.

1. Конфіденційність: характеристика інформаційних ресурсів, включаючи інформацію, полягає в їхній недоступності та нерозкритості для неуповноважених осіб.

2. Цілісність: незмінність інформації у її передачі чи зберігання.

3. Доступність: властивість інформаційних ресурсів, зокрема інформації, визначальне можливість їх отримання та використання на вимогу уповноважених осіб.

Функціональні характеристики забезпечення інформаційної безпеки підприємства включають створення таких умов:

1. Суворе виконання зобов'язань: підтвердження всіх дій, вчинених в інформаційній системі, і подій, наказаних до здійснення, таким чином, що ці дії та події не можуть бути пізніше скасовано, крім випадків, передбачених регламентом.

2. Реалізація підзвітності та ідентифікації: забезпечення однозначної ідентифікації всіх суб'єктів інформаційної системи та користувачів інформації, які мають певні права доступу до неї, та реєстрації всіх дій, пов'язаних з отриманням та обробкою інформації.

3. Досягнення достовірності: підтвердження відповідності операцій, що здійснюються, регламентованим діям та результатам.

4. Забезпечення справжності: формування умов, що гарантують фактичну ідентичність інформаційних ресурсів заявлених параметрів.

Способи та засоби забезпечення інформаційної безпеки зводяться до трьох сфер апаратного забезпечення, програмне забезпечення та канали комунікації.

Такий комплексний підхід до захисту інформації передбачає застосування процедур та механізмів на кожному рівні: фізичному, персональному та організаційному. Це допомагає забезпечити цілісність, конфіденційність та доступність інформації.

Так, концепцію інформаційної безпеки можна представити у вигляді структурної схеми, базові та функціональні ознаки, способи та засоби забезпечення інформаційної безпеки, що відображає її, процедури та механізми захисту інформації. Концепція інформаційної безпеки відображена у вигляді схеми на Рисунок 1.1.

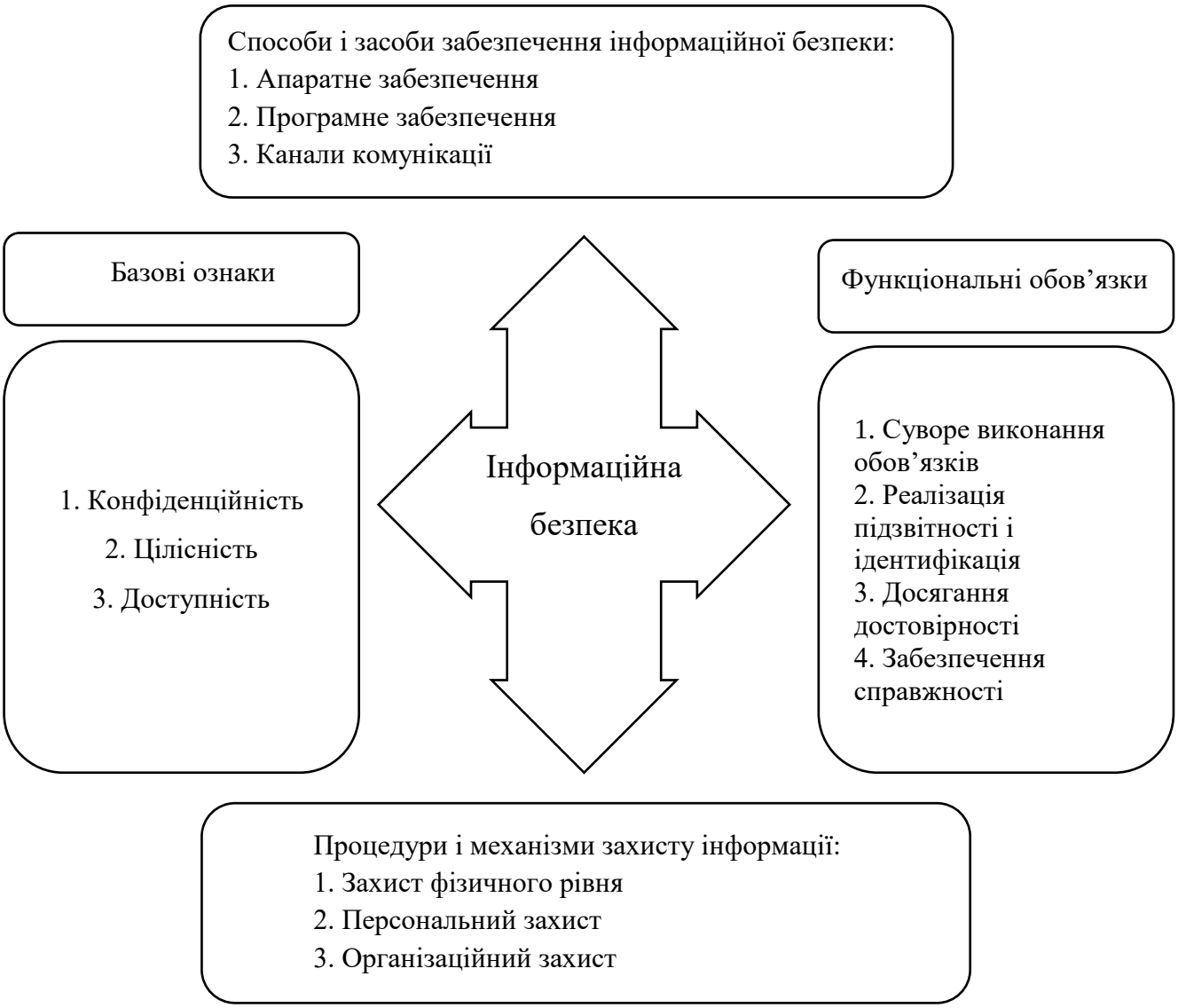


Рисунок 1.1 Концепція інформаційної безпеки

У контексті того, що зараз підприємства активно впроваджують інформаційні технології у свою діяльність, забезпечення інформаційної безпеки стає дуже актуальним питанням для підприємств, на користь яких мінімізувати загрози інформаційній безпеці.

Об'єктивною умовою виникнення поняття інформаційної безпеки є поява загроз нанесення шкоди майновим та іншим інтересам внаслідок впливу безпосередньо на інформацію чи кошти комунікації, якими вона передається. В даний час розвиток інформаційних технологій призвів до появі широкого розмаїття як засобів обробки та передачі даних, так і можливостей їх розкрадання та використання у корисливих цілях. Внаслідок цього компанії мають забезпечувати захист власної інформації для запобігання промисловому шпигунству та завданню іншої шкоди своїм інтересам, мінімізуючи потенційні та усуваючи існуючі загрози своїй інформаційній безпеці.

Відповідно до концепції забезпечення інформаційної безпеки компанії лише виявлення та контроль всього. Спектр загроз дозволяє побудувати ефективну систему захисту інформації.

Стосовно інформаційної системи підприємства, загрози інформаційної безпеки можуть бути внутрішніми чи зовнішніми. Внутрішні загрози включають порушення внутрішніх правил і політик щодо використання інформаційних ресурсів підприємства, недобросовісне використання даних компанії в особистих цілях, введення вірусів до інформаційної мережі співробітниками, розкрадання конфіденційних даних та інші подібні порушення. Зовнішні загрози є наслідком дій суб'єктів, які не мають прямого зв'язку з підприємством. Типовими прикладами є хакерські атаки на інформаційну систему підприємства, спроби злому та несанкціонованого доступу до даних, а також саботаж підтримуючої інфраструктури, який може призвести до відключення системи чи зниження її ефективності. За ознакою навмисності загрози поділяють на навмисні та ненавмисні.

До ненавмисних загроз відносять факти випадкового видалення даних персоналом, форс-мажорні обставини, пов'язані з роботою інформаційної системи, стихійні лиха, що ведуть до поломки апаратного забезпечення тощо. Навмисні

загрози мають на меті завдання відчутної шкоди підприємству, а суб'єкти, які здійснюють такі дії, слідують чітким планам щодо подолання можливого захисту.

Залежно від мети загрози виділяють дії, спрямовані на отримання даних, знищення даних, зміна або внесення даних, порушення роботи програмного забезпечення, контроль над роботою програмного забезпечення забезпечення та інші.

Функціональна класифікація загроз інформаційній безпеці оперує чотирма критеріями (табл. 1.1).

Таблиця 1.1

Функціональна класифікація загроз інформаційній безпеці

Критерій інформаційної безпеки	**Загрози інформаційній безпеці**
Загальна інформаційна безпека	За базовими ознаками доступності, цілісності, конфіденційності, проти яких загрози спрямовані насамперед
Компоненти інформаційних систем	На ці компоненти безпосередньо спрямовані загрози: дані, програми, апаратура, підтримуюча інфраструктура.
Спосіб здійснення	Випадкові/навмисні дії/загрози Дії/загрози природного/техногенного характеру
Розташування джерела загроз	Усередині інформаційної системи чи поза нею

Враховуючи багатогранність сучасних інформаційних систем, можна погодитись із твердженням, що "не можна захиститися від усіх можливих і немислимих загроз ІБ хоча б тому, що неможливо передбачити дії зловмисників, не кажучи вже про всі помилки користувачів ".

Вибудовуючи інформаційну систему та роблячи конкретні кроки, спрямовані на попередження загроз інформаційній безпеці, необхідно опрацьовувати заходи прямого захисту від відомих загроз та забезпечувати можливість оперативного реагування на ті загрози, котрим заходи захисту передбачені базовим регламентом.

1.2 Сутність і проблеми забезпечення інформаційної безпеки на підприємстві

Розвиток проблеми захисту інформації з моменту її появи і до сучасного стану пройшов тривалий і часто суперечливий шлях. З початку існувало два напрями розв'язання задачі підтримки конфіденційності: використання криптографічних методів захисту інформації в середовищах передачі та зберігання даних та програмно-технічне розмежування доступу до даних та ресурсів обчислювальних систем. Варто врахувати, що на початку 80-х років комп'ютерні системи були слабо розподіленими, а технології глобальних і локальних обчислювальних мереж знаходилися на своїх початкових стадіях розвитку. В той час вдалося досить успішно вирішувати зазначені завдання і забезпечувати достатній рівень захисту інформації.

Пізніше, з появою тенденції до розподіленої інформації, класичний підхід до організації розділення ресурсів та класичні криптографічні протоколи почали поступово вичерпувати себе та еволюціонувати. Першорядними стали проблеми автентифікації взаємодіючих елементів системи, а також способи управління криптографічними механізмами в розподілені комп'ютерні системи.

У світлі цього, почало розглядатися питання про рівноправність функцій криптографічного захисту в автоматизованій системі та їх взаємозв'язок з іншими функціями. Ця теорія стала основою для поділу проблематики на засоби захисту, які включають криптографічні засоби, засоби контролю доступу та інші, та засоби, що забезпечують їх коректну роботу.

Забезпечення інформаційної безпеки має бути спрямоване насамперед на запобігання ризикам, а не на ліквідацію їх наслідків. Саме вжиття запобіжних заходів щодо забезпечення конфіденційності, цілісності, а також доступності інформації є найбільш правильним підходом у створенні системи інформаційної безпеки.

Будь-який незаконний витік інформації може призвести до серйозних проблем для компанії, від значних фінансових збитків до повної ліквідації. І хоча проблема витоків інформації не виникла сьогодні, промислове шпигунство та переманювання кваліфікованих фахівців існували ще до епохи комп'ютеризації, з появою

персональних комп'ютерів та Інтернету з'явилися нові методи незаконного отримання інформації.

Раніше для викрадення цілого стосу паперових документів з фірми зловмиснику доводилося виконати складні фізичні дії. Але сьогодні величезні обсяги важливої інформації можна легко скопіювати на флешку, яка поміщається в портмоне, або передати через мережу, скориставшись руткітами, троянами, бекдорами, кейлоггерами та ботнетами. Знищення важливої інформації також може бути здійснене вірусами, які функціонують як засоби диверсії.

Зазвичай, у компаній найчастіше стають об'єктом витоку документи, що мають фінансовий характер, технологічні та конструкторські розробки, а також інформація щодо логінів та паролів для доступу до мереж інших організацій. Однак, не менш небезпечним може бути витік персональних даних співробітників, що може спричинити серйозні наслідки. Особливо це стосується країн Заходу, де в судах часто подаються позови через такі витоки, що можуть призвести до накладання значних грошових штрафів, виплата яких серйозно ушкоджує фінансову стабільність компаній.

Дуже часто стається так, що наслідки витоку інформації негативно впливають на компанію через деякий період часу, можливо, навіть через кілька місяців або років після самого витоку. Ця інформація може потрапити у руки конкурентів чи журналістів і завдати значної шкоди. Тому важливо приділяти увагу комплексному захисту даних. Відмовитися від розподілу інформації на категорії "дуже важлива" та "менш важлива" є ключовим аспектом. Всі дані, що стосуються діяльності компанії та не призначені для публічного доступу, повинні залишатися в межах компанії і бути ефективно захищені від можливих загроз.

Крім того, важливо пам'ятати, що витік конфіденційної інформації може мати серйозні наслідки не лише для фінансової стійкості компанії, але й для її репутації та взаємовідносин з клієнтами і партнерами. Втрата довіри може призвести до втрати бізнесу та зниження конкурентоспроможності.

Сформулюємо основні джерела виникнення загроз інформаційній безпеці підприємства (Рисунок 1.2).

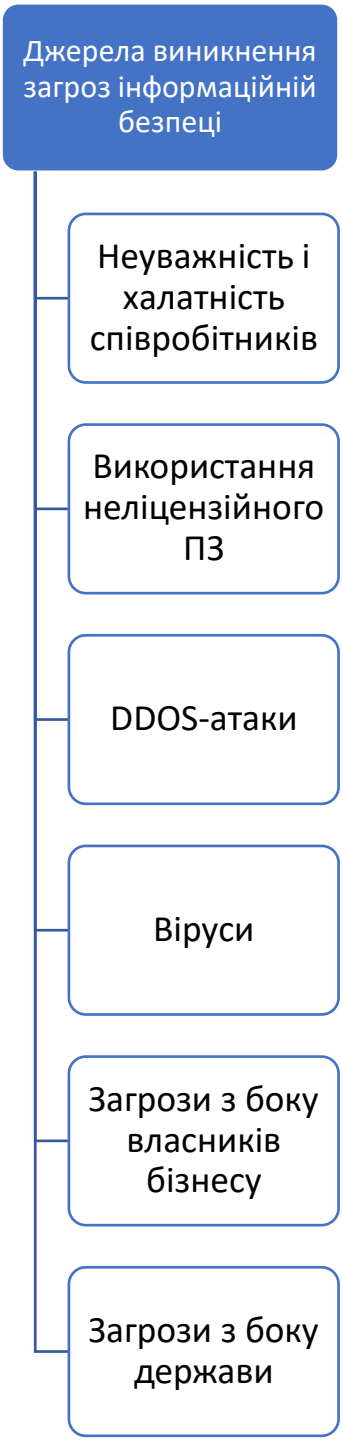


Рисунок 1.2 Джерела виникнення загроз інформаційній безпеці підприємства

1. Неуважність та недбалість співробітників.

Загрозу інформаційної безпеки компанії, як не дивно, можуть представляти цілком лояльні співробітники, які не думають про крадіжку важливих даних. Ненавмисна шкода конфіденційним відомостям завдається за простою недбалістю чи необізнаності працівників. Завжди є можливість того, що хтось відкриє фішинговий

лист та впровадить вірус із особистого ноутбука на сервер компанії. У такій ситуації інформація виявляється дуже легкою здобиччю.

2. Використання піратського ПЗ. Деякі керівники компаній, у своєму бажанні зекономити кошти, можуть вирішити скористатися піратським програмним забезпеченням. Проте, варто пам'ятати, що такий підхід не забезпечує належного захисту від шахраїв, які мають інтерес до крадіжки інформації за допомогою вірусів. Власник неліцензійного програмного забезпечення лишається без технічної підтримки та своєчасних оновлень, які надаються офіційними розробниками. Крім того, використання піратського ПЗ також приносить ризик отримання вірусів, які можуть негативно вплинути на систему комп'ютерної безпеки. Згідно з дослідженням Microsoft, було виявлено спеціальне зловмисне програмне забезпечення для крадіжки паролів та персональних даних у 7% досліджених неліцензійних програм.

3. DDoS-атаки. що означають "розподілена відмова від обслуговування", представляють собою надходження великого потоку помилкових запитів від сотень тисяч географічно розподілених хостів, з метою перешкоджати нормальному функціонуванню цільового ресурсу.

Існують два основних способи здійснення таких атак:

Перший спосіб - пряма атака на канал зв'язку, де велика кількість непотрібних даних перекриває доступ до ресурсу, повністю блокуючи його передачу.

Другий спосіб - атака безпосередньо на сервер ресурсу, де надходження великого обсягу запитів спрямовується на сервер з метою перевантаження його ресурсів та призводить до недоступності або погіршення якості роботи публічних веб-сервісів.

Такі атаки можуть тривати від кількох годин до кількох днів і спричиняти серйозні проблеми з доступністю та функціонуванням цільового ресурсу.

Зазвичай подібні атаки застосовують у ході конкурентної боротьби, шантажу підприємств чи відвернення уваги системних адміністраторів від деяких протиправних процесів на кшталт викрадення коштів з рахунків. На думку фахівців, саме крадіжки є основним мотивом DDoS-атак. Метою зловмисників частіше стають сайти банків, у половині випадків (49%) торкнулися саме вони.

4. Віруси. Однією з найнебезпечніших на сьогодні загроз інформаційної безпеки є комп'ютерні віруси. Це підтверджується багатомільйонними збитками, які несуть компанії внаслідок вірусних атак. В останні роки суттєво збільшилася їх частота та рівень шкоди. Збільшилася кількість об'єктів для можливих вірусних атак. Якщо раніше атакам піддавалися в основному сервери стандартних веб-служб, то сьогодні віруси здатні впливати і на міжмережеві екрани, комутатори, мобільні пристрої, маршрутизатори.

5. Загрози з боку співвласників бізнесу. Саме легальні користувачі одна з основних причин витоків інформації в компаніях. Такі витоки фахівці називають інсайдерськими, а всіх інсайдерів умовно поділяють на кілька груп:

- «порушники» — середня ланка та топ-менеджери, які дозволяють собі невеликі порушення інформаційної безпеки — грають у комп'ютерні ігри, роблять онлайн-покупки з робочих комп'ютерів, користуються особистою поштою. Така безладність здатна викликати інциденти, але найчастіше вони є ненавмисними.

- "злочинці". Найчастіше інсайдерами є топ-менеджери, які мають доступ до важливої інформації та зловживають своїми привілеями. Вони самостійно встановлюють різні програми, можуть надсилати конфіденційну інформацію зацікавленим у ній третім особам тощо.

- «Кроти» - співробітники, які навмисне крадуть важливу інформацію за матеріальну винагороду від компанії-конкурента. Це досить досвідчені користувачі, які вміло знищують усі сліди своїх злочинів. Впіймати їх через це буває дуже непросто.

- звільнені та скривджені на компанію співробітники, які забирають із собою всю інформацію, до якої вони мали доступ.

6. Законодавчі перипетії. Державні органи в Україні наділені правом конфіскувати під час перевірок обладнання та носії інформації. Оскільки більшість важливих даних компанії зберігається в електронному вигляді на серверах, то у разі їх вилучення компанія на якийсь час просто зупиняє свою діяльність.

Розробники засобів захисту інформації постійно вдосконалюють свої рішення, оскільки кількість загроз неперервно зростає, а нові віруси та DDoS-атаки стають

більш інтенсивними і поширеними. На кожну конкретну загрозу з'являється нове або вдосконалюється вже існуюче захисне програмне забезпечення. Розробники стежать за новими техніками та методами атак і активно працюють над створенням ефективних рішень, щоб запобігти або пом'якшити наслідки таких загроз. Це включає розробку нових алгоритмів, методів виявлення інтранет-атак, інтелектуальних систем аналізу трафіку та механізмів реагування на вразливості. Розробники також активно співпрацюють зі спеціалістами з безпеки, дослідниками і іншими гравцями в галузі, щоб обмінюватися досвідом і знаннями та вдосконалювати свої рішення відповідно до змінюючихся умов та загроз. Серед засобів інформаційного захисту можна виділити:

Фізичні засоби захисту. Вони включають в себе різні заходи для обмеження доступу сторонніх осіб на територію компанії. Це можуть бути обмеження або повна заборона доступу до певних зон, пропускні пункти, які оснащені спеціальними системами контролю доступу. Один з популярних і широко використовуваних засобів контролю доступу - це HID-картки. Ця система дозволяє обмежити доступ до серверних приміщень або інших важливих підрозділів компанії лише тим особам, яким надано відповідні привілеї і дозволи за протоколом. Це забезпечує підвищений рівень безпеки, оскільки лише авторизованим особам дозволяється займатися важливими операціями та отримувати доступ до цінної інформації.

Основні засоби захисту електронної інформації. Є важливою складовою інфраструктури інформаційної безпеки компанії. Ці засоби включають в себе різноманітні антивірусні програми, які допомагають виявляти і блокувати шкідливе програмне забезпечення. Крім того, використовуються системи фільтрації електронної пошти, які відсіюють небажану або підозрілу кореспонденцію, забезпечуючи захист користувачів від шкідливих повідомлень. Важливою практикою є обладнання корпоративних поштових скриньок такими системами. Додатково, важливими засобами захисту є диференційований доступ до інформації, що означає, що лише авторизовані особи мають доступ до конфіденційної інформації, залежно від їхніх ролей і повноважень.

Анти-DDoS. Розглядається як ефективний засіб захисту від DDoS-атак, оскільки самостійно впоратися з такими нападами є складно. Багато розробників програмного забезпечення пропонують анти-DDoS послуги, які спеціалізуються на виявленні та захисті від таких атак. При спостереженні за незвичайним або підозрілим трафіком, система захисту активується і блокує шкідливий трафік, одночасно дозволяючи безперешкодний пропуск легітимного бізнес-трафіку. Особливістю анти-DDoS систем є їхній здатність працювати без обмежень, спрацьовуючи необмежену кількість разів, поки загроза повністю не буде усунена. Це дозволяє забезпечити неперервну доступність системи навіть під час активних DDoS-атак. Застосування анти-DDoS технологій допомагає компаніям зменшити вплив таких атак на їхню діяльність та забезпечити стабільну роботу мережі і сервісів.

Резервне копіювання даних. Це рішення, яке передбачає збереження важливої інформації не тільки на конкретному комп'ютері, але й на інших пристроях: зовнішньому носії чи сервері. Останнім часом особливо актуальною стала послуга віддаленого зберігання різної інформації в хмарі дата-центрів. Саме таке копіювання здатне захистити компанію у разі надзвичайної ситуації, наприклад, у разі вилучення сервера органами влади. Створити резервну копію та відновити дані можна у будь-який зручний для користувача час, у будь-якій географічній точці.

План аварійного відновлення. Крайній захід захисту інформації після втрати даних. Такий план необхідний кожній компанії для того, щоб у максимально стислий термін усунути ризик простою та забезпечити безперервність бізнес-процесів. У ньому обов'язково має бути передбачена можливість запровадження аварійного режиму роботи на період збою, а також усі дії, які мають бути вжиті після відновлення даних.

Шифрування даних під час передачі інформації в електронному форматі (end-to-end protection). Для забезпечення конфіденційності інформації при її передачі в електронному форматі застосовуються різні види шифрування. Шифрування дає можливість підтвердити справжність інформації, що передається, захистити її при зберіганні на відкритих носіях, захистити ПЗ та інші інформаційні ресурси компанії від несанкціонованого копіювання та використання.

1.3 Методи і засоби захисту інформації на сучасному підприємстві

При розгляді питань захисту автоматизованих систем доцільно використовувати чотирирівневу градацію доступу до збереженої, оброблюваної та системі інформації, що захищається, яка допоможе систематизувати як можливі загрози, так і заходи щодо них нейтралізації та парирування, тобто. допоможе систематизувати та узагальнити весь спектр методів забезпечення захисту, що належать до інформаційної безпеки. Ці рівні такі:

- рівень носіїв інформації;
- рівень засобів взаємодії з носієм;
- рівень подання інформації;
- рівень змісту інформації.

Дані рівні були введені виходячи з того, що:

1. Інформація для зручності маніпулювання частіше всього фіксується на деякому матеріальному носії, яким може бути папір, дискета чи інший носій;

2. Якщо спосіб подання інформації такий, що вона може бути безпосередньо сприйнята людиною, виникає потреба у перетворювачах інформації доступний для людини спосіб подання.

3. Як було зазначено, інформація може бути охарактеризована способом свого подання або тим, що називається мовою в повсякденному сенсі.

4. Людині має бути доступний зміст поданої інформації, її семантика.

Організаційно-технічні та організаційно-правові заходи включаються в систему організаційного захисту інформації з метою забезпечення безпеки та конфіденційності. Ці заходи виконуються під час всього життєвого циклу комп'ютерних систем (КС) для захисту передаваної та зберіганої інформації.

Під час будівництва або ремонту приміщень, де будуть розміщені КС, проводяться заходи забезпечення безпеки, такі як контроль доступу, обмеження фізичного доступу сторонніх осіб, встановлення систем виявлення та запобігання несанкціонованому проникненню, інсталяція систем вогнезахисту та контролю вологості.

Під час проектування системи КС враховуються принципи захисту інформації, встановлюються заходи щодо шифрування, аутентифікації та контролю доступу, резервного копіювання та відновлення даних, а також виявлення та відновлення системи після інциденту безпеки.

При монтажі та налагодженні технічних та програмних засобів КС виконуються заходи для забезпечення їхньої безпеки, встановлення необхідних патчів та оновлень, налаштування систем моніторингу та виявлення вторгнень.

Випробування та перевірка працездатності КС перед їхнім впровадженням допомагають виявити потенційні уразливості та недоліки, а також забезпечити високу ступінь безпеки системи перед її фактичним використанням.

Основні властивості методів та засобів організаційного захисту:

- забезпечення повного чи часткового перекриття значної частини каналів витоку інформації (наприклад, розкрадання або копіювання носіїв інформації);

- об'єднання всіх використовуваних у КС засобів у цілісний механізм захисту інформації.

Методи та засоби організаційного захисту інформації включають:

- обмеження фізичного доступу до об'єктів КС та реалізація режимних заходів;

- обмеження можливості перехоплення;

- розмежування доступу до інформаційних ресурсів та процесів КС (встановлення правил розмежування доступу, шифрування інформації при її зберіганні та передачі, виявлення та знищення апаратних та програмних закладок);

- резервне копіювання найважливіших з точки зору втрати масивів документів;

- профілактику зараження комп'ютерними вірусами.

Організаційні заходи в сфері інформаційної безпеки базуються на використанні та підготовці законодавчих та нормативних документів. Ці документи мають на меті створення правової бази для регулювання доступу до інформації з боку користувачів і споживачів.

В українському законодавстві пізніше, ніж у законодавстві інших розвинутих країн, з'явилися необхідні правові акти, при цьому далеко не всі.

Можна виділити чотири рівні правового забезпечення інформаційної безпеки.

1. Міжнародні договори, до яких приєдналася Україна, та Закони України.

2. Підзаконні акти, до яких належать укази Президента України та постанови Кабінета міністрів України.

3. Державні і міжнародні стандарти в галузі захисту інформації, керівні документи, норми, методики та класифікатори, розроблені відповідними державними органами.

4. Локальні нормативні акти, положення, інструкції, методичні рекомендації та інші документи щодо комплексного захисту інформації в КС конкретної організації.

Інженерно-технічні методи і засоби захисту

Під інженерно-технічними засобами захисту інформації розуміють різноманітні фізичні об'єкти, механічні, електричні та електронні пристрої, елементи конструкції будівель, засоби пожежогасіння та інші засоби, які спрямовані на забезпечення належного рівня захисту інформації:

- захист території та приміщень КС від проникнення порушників;

- захист апаратних засобів КС та носіїв інформації від розкрадання;

- запобігання можливості віддаленого (через меж охоронюваної території) відеоспостереження (підслуховування) за роботою персоналу та функціонуванням технічних засобів КС;

- організацію доступу до приміщень КС співробітників; • контроль за режимом роботи персоналу КС;

- контроль над переміщенням співробітників КС у різних виробничих зонах;

- протипожежний захист приміщень КС;

- мінімізацію матеріальних збитків від втрат інформації, що виникли внаслідок стихійних лих і техногенних аварій.

Технічні засоби охорони є важливою складовою інженерно-технічних засобів захисту інформації. Вони виконують роль першого рубежу захисту комп'ютерних систем і забезпечують фізичний контроль доступу до приміщень, де знаходяться комп'ютерні системи.

Програмні та програмно-апаратні методи і засоби захисту

Апаратні засоби захисту інформації включають електронні та електронно-механічні пристрої, які складаються з технічних компонентів і виконують функції забезпечення інформаційної безпеки. Ці засоби можуть бути самостійними або інтегрованими з програмними засобами для забезпечення комплексного захисту.

До основних апаратних засобів захисту інформації відносяться:

- пристрої для введення ідентифікуючої користувача інформації (магнітних та пластикових карток, відбитків пальців тощо);

- пристрої для шифрування інформації;

- пристрої для запобігання несанкціонованому включенню робочих станцій і серверів (електронні замки та блокатори).

Програмні засоби призначені виключно для забезпечення захисних функцій і виконують різноманітні завдання, пов'язані з контролем, виявленням і реагуванням на можливі загрози та інциденти безпеки.

До основних програмних засобів захисту інформації відносяться:

- програми ідентифікації та аутентифікації користувачів КС;

- програми розмежування доступу користувачів до ресурсів КС;

- програми шифрування інформації;

- програми захисту інформаційних ресурсів (системного та прикладного програмного забезпечення, баз даних, комп'ютерних засобів навчання тощо) від несанкціонованої зміни, використання та копіювання.

- розуміють однозначне розпізнавання унікального імені суб'єкта КС.

Аутентифікація означає підтвердження того, що пред'явлене ім'я відповідає даному суб'єкту (підтвердження справжності суб'єкта).

До переваг програмних засобів захисту інформації відносяться:

- простота тиражування;

- гнучкість (можливість налаштування на різні умови застосування, що враховують специфіку загроз інформаційній безпеці конкретних КС);

- простота застосування – одні програмні засоби, наприклад шифрування, працюють у «прозорому» (непомітному для користувача) режимі, а інші не вимагають від користувача жодних нових (порівняно з іншими програмами) навичок;

- практично необмежені можливості їх розвитку шляхом внесення змін для врахування нових загроз безпеки інформації.

До недоліків програмних засобів захисту інформації відносяться: - зниження ефективності КС за рахунок споживання її ресурсів, необхідних для функціонування програм захисту;

- нижча продуктивність (порівняно з апаратними, що виконують аналогічні функції засобами захисту, наприклад шифрування);

- пристикованість багатьох програмних засобів захисту (а не їх вбудованість у програмне забезпечення) КС), що створює для порушника принципову можливість їх обходу;

- можливість зловмисної зміни програмних засобів захисту в процесі експлуатації КС.

Висновки за розділом 1

Отже, сьогодні спостерігається критично високе значення інформаційних активів підприємств у контексті їх превалюючого значення стосовно вартості матеріальних ресурсів організації.

Проблема захисту інформації з моменту появи до сучасного стану пройшла тривалий і багато в чому задачі підтримки конфіденційності: використання криптографічних методів захисту суперечливий шлях у своєму розвитку. Із початково існувало два напрями розв'язання інформації в середовищах передачі та зберігання даних та програмно-технічне розмежування доступу до даних та ресурсів обчислювальних систем

Враховуючи рівень сучасного розвитку інформаційних технологій, питання забезпечення захисту інформації стають однією з фундаментальних детермінантів економічної безпеки компанії. Інформаційна безпека є єдино можливим напрямом для запобігання завданню шкоди економічним інтересам компанії шляхом організації захисту від існуючих та потенційних загроз інформаційних ресурсів підприємства.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНОГО ПІДПРИЄМСТВА

2.1 Організаційна характеристика підприємства

Сучасне суспільство потребує надання послуг та підтримки критично важливих функцій протягом усього життєвого циклу. Це досягається шляхом розбудови безперебійно-функціонуючої інфраструктури, яка також сприяє добробуту суспільства в цілому та його подальшому розвитку. Однак, інфраструктури в усьому світі постійно перебувають під загрозою значної кількості взаємодіючих антропогенних небезпек та природних явищ, які можуть перешкоджати роботі окремих об'єктів та інфраструктурної системи в цілому. Навіть якщо ймовірність цього низька, важливо пам'ятати, що наслідки можуть бути величезними, особливо у вигляді людських і економічних втрат та екологічних катастроф.

Група Нафтогаз - найбільша державна компанія в Україні. Це провідна компанія в паливно-енергетичному секторі України. Офіційна назва: Національна акціонерна компанія "Нафтогаз України" Група "Нафтогаз України" – вертикально-інтегрована нафтогазова компанія, яка займається розвідкою, розробкою, експлуатацією та облаштуванням родовищ, транспортуванням, зберіганням нафти і газу та постачанням їх споживачам.

Група імпортує газ, переробляє газ та нафту і конденсат з метою виробництва палива, скрапленого газу та інших нафтопродуктів на п'яти газопереробних заводах. Група має мережу автозаправних станцій.

Газова галузь України, 90% якої належить державній компанії НАК "Нафтогаз України", є організованою системою з елементами, що складають повний цикл видобутку та постачання газу кінцевому споживачеві. А саме: видобуток газу, підприємства, що експлуатують газотранспортні системи і транспортні мережі, та продаж газу споживачам (як домогосподарствам, так і юридичним особам, які

займаються виробничою діяльністю, що є частиною національної економічної системи і використовують газ як сировину).

Нафтогаз є найбільшим платником податків в Україні. У 2020 році податкові та дивідендні надходження групи сягнули 137 млрд грн, що становить приблизно 15% від загальних доходів державного бюджету.

Профіль компанії НАК "Нафтогаз України":

– нафтові родовища в експлуатації-234;

– видобувні свердловини (газові/нафтові/нагнітальні) - 2568/2494/312;

– протяжність магістральних газопроводів високого тиску(тис. км)- 38,2;

– компресорні станції/цехи- 73/110;

– потужність компресорних станцій, МВт-5450;

– протяжність газорозподільної системи, тис. км-347;

– підземні сховища газу -13;

– довжина магістральних нафтопроводів, тис. км - 4,7;

– насосні станції – 28;

– потужність насосних станцій, МВт-357;

– газопереробні заводи-5;

– АГНКС-91;

– кількість працівників, тис.-172.

Діяльність та послуги компанії:

– видобуток сирої нафти;

– видобуток природного газу

– надання допоміжних послуг у сфері видобування нафти та газу;

– оптова торгівля твердим, рідким і газоподібним паливом і подібними продуктами;

– трубопровідний транспорт;

– наукова діяльність;

– розподіл газоподібного палива через регіональні трубопроводи.

НАК "Нафтогаз України" складається з трьох дочірніх компаній, п'яти асоційованих компаній, двох державних акціонерних товариств та двох відкритих акціонерних товариств. Компанія має чотири бізнес-лінії: видобуток, переробка, транспортування та збут.

На Рисунок 2.1 зображено схематично організаційну структуру АТ НАК “Нафтогаз України».

Рисунок 2.1 Схема організаційної структури АТ НАК “Нафтогаз України

З метою підвищення ефективності роботи компанії Нафтогаз впровадив реформу корпоративного управління. Реформи розпочалися у 2015 році. Експерти та юридичні радники розробили план дій з корпоративного управління. Реформа Нафтогазу також започаткувала реформу корпоративного управління в усіх державних підприємствах України. Реформи передбачають відповідність найкращим міжнародним практикам, захист прав власників, наявність повноцінних та ефективних органів управління, чітке делегування повноважень, функціонування систем внутрішнього контролю, усунення політичного впливу та створення рівних

умов з комерційними компаніями відповідно до принципів, правил та процедур корпоративного управління організації економічного співробітництва та розвитку.

Склад системи АТ НАК «Нафтогаз України»:

-ДПКС «Яготин», м. Яготин Київської області (КС «Глушківська», контрольні пункти телемеханіки, газорозподільчі станції);

-ДПКС «Бердичів», с. Садки Житомирської області (КС «Бердичів», контрольні пункти телемеханіки, газорозподільчі станції);

-ДПКС «Гребенківська», м. Лохвиця Полтавської області (КС «Гребенківська»);

- ДПКС «Диканька», смт Диканька Полтавської області (КС «Диканька», контрольні пункти телемеханіки, газорозподільчі станції);

- ДПКС «Ромненська» (КС «Ромненська», контрольні пункти телемеханіки);

- КС «Боярка» (м. Боярка Київської області);

- КС «Зіньків» (м. Зіньків Полтавської області);

- КС «Решетилівка» (смт Решетилівка Полтавської області);

- КС «Красилів» (м. Красилів Хмельницької області);

- КС «Лубни» (м. Лубни Полтавської області); -Центральний ДПКС «Київ».

Наступним кроком до підвищення ефективності після реформи корпоративного управління стало те, що 14 січня 2019 року Рада директорів Нафтогазу затвердила нову модель управління бізнесом. Модель передбачає створення бізнес-підрозділів за ключовими напрямками. Зокрема, буде створено інтегрований газовий дивізіон ("Газовий дивізіон") та нафтовий дивізіон ("Нафтовий дивізіон").

Важливо також здійснити аналіз фінансової стану підприємства за коефіцієнтним методом за використання даних фінансової звітності "Нафтогаз України" за 2019-2022 роки.

Спочатку слід оцінити відповідність балансу досліджуваного підприємства умовам фінансової стійкості (табл. 2.1).

Таблиця 2.1

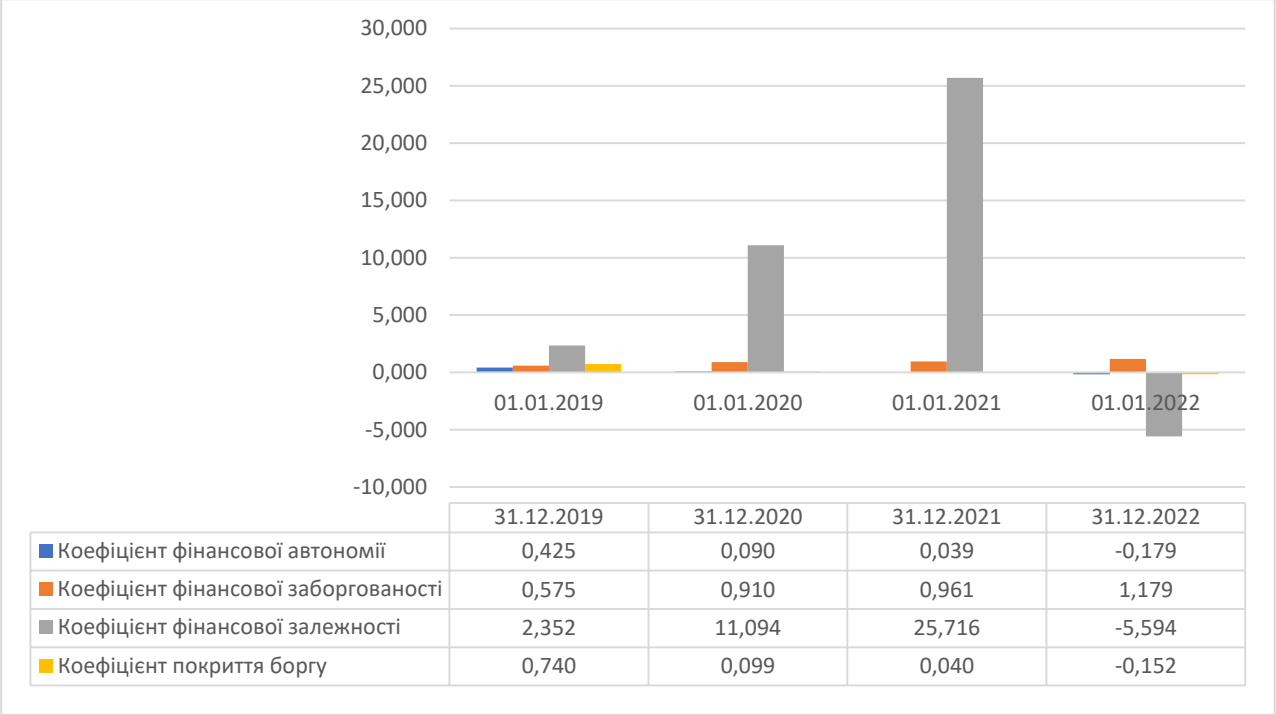
Оцінка відповідності балансу умовам фінансової стійкості "Нафтогаз України" за 2019-2022 роки

Показники	**Роки**				**Відхилення**	
	2019	2020	2021	2022	Відс. пунктів	%
Коефіцієнт співвідношення оборотних та необоротних активів	0,648	0,673	0,873	0,480	-0,168	-25,994
Коефіцієнт співвідношення зобов’язань та власного капіталу	10,094	24,716	-6,594	-7,416	-17,510	-173,463

Аналізуючи відповідність балансу підприємства умовам фінансової стійкості, можна відзначити, що рівень співвідношення оборотних та необоротних активів підприємства відповідає нормативам, але в динаміці років має тенденцію до зменшення. Така ситуація є негативною, адже зменшення оборотних активів погіршує рівень фінансової стійкості підприємства.

Рівень співвідношення зобов’язань та власного капіталу значно нижче нормативного показника, має негативну динаміку розвитку. Така ситуація значно знижує рівень фінансової стійкості підприємства, адже збільшує залежність від зовнішніх джерел фінансування.

Наступним кроком стала оцінка фінансової стійкості за використання окремих коефіцієнтів, що запропоновані у першому розділі. Динаміка зміни показників фінансової стійкості "Нафтогаз України" за 2019-2022 роки представлена на Рисунок 2.2



	31.12.2019	31.12.2020	31.12.2021	31.12.2022
Коефіцієнт фінансової автономії	0,425	0,090	0,039	-0,179
Коефіцієнт фінансової заборгованості	0,575	0,910	0,961	1,179
Коефіцієнт фінансової залежності	2,352	11,094	25,716	-5,594
Коефіцієнт покриття боргу	0,740	0,099	0,040	-0,152

Рисунок 2.2 Динаміка показників фінансової стійкості "Нафтогаз України" у 2019-2022 роках

Аналіз фінансової стійкості проаналізованого підприємства показує, що коефіцієнт фінансової автономії НАК "Нафтогаз України" є низьким, оскільки компанія має низьку частку власного капіталу, яка значно зменшилася за останні роки.

Це також можна пояснити тим, що рівень фінансового боргу НАК "Нафтогаз України" стрімко зростав протягом багатьох років. Це означає, що борги значно перевищують власний капітал компанії. Рівень фінансової залежності показує, що залежність НАК "Нафтогаз України" від зовнішнього фінансування є досить високою і перевищує норму в 10 разів.

Крім того, рівень покриття боргу підприємства також є дуже низьким і знижувався протягом звітного року. Така ситуація є несприятливою для підприємства, оскільки наражає його на ризик банкрутства.

Динаміка зміни показників ліквідності та платоспроможності "Нафтогаз України" за 2019-2022 роки представлена на Рисунок 2.5

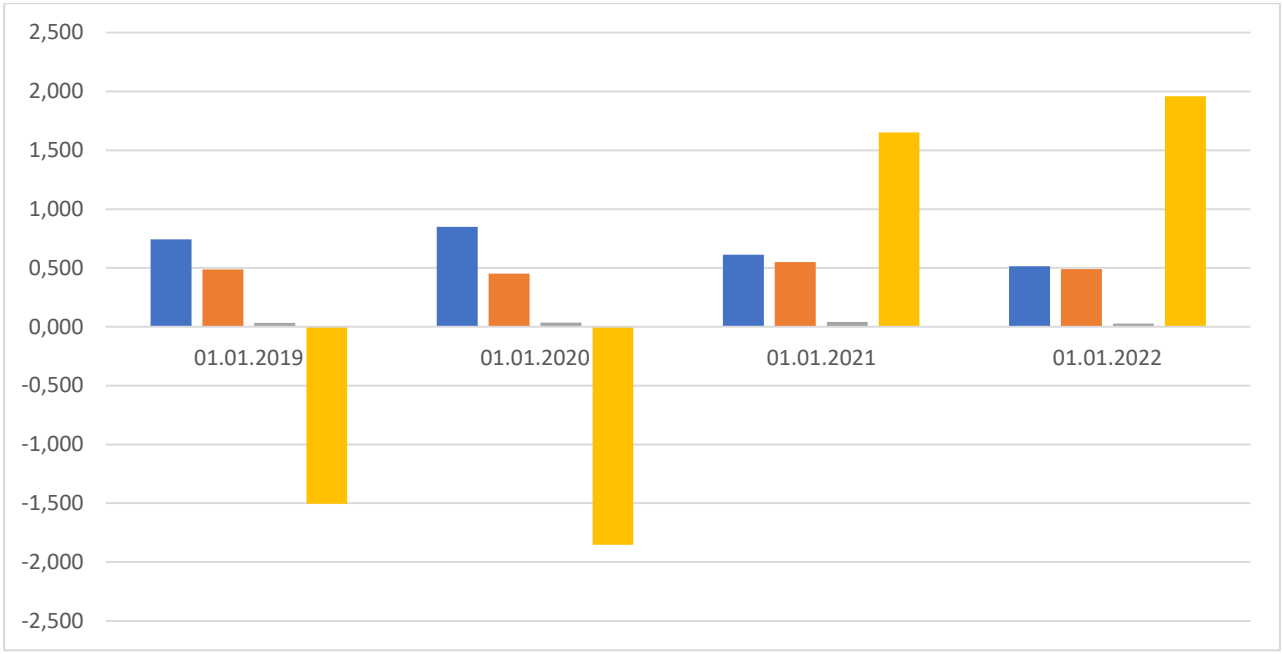


Рисунок 2.5 Динаміка показників ліквідності та платоспроможності "Нафтогаз України" у 2019-2022 роках

Аналіз ліквідності та платоспроможності НАК "Нафтогаз України" показує, що у 2019-2022 роках компанія формуватиме власний оборотний капітал за рахунок позикових коштів і не здійснюватиме жодних інвестицій за рахунок власних коштів. Про це свідчить показник власного оборотного капіталу у відсотках до закритих запасів, який залишається від'ємним з 2019 року і демонструє зростаючу негативну тенденцію. Це несприятливо для компаній, оскільки наражає їх на ризик ліквідності, ризик платоспроможності та, зрештою, ризик неплатоспроможності.

Загальний коефіцієнт покриття, який показує рівень ліквідності компанії, свідчить про те, що ліквідність НАК "Нафтогаз України" у звітному періоді є нижчою за встановлений законодавством ліміт і має тенденцію до зниження. Така ж тенденція спостерігається при аналізі проміжного коефіцієнту покриття та коефіцієнту абсолютної ліквідності.

Іншими словами, НАК "Нафтогаз України" є підприємством з низькою ліквідністю. Його платоспроможність також є низькою, про що свідчить недостатність його резервів для покриття поточних зобов'язань. Таким чином, НАК "Нафтогаз України" є компанією з низькою ліквідністю, а її платоспроможність знаходиться на критичному рівні.

Наступним відносним показником, що характеризує фінансову стійкість компанії, є рентабельність. Для того, щоб проаналізувати та оцінити прибутковість компанії, необхідно знати рівень та розмір прибутку компанії, а отже, необхідно оцінити формування чистого прибутку.

Відповідно аналіз фінансових результатів за елементами здійснюють відповідно з алгоритмом їх формування у фінансовій звітності (табл. 2.2).

Таблиця 2.2

Аналіз формування фінансових результатів "Нафтогаз України" у 2019-2022 роках

Показники	**Роки**				**Відхилення**	
	2019	2020	2021	2022	Відс. пунктів	%
1. Чистий дохід від реалізації	14636689	23983085	12724865	17849182	3212493,00	21,95
2. Собівартість реалізованої продукції	9769262	20853255	9629379	13118292	3349030,00	34,28
3. Адміністративні витрати	407867	560355	882786	1339817	931950,00	228,49
4. Витрати на збут	886315	1054480	1747148	2037403	1151088,00	129,87
5. Інші операційні витрати	844962	37382	9633612	14107664	13262702,00	1569,62
6. Інші операційні доходи	1983	900	119270	93134	91151,00	4596,62
7. Фінансові доходи	50102	20203	249360	44716	-5386,00	-10,75

продовження табл. 2.2

8. Фінансові витрати	1244033	2135532	1994562	2144444	900411,00	72,38
9. Фінансовий результат від операційної діяльності	-5322906	-6486383	-3559119	-1802639	3520267,00	-66,13
10. Податок на прибуток	-7094321	907622	7629	501	7094822,00	-100,01
11. Чистий прибуток	-12417227	-5578761	-3551490	1802138	-10615089,00	-85,49

Аналіз процесу формування результатів діяльності НАК "Нафтогаз України" показує, що суттєво зросли адміністративні витрати компанії - на 228,49%, витрати на збут-на 129,87% та інші операційні витрати-на 1569,62%. Водночас фінансовий дохід компанії зменшився(-10,75%). Загалом, фінансовий результат компанії збільшився з боку доходів, але повільнішими темпами, ніж з боку витрат.

Фінансовий результат від операційної діяльності суттєво зменшився (-66,13%) внаслідок значного збільшення витрат компанії, що призвело до збитковості компанії за 2019-2022 роки. Єдиним позитивним аспектом є те, що збиток компанії зменшився порівняно з попереднім роком. Однак це не є позитивним показником для діяльності компанії. Тому результати оцінки слід взяти до уваги та вжити відповідних заходів для зростання компанії та підвищення її прибутковості.

Однак слід зазначити, що абсолютні показники формування прибутку не дають повного уявлення про ефективність діяльності підприємства. Адже абсолютна величина прибутку відображає лише досягнутий підприємством ефект і не відображає рівень ефективності його господарської діяльності. Тому для характеристики ефективності господарської діяльності, рівня використання ресурсів

та раціональності понесених витрат широко використовуються відносні показники рентабельності.

Для досліджуваного підприємства пропонується розрахувати рентабельність господарської діяльності, рентабельність активів, рентабельність власного капіталу, рентабельність зобов'язань та рентабельність витрат і продукції для аналізованого підприємства.

Результати розрахунків рівня рентабельності реалізації для "Нафтогаз України" наведено в табл. 2.3

Таблиця 2.3

Показники рентабельності "Нафтогаз України" у 2019-2022 роках

Показники	Роки				Відхилення	
	2019	2020	2021	2022	Відс. пунктів	%
Рентабельність реалізації						
Рентабельність за валовим прибутком	0,333	0,131	0,243	0,265	-0,068	-20,298
Рентабельність за операційним прибутком	0,264	0,111	-0,141	0,036	-0,227	-86,297
Рентабельність за чистим прибутком	-0,848	-0,233	-0,279	-0,101	0,747	-88,099
Рентабельність власного капіталу						
Рентабельність власного капіталу	-4,123	-3,198	0,488	0,286	4,410	-106,946
Рентабельність позикового капіталу	-0,408	-0,129	-0,074	-0,039	0,370	-90,545
Рентабельність активів						

продовження табл. 2.3

Рентабельність активів	-0,372	-0,124	-0,087	-0,045	0,327	-87,989
Рентабельність необоротних активів	-0,613	-0,208	-0,163	-0,066	0,546	-89,217
Рентабельність оборотних активів	-0,945	-0,309	-0,187	-0,138	0,807	-85,429

Дослідження показало, що прибутковість продажів НАК "Нафтогаз України" демонструвала неоднорідну тенденцію протягом багатьох років. Рентабельність валового прибутку впала на 20,29%, що свідчить про неефективність збутової політики підприємства.

Рентабельність операційного прибутку та чистого прибутку також суттєво знизилася (-86,29% та-88,09% відповідно). Така тенденція була спричинена різким зростанням операційних витрат підприємства та зменшенням чистого прибутку.

Збитки, яких зазнав "Нафтогаз України" у 2019-2022 роках, призвели до зниження рентабельності власного капіталу та боргового навантаження компанії. Важливим кроком для компанії на цьому етапі буде зменшення залежності від зовнішніх джерел фінансування та підвищення ефективності використання наявних джерел фінансування.

Крім того, рентабельність активів відносно як основних, так і оборотних активів з роками знизилася. Це свідчить про неефективне використання наявних матеріально-технічних ресурсів компанії. На цю тенденцію негативно вплинуло значне подовження періоду окупності активів компанії.

Використання комп'ютерних комплексів підтримки диспетчерських рішень (КПДР), з інтерфейсами, подібними до реальних систем управління, може прискорити такі процеси навчання і зробити їх більш ефективними.

Впровадивши комплекси підтримки диспетчерських рішень на підприємствах, керівництво значно покращує професійний рівень операторів, які приймають рішення в результаті отримання, передачі й оброблення інформації САК.

2.2 Характеристика стану інформаційної безпеки на підприємстві

Відповідно до Технічного завдання на модернізацію на об'єкті КІІ організується доступ до мережі зв'язку міжнародного інформаційного обміну (Інтернет), отже, існують лінії зв'язку, що виходять за межі контрольованої зони (КЗ), що робить актуальною загрозу з боку зовнішнього порушника.

Загрози безпеки інформації в інформаційній системі можуть бути реалізовані такими видами порушників:

– спеціальні служби іноземних держав (блоків держав);

– терористичні, екстремістські угруповання;

– злочинні групи (кримінальні структури);

– зовнішні суб'єкти (фізичні особи);

– конкуруючі організації;

– розробники, виробники, постачальники програмних, технічних та програмно-технічних засобів;

– особи, які залучаються для встановлення, налагодження, монтажу, пусконалагоджувальних та інших видів робіт;

– особи, які забезпечують функціонування інформаційних систем або обслуговуючі інфраструктуру оператора (адміністрація, охорона, прибиральники та тощо);

– користувачі інформаційної системи;

– адміністратори інформаційної системи та адміністратори безпеки;

– колишні працівники (користувачі).

Як можливі цілі (мотивації) реалізації порушниками загроз безпеки інформації в інформаційній системі можуть бути:

– заподіяння шкоди державі, окремим її сферам діяльності або секторам економіки;

– реалізація загроз безпеці інформації щодо ідеологічних або політичним мотивам;

– організація терористичного акту;

– заподіяння майнової шкоди шляхом шахрайства чи іншим злочинним шляхом;

– дискредитація чи дестабілізація діяльності органів державної влади, організацій;

– отримання конкурентних переваг;

– впровадження додаткових функціональних можливостей у програмне забезпечення чи програмно-технічні засоби на етапі розробки;

– цікавість чи бажання самореалізації.

Метою визначення можливих способів реалізації загроз безпеці інформації є формування припущень про ці способи, описують послідовність дій окремих видів або груп порушників, та застосовувані порушниками методи та засоби для реалізації загроз безпеці інформації.

Зокрема будемо розглядати як КВОІ систему диспетчеризації АТ НАК «Нафтогаз України». Система диспетчеризації АТ НАК «Нафтогаз України» складається з локальних диспетчерських пунктів компресорних станцій (ДПКС). На цих об'єктах використовуються новітні інформаційні технології та засоби зв'язку.

Система керує та контролює технічні процеси. Вона також контролює транспортування та розподіл газу на всіх компресорних станціях та газорозподільчих станціях.

Основною функцією ДПКС є організація централізованого прийому, обробки та своєчасного доступу до технічної інформації з різних джерел.

ДПКС оснащена засобами контролю параметрів та самодіагностики, які здійснюються за допомогою відповідного програмного забезпечення.

Крім того, ДПКС постійно працює на резервних серверах збору та обробки даних.

Основними вимогами до комплексу системи диспетчеризації АТ НАК «Нафтогаз України» є:

1) безпечне зберігання та доступ до інформації;

2) працює в безперервному режимі;

3) автоматичне завантаження протягом періоду, що не перевищує п'яти хвилин, у разі збою апаратного або програмного забезпечення;

4) підключення та оновлення всіх параметрів програмного та апаратного забезпечення з використанням стандартних протоколів обміну інформацією;

5) оновлення поточної технічної інформації протягом періоду, що не перевищує однієї хвилини;

6) зберігання технічних параметрів у системі управління базами даних (СУБД) протягом періоду до одного року;

7) надання поточних та історичних параметрів у вигляді звітів, трендів, мнемо схем і таблиць на робочому місці оператора, на веб-сторінках на комп'ютерах у локальній мережі НАК "Нафтогаз України" або з використанням мережі Інтернет;

8) надання стандартизованих інструментів для формування звітів з використанням архівних даних;

9) дистанційне керування;

10) здійснення самодіагностики.

Склад системи:

-ДПКС «Яготин», м. Яготин Київської області (КС «Глушківська», контрольні пункти телемеханіки, газорозподільчі станції);

-ДПКС «Бердичів», с. Садки Житомирської області (КС «Бердичів», контрольні пункти телемеханіки, газорозподільчі станції);

-ДПКС «Гребенківська», м. Лохвиця Полтавської області (КС «Гребенківська»);

- ДПКС «Диканька», смт Диканька Полтавської області (КС «Диканька», контрольні пункти телемеханіки, газорозподільчі станції);

- ДПКС «Ромненська» (КС «Ромненська», контрольні пункти телемеханіки);

- КС «Боярка» (м. Боярка Київської області); - КС «Зіньків» (м. Зіньків Полтавської області);

-КС «Решетилівка» (смт Решетилівка Полтавської області); -КС «Красилів» (м. Красилів Хмельницької області);

- КС «Лубни» (м. Лубни Полтавської області);

-Центральний ДПКС «Київ».

Інформація з локальних ДПКС зберігається у центральному ДПКС «Київ». Під час цього процесу локальний архівний сервер передає дані до центрального архівного сервера за допомогою функції копіювання даних. Ця функція додатково підвищує надійність зберігання інформації.

Регіональні центри обробки даних зберігають дані в режимі реального часу і передають їх на регіональний архівний сервер, який, у свою чергу, передає їх у режимі реального часу до центрального київського центру обробки даних, який у процесі відтворює отримані дані за допомогою регіональних автоматизованих робочих місць (АРМ).

Центральний ДПКС «Київ» та кожна регіональна ДПКС та складаються з наступних елементів (Рисунок 2.2):

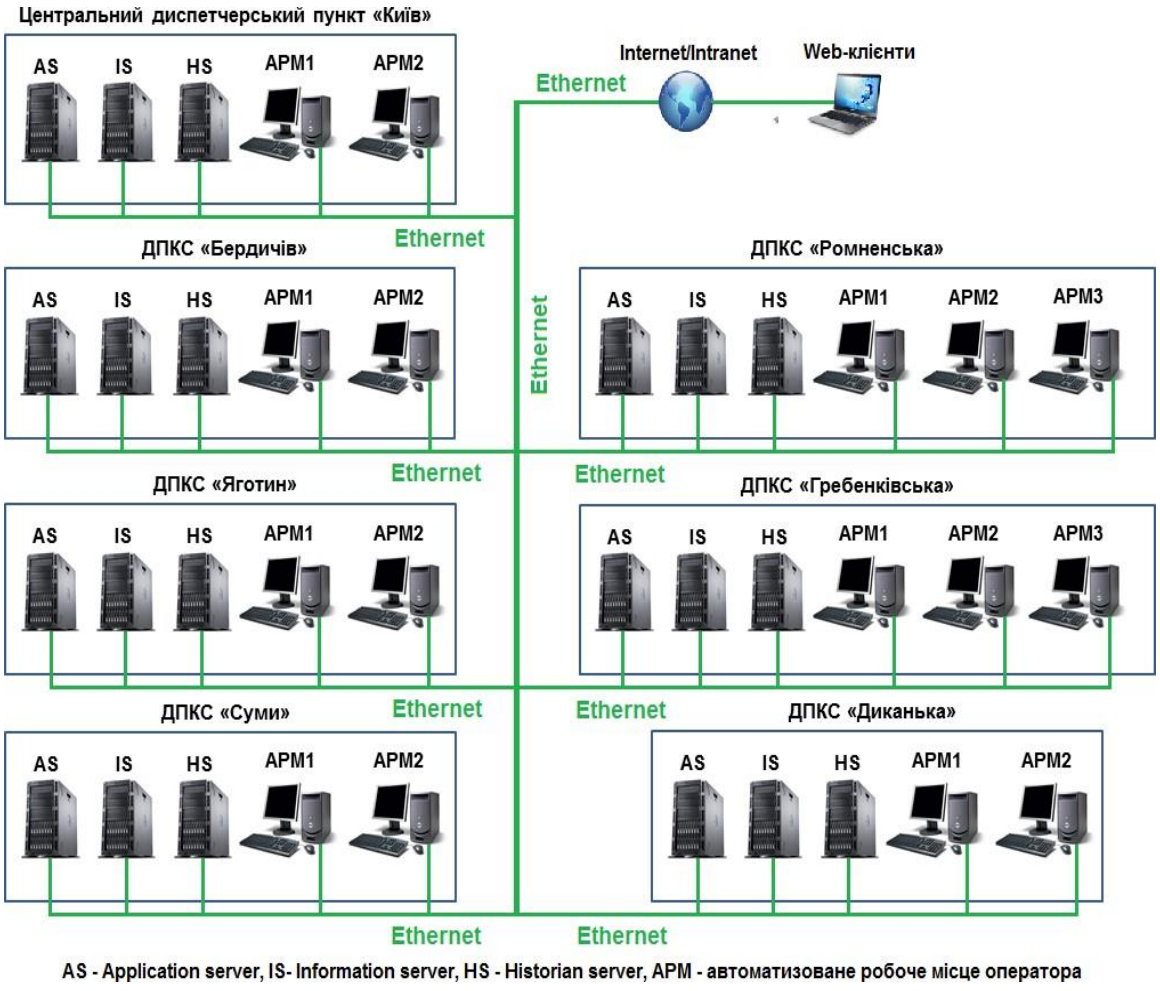


Рисунок 2.2 - Структура основних елементів (вузлів) системи

1. Сервер додатків (Application Server,AS)- основний сервер для зберігання та обробки інформації;

2. Сервер історій (Historian Server,HS)- сервер для зберігання архівної інформації;

3. Інформаційний сервер (Information Server,IS)- резервний сервер для зберігання та обробки інформації та має додаткову функцію надання інформації та архівних даних у режимі реального часу за допомогою веб-інтерфейсу;

4. Також має декілька автоматизованих робочих місць операторів для контролю та управління технічними процесами.

2.3 Оцінка політики інформаційної безпеки на підприємстві

Існуючі моделі оцінки ІБ підприємства як складника його стратегічного корпоративного управління в основному зосереджені або на продуктивності в конкретних галузях, таких як стратегія ІБ, політика ІБ, комплаєнс співробітників, управління вразливістю, програмне забезпечення та ін, або на продуктивності конкретних секторів економіки. Це спричиняє проблеми, пов'язані з відсутністю єдиної інформаційної політики безпеки, обмеженим використанням управління ризиками та несвоєчасним прийняттям рішень щодо управління вразливістю та інцидентами ІБ.

Вивчення існуючих кількісних моделей показало, що вони засновані переважно на оцінці управління інформаційною безпекою підприємства шляхом використання опитувань та показників самооцінки відповідності галузевим метрикам, які не дають загальну застосовну на практиці картину або вузько спрямовані на оцінку ризиків, результати якої важко застосовні для стратегічного управління розвитком підприємства у реальних умовах.

В авторській моделі для забезпечення постійного покращення результатів вимірювань використовуються ключові показники ефективності (KPI), які були

встановлені на основі нормативних вимог та міжнародних стандартів інформаційної безпеки (ISO/IEC 27k, COBIT та ін.).

Крім цього, модель забезпечує подання результатів для полегшення процесу прийняття рішень, оскільки менеджер отримує інформацію про конкретні проблеми та загальну позицію безпеки в організації, а отже, може ставити досяжні цілі та вибирати найкращі альтернативи, своєчасно коригуючи заходи впливу та оптимально перерозподіляючи доступні ресурси. Модель розглядає найбільш значущі фактори, що впливають на достовірність оцінки інформаційної безпеки підприємства як складника частини стратегічного корпоративного управління (табл. 2.5).

Таблиця 2. 5

Значні чинники успіху оцінки ефективності ІБ підприємства

№ п/п	Назва фактору	Опис фактору
1	Фізичний контроль інформаційної безпеки	Включає забезпечення заходів фізичної безпеки всередині та за межами організації за допомогою обмеження доступу до будівель та обладнання, контролю безпеки джерел інформації, контролю безпеки в прилеглих до об'єктів захисту районах.
2	Технічний контроль інформаційної безпеки	Полягає у контролі роботи інформаційних систем, виявленні аномалій та запобіганні несанкціонованим діям за допомогою накладання технічних обмежень на користувацькі можливості в межах використання даних, технічних засобів, додатків та мереж.

Продовження таблиці 2.5

3	Управління інформаційними ресурсами	Складається у підтримці конфіденційності та цілісності інформаційних ресурсів на всіх стадіях життєвого циклу інформації. Включає шифрування, створення резервних копій, безпечне знищення даних, організацію захищеного віддаленого доступу та інші аспекти.
4	Управління HR (Human resources)	Полягає у перевірці компетенцій та мотивів всіх користувачів, що взаємодіють з інформацією тимчасово або на постійній основі, проведення заходів підвищення рівня обізнаності щодо важливості інформаційної безпеки.
5	Управління інформаційними ризиками та обробка подій	Полягає у виявленні, аналізі та мінімізації ризиків інформаційного характеру за дотримання раціонального співвідношення між ризиками та інвестиційною привабливістю. Має на увазі реагування на події та ліквідацію загроз при появі.
6	Підтримка керівництва	Найбільша відповідальність у питаннях інформаційної безпеки на підприємстві покладається на керівництво, що зобов'язує його створити якісно організовані умови в поточній та стратегічній перспективах. Мається на увазі створення механізмів зворотний зв'язок між користувачами з метою формування потреб.

Продовження таблиці 2.5

7	Політика ІБ та комплаєнс	Полягає в нерозривності зв'язків між стратегією та політикою управління інформаційною безпекою, описі заборонених дій, обліку потреб користувача та дотриманні актуальних нормативних актів.
8	Ступінь зрілості управління безпекою	Передбачає необхідність високої оцінки рівня зрілості управління безпекою для забезпечення інформаційної безпеки, що може бути досягнуто за рахунок функціонування ІБ у формі окремого бізнес-процесу, та підтримці позитивних настроїв серед співробітників підприємства щодо політики ІБ.
9	Відносини з третіми особами	Включає аналіз уразливостей у рамках відносин із партнерами та клієнтами, дослідження ступеня розвиненості у питанні інформаційної безпеки. Має на увазі кооперацію між організаціями для створення спільного інформаційно-захищеного простору.
10	Зв'язок із зовнішнім середовищем	Потрібно враховувати такі глобальні сфери, як соціальна, економічна та політична при формуванні гнучкої системи інформаційної безпеки.

Сьогодні на промислових підприємствах здебільшого використовуються стандартизовані системи SCADA та системи промислового управління зі стандартизованими протоколами обміну даними.

Використання стандартизованих систем мережевого управління та передачі інформації підвищує ефективність за рахунок полегшення обміну даними між

системами на різних рівнях, але також збільшує потенціал мережевих загроз. Хоча ця проблема потребує термінового вирішення, нові безпечні SCADA-системи потребують тривалого часу для побудови та розгортання, тому на даному етапі необхідно шукати та усувати вразливі місця в безпеці інформаційних систем.

Сьогодні промислові системи спеціалізуються на мережевих технологіях, таких як Ethernet і TCP/IP. Ці технології широко використовуються в системах промислового управління і SCADA, створюючи необхідні умови для ефективної роботи підприємств і роблячи системи управління більш доступними.

Однак, крім переваг, інтеграція інформаційних мереж на різних рівнях підприємства в єдиний інформаційний простір призвела до значного підвищення вразливості системи до зовнішніх атак, мережевих черв'яків, вірусів і хакерів.

Для пояснення принципу побудови архітектури кіберфізичної безпеки наведемо цитату з публікації МАГАТЕ: «Розподіл обладнання на зони повинен бути належним чином задокументований, включаючи короткий огляд усіх комп’ютерних систем, усіх відповідних ліній комунікацій, усіх зональних перетинів і всіх зовнішніх підключень, а також враховуючи результати аналізу ризиків кіберфізичної безпеки, специфіки середовища та установок підприємства промисловості та транспорту».

На Рисунок 2.3 ЗДТУ – це засоби диспетчерського та технологічного управління.

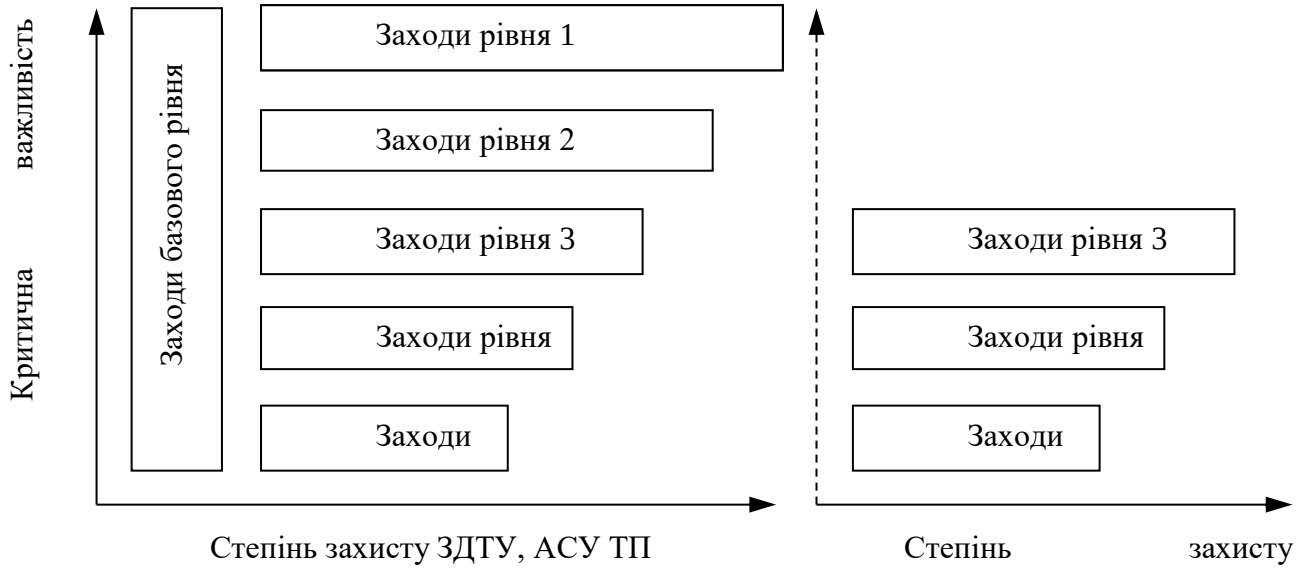


Рисунок 2.3 Рівень безпеки/дієвість заходів фізичної безпеки та безпеки засобів телекомунікацій

Нормами МАГАТЕ [МАГАТЕ STI/PUB/1527] надається приклад застосування моделі рівнів кіберфізичної безпеки. На основі цього прикладу покажемо рекомендований розподіл рівнів безпеки засобів телекомунікацій у координатах міри важливості систем для безпеки установки підприємства промисловості та транспорту та степені засобів захисту.

Для всього обладнання установки та засобів телекомунікації передбачено, що:

– заходи базового рівня слід застосовувати у відношенні всіх комп'ютерних та телекомунікаційних систем;

– рівні фізичної безпеки різні: від рівня 5 (необхідний найменший захист) і до рівня 1 (необхідний максимальний захист);

– рівні кібербезпеки засобів телекомунікацій різні: від рівня 5 до рівня 3;

– не допускаютьсяь прямі канали з'єднання, які проходять через декілька зон;

– заходи, що відповідають кожному рівню, не являються сукупними (тому можливі повторення).

– базовий рівень захисту повинен бути не меншим, ніж встановлений рівень захисту інформаційних систем, які використовуються у державних установах та підприємствах.

Аналіз поточного стану систем автоматичного керування газоперекачувальними агрегатами НАК "Нафтогаз України" показує, що 67% систем відпрацювали свій ресурс, а 17% відпрацюють свій ресурс протягом 1-3 років. Таким чином, 59% систем САК на компресорних станціях відпрацювали свій термін експлуатації, а 18% відпрацюють свій термін експлуатації. Відсутність запасних частин, а також відсутність деяких виробників САК та розробників програмного забезпечення для САК унеможливлюють забезпечення надійної роботи систем автоматизації.

Окрім того на 2019 рік доля вразливостей за виробником компонетів САК для АТ НАК «Нафтогаз України», а саме Schneider Electric склала – 47.

В системі на базі Wonderware System Platform 4.0 були виявлені вразливості, наслідком виконання атак на які буде можлива «Відмова в обслуговуванні» нашій системі, тобто зупинка постачання газу користувачам.

Зокрема, уразливість CVE-2011-2962 дозволяє віддаленим зловмисникам викликати переповнення буфера, що призводить до відмови в обслуговуванні. При цьому відбувається повне розкриття всіх системних файлів. Дана уразливість має високий рівень системної загрози (9.3 за шкалою CVSS).

Зловмисник може викликати переповнення буфера в стеку шляхом запиту неіснуючих файлів та виконати довільний код; може бути запущена серія атак на сервіси серверів АС, що використовують стек протоколів TCP/IP зі стандартними атаками на відмову в обслуговуванні, що може бути однією з найсерйозніших загроз для функціонування промислових мереж.

Атаки є багатогранними і можуть здійснюватися як на системи інформаційного забезпечення та рівня управління, так і на системи, непов'язані безпосередньо з програмним забезпеченням контролерів.

Для здійснення такої атаки необхідно використати вразливості в системі. Одна з них дозволяє використовувати XML-код у файлі як для порушення, так і для підтримки функціональності системи. Експерти Positive Research, дослідницького центру компанії Positive Technologies, виявили уразливість CVE-2013-0686, пов'язану з неправильною перевіркою даних в Wonderware Information Server.

Уразливість WIS дозволяє зловмисникам отримати доступ до локальних ресурсів (файлів та внутрішніх ресурсів) за допомогою небезпечної обробки зовнішніх XML-сутностей. Використовуючи спеціально створений XML-файл, зловмисник може відправити вміст локального або віддаленого ресурсу на власний сервер або викликати відмову в обслуговуванні (DoS).

В Wonderware Information Server також існує вразливість CVE-2014-2380,пов'язана з ненадійним шифруванням даних облікових записів. 35 Шифрування в WIS не є стандартизованим. Зловмисник може підвищити привілеї, розшифрувавши дані облікового запису. Ця атака вимагає, щоб система була скомпрометована.

За результатами оцінки, відповідно до переліку показників критеріїв значущості, масштабу можливих наслідків у разі виникнення комп'ютерних інцидентів на об'єктах критичної інформаційної інфраструктури об'єкту АТ НАК «Нафтогаз України» було присвоєно категорію значимості із найвищим значенням – 3 категорія значимості.

Видається доцільним дійти розуміння, що істотний негативний вплив на ІБ надають інформаційні ризики та некомпетентність в управлінні ними.

Використання представленої авторами моделі дозволить не просто з'ясувати поточний рівень інформаційної безпеки на сучасних підприємствах, а буде сприяти усуненню вразливостей у корпоративних інформаційних системах за допомогою таких дій, як:

– відстеження сучасних тенденцій та трендів на ринку ІБ;

– створення та підтримка функціонуючої системи управління безпекою;

- управління якістю;

– чіткий розподіл відповідальності між ролями, задіяними у забезпеченні інформаційної безпеки;

- тотальне поінформування користувачів про важливість ІБ;

- Впровадження ІБ у перелік стратегічних цілей;

– безперервне спостереження за процесами та результатами діяльності;

– створення та підтримка системи для комунікацій між користувачами.

Для цього пропонується:

– враховувати у стратегії розвитку підприємства потреба у забезпеченні незалежності управління його інформаційною безпекою поряд із потребою безперервного управління якістю;

– чітко регламентувати відповідальних за інформаційну безпеку та культуру, їх контроль та розвиток;

– поряд з метою забезпечення ефективності бізнес-процесів, ставити за мету забезпечення інформаційної безпеки підприємства, здійснювати її безперервний моніторинг та контроль, забезпечувати координацію між співробітниками, розуміння цілей та завдань, взаємозалежності стратегії безпеки та цілей організації.

Висновки за розділом 2

Отже, застосування комп'ютерних комплексів підтримки диспетчерських рішень (КПДР), з інтерфейсом, подібним до інтерфейсу реальної системи управління, зробить ці процеси навчання швидшими та ефективнішими. Впровадження диспетчерських систем підтримки прийняття рішень на підприємствах дозволяє керівництву значно підвищити професійний рівень осіб, які приймають рішення, в результаті отримання, передачі та обробки інформації САК.

Система диспетчеризації АТ НАК «Нафтогаз України» створена на базі Wonderware System Platform 4.0, програмного пакету, який забезпечує вищезгадані функції для розподілених систем управління.

Автоматизоване робоче місце оператора оснащене програмним забезпеченням In Touch for System Platform, яке гарантує людино-машинний інтерфейс в режимі реального часу.

Центральний ДПКС «Київ» а також кожна регіональна ДПКС поєднані в локальну обчислювальну мережу АТ НАК «Нафтогаз України».

Тому ефективна система менеджменту ІБ компанії має бути спрямована на мінімізацію ризиків реалізації бізнес-процесів, зростання інвестицій та їх рентабельності, забезпечення загального рівня конкурентоспроможності підприємства на основі аналізу процесів її інформаційних систем та їх розвиток.

РОЗДІЛ 3
ЕТАПИ ВДОСКОНАЛЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНОГО ПІДПРИЄМСТВА

3.1 Планування заходів із вдосконалення політики інформаційної безпеки

Відомо, що ДПКС системи диспетчеризації АТ НАК «Нафтогаз України» розподілені територіями Київської, Полтавської, Чернігівської, Хмельницької, Житомирської та Сумської областей і мають представництва у певних населених пунктах.

Центральне відділення, яке контролює роботу всієї системи диспетчеризації розташовано у Києві. Отже, система складається із c = 1,2,...,11 компонентів, які взаємодіють між собою.

Завдання полягає в побудові системи захисту інформації для описаної КВОІ, яка забезпечить здійснення функцій інформації: цілісність, конфіденційність та доступність даних.

Припускаємо, що інформація щодо обчислювального середовища та технологій обробки інформації є доступною і можливо потрапить до зловмисника.

Проведемо аналіз системи та виділимо її компоненти c на початковому етапі побудови СЗІ. Потрібно визначити цінність qc компонентів системи (КС) c, яка в подальшому буде використовуватися для оцінки можливих збитків.

Успішне здійснення загрози проти якогось з компонентів системи спричинить зупинку постачання газу користувачам (відмова в обслуговуванні), що еквівалентна цінності цього компонента для функціонування системи в цілому.

За відсутності статистичних даних та фінансових звітів, припустимо, що завданий збиток qc пропорційний кількості населенню району атакованої КС (табл. 3.1).

Таблиця 3.1

Компоненти системи (КС населеного пункту) с та їх цінності q_c

№ з/п	КС системи с	Цінність $\boldsymbol{qc}$
1.	Центральний диспетчерський пункт «Київ»	3635278
2.	КС «Боярка» (м. Боярка Київської області)	364941
3.	КС «Глушківська» (м. Яготин Київської області)	98695
4.	КС «Лубни» (м. Лубни Полтавської області)	493918
5.	КС «Гребінківська» (м. Лохвиця Полтавської області)	53407
6.	КС «Диканька» (смт Диканька Полтавської області)	330026
7.	КС «Зіньків» (м. Зіньків Полтавської області)	33815
8.	КС «Решетилівка» (смт Решетилівка Полтавської області)	11660
9.	КС «Роменська» (с. Миколаївка Сумської області)	148048
10.	КС «Бердичів» (с. Садки Житомирської області)	844578
11.	КС «Красилів» (м. Красилів Хмельницької області)	604336

Існує 3 моделі побудови системи захисту інформації :

AD («зловмисникзахисник»),

DA («захисник- зловмисник») та

DAD («захисник- зловмисникзахисник»), які застосовуються для вирішення проблем захисту конкретних об’єктів критичної інфраструктури.

Для нашої системи ми будемо застосовувати модель «захисник-зловмисник».

Для побудови цільової функції визначаються змінні. В розділі була здійснена побудова цільової функції для моделі системи захисту інформації «захисник-зловмисник». А саме – визначено множина загроз, множина профілів захищенності в

якості змінних. Було приведено і описано етапи проведення атаки зловмисником як кроки позиційної гри:

- Зловмисник проводить розвідку.

- Зловмисник проводить атаку.

-Зловмисник приховує сліди.

І, нарешті, отримано кінцеву цільову функцію для заданих обмежень (обмеження на кількість одночасно реалізованих загроз, обмеження на ресурси захисника).

3.2 Розробка системи інформаційної безпеки підприємства

Для побудови цільової функції маємо визначити змінні. Позначимо множину загроз, які можуть бути реалізовані в системі ДПКС та нанести їй збиток через a ∈ A, A={$a1,\ldots, an$ }.

Список можливих загроз складається, базуючись на вже існуючих вразливостях, що можуть бути застосовані зловмисниками різних типів (як внутрішніми, так і зовнішніми), із різним рівнем кваліфікації в сфері захисту інформації, різними правами доступу (від користувачів до адміністраторів), різними теоретичними та практичними знаннями.

Завданий збиток Qc , який виражається у виді витрат та втраченої вигоди є кількісною величиною для оцінки ризиків. Як наслідок, значення збитку Qc , що було спричинене певній КС с тотожне цінності даного компонента qc для роботи системи загалом.

Далі будемо вважати ці величини еквівалентними. Завдання захисника цієї системи зводиться до вибору функціональних профілів захищеності p ∈ P, P = {$p,\ldots, pm$} для кожної КС, які сприятимуть мінімізації збитків від можливих дій зловмисника за існуючих загроз та обмежень на впровадження системи захисту.

Подолання потенційних атак буде здійснюватися з використанням функціональних профілів захищеності p. Кожен із профілів захищенності може нейтралізувати одну чи більше загроз a із множини A.

Введемо матрицю захищеності D ={dap}, що відповідає за здатність певного профілю p протидіяти потенційній атаці a. Визначимо dap так: dap = 1, якщо механізм захисту p здатний протидіяти атаці a на КС (ймовірність виявлення або нейтралізацію загрози

а) dap = 0, інакше. В системі наявна певна статистична невизначеність, тобто відомо деякі ймовірності вибору стратегій захисником. Визначимо ймовірність впровадження загрози a на компресорній станції c як hac так що: hac = 1; якщо атака a на компресорну станцію c успішна; hac = 0, інакше.

Треба відобразити вплив стратегій захисника на ризик в системі. Для цього введемо додаткову змінну, що буде характеризувати здатність системи захисту протистояти атаці a на КС *c – Vac*.

Таким чином, (1 – Vac) можна інтерпретувати як існування незахищеної вразливості, яка може бути використана зловмисником. Загалом для функції ризику інформаційної безпеки *Rac* запишемо співвідношення у вигляді добутку ймовірності *Pac* реалізації загрози a та завданого збитку при реалізації цієї загрози Qc із урахуванням ймовірності нейтралізації загрози з використанням встановлених додаткових механізмів захисту Vac:

$$\text{Rac} = \text{Pac} \cdot \text{Qc} \cdot (1 - \text{Vac}) \qquad (3.1)$$

Будемо вважати, що атака зловмисника складається із K етапів, при цьому збиток буде завданий, за умови, якщо всі етапи завершено успішно. Тоді, ймовірність реалізації загрози представимо в виді добутка ймовірностей успішної реалізації кожного з етапів k.

Тоді, відповідно, співвідношення ризику:

$$\text{Rac} = \prod \textit{Pac}\ k \cdot \text{Qc} \cdot (\ 1 - \text{Vac}\ )\ K\ k{=}1 \qquad (3.2)$$

В співвідношенні (3.2) висвітлено динамічний характер поведінки системи, за умови зміни стану під дією кожної з сторін. З огляду на поетапність здійснення атаки,

опишемо відносини захисника та зловмисника, використовуючи позиційну гру, в якій учасники роблять ходи по черзі з намаганням досягти для себе максимальної користі.

Можемо виокремити такі етапи позиційної гри відповідно до етапів комплексної атаки:

- На першому етапі, метою якого є вивчення, аналіз та пошук вразливостей в системі захисту для здійснення атаки, зловмисник здійснює розвідку.

-Завданням захисника на даному етапі є попередження можливої атаки, через нейтралізацію вразливостей, а також викриття зловмисника.

-На другому етапі, використовуючи знайдену вразливість, зловмисник знешкоджує систему захисту та здійснює атаку. Таким чином, одна чи кілька фундаментальних властивостей інформації (конфіденційність, цілісність, доступність) зазнає порушень на цьому етапі.

-З метою нейтралізації небажаних дій захисник застосовує визначені заходи та засоби захисту.

-На завершальному етапі атаки зловмисник знищує сліди, які можуть його викрити. У випадку, якщо захисник зможе виявити та знешкодити зловмисника, може відбутися завершення гри на одному із ранніх етапів. Проте, якщо атака проведена успішно гра може бути завершена на останньому етапі.

Отже, апріорні ймовірності, відповідно до реалізації загроз $hac\ k$ та їх знешкодження $dap\ k$ можуть змінюватися з часом, і тому повинні задаватися для кожного з етапів k.

Виразимо цільову функцію через ризик інформаційної безпеки, яку захисник намагається зменшити, а зловмисник збільшити. Зловмисник обираючи стратегію дій оперує ймовірністю реалізації загроз: Pас k = hac k · уас k та потенційним збитком с Qc= q.

Захисник може зменшити ризик завдяки встановленню додаткових механізмів захисту: Vac = (∑ $dap\ k\ P\ p$=1 · $xcp\ k$) Якщо Vac = 1, то К с є повністю захищеною від загрози a .

У цьому випадку з метою недопущення встановлення надмірних засобів та заходів захисту застосовується обмеження $Vac \leq 1$.

Після підстановки визначених змінних в (3.2) та врахування мети захисника та зловмисника цільову функцію можна записати в такому вигляді:

$$R = min\ x\ max\ y \prod \sum \sum hac\ k\ c\ c{=}1\ A\ a{=}1\ K\ k{=}1 \cdot yac\ k \cdot qc \cdot (1 - \sum dap\ k\ P\ p{=}1 \cdot xcp\ k) \quad (3.3)$$

За наступних обмежень:

$\sum yac\ k\ a,c,k \le L$, де L – обмеження на кількість одночасно реалізованих загроз, $\sum wp \cdot xcp\ k\ c,p,k \le W$, де W – обмежені ресурси захисника, 40 $\sum dap\ k\ P\ p{=}1 \cdot xcp\ k \le 1$, $xcp\ k = \{0,1\}$, $yac\ k = \{0,1\}$.

Для розв'язання нелінійної задачі (3.3) спершу перейдемо до двоїстої, через введення змінної θ та фіксацію значень стратегій захисника

$$X : R = \min \theta \prod \sum \theta\ ac\ k\ k\ a,c \quad (3.4)$$

За обмежень: $\theta\ ac\ k \le hac\ k \cdot qc \cdot (1 - \sum dap\ k\ P\ p{=}1 \cdot xcp\ k)$, $\sum wp \cdot xcp\ k\ c,p,k \le W$, $\sum dap\ k\ P\ p{=}1 \cdot xcp\ k \le 1$, $\theta\ ac\ k \ge 0$.

Подальший розв'язок задачі (3.4) відбувається з використанням методу гілок та границь [14].

У результаті розв'язання отримуємо оптимальний набір рішень захисника $xcp\ k$ та зловмисника $yac\ k$.

3.3 Побудова моделі структури системи інформаційної безпеки підприємства

Формування моделі порушника є обов`язковим етапом створення політики безпеки. Зважаючи на запропоновану задачу, виникає необхідність у передбаченні захисту від зовнішніх порушників, які мають високу кваліфікацією та оснащені потрібними апаратними та програмними засобами для віддаленої реалізації загроз інформаційної безпеки.

Їх метою є: отримання доступу до закритої інформації; отримання можливості внесення відповідних змін до інформаційних потоків у відповідності до своїх намірів; перехоплення управління; виклик відмови в обслуговуванні.

За умови володіння інформацією про характерні особливості зловмисника та його мету виникає можливість вибору типових загроз інформаційній безпеці а, з використанням яких, порушник зможе досягнути поставленої цілі.

Запропонований підхід пропонує розглядати атаку у вигляді динамічного процесу. Тому виникає необхідність роподілу загроз на етапи *k* у такій послідовності, в якій вони будуть реалізовані зловмисником.

З огляду на зазначений вище підхід пропонуємо поділити процес здійснення загрози на 3 етапи (табл. 3.2).

Таблиця 3.2

Загрози інформаційній безпеці а та ймовірності їх виникнення $\boldsymbol{h}$а

Етап *k*	**№**	**Загрози** *a*	**Ймовірності реалізації** $\boldsymbol{h_a}$
1		**Розвідка**	
	4	Обхід механізмів захисту	0,7
2		**Проникнення**	
	1	Віддалене виконання коду	0,9
	3	Переповнення буфера	0,8
	6	Підробка міжсайтового запиту (XSS)	0,6
	7	Введення (залучення, впровадження) операторів SQL	0,5
3		**Реалізація мети**	
	2	Розкриття інформації	0,8
	5	Відмова в обслуговуванні(DDoS-атаки)	0,7

Припускаємо, що для кожного компоненту системи с застосовуються однотипні технології обробки інформації, а тому наявні вразливості до наведених загроз інформації, при цьому ймовірність здійснення загрози проти кожного з компонентів системи буде однакова ∀a, ∀c⇒$hac = ha$.

Для спрощення вважатимемо, що ймовірність реалізації загрози залежить лише від виду загрози, але не буде залежати від особливостей кожного компоненту, у крайньому випадку доки не буде реалізована система захисту інформації.

Вибір механізмів захисту, з орієнтацією на архітектуру обчислювального середовища та модель загроз є наступним етапом розробки політики безпеки. За допомогою методу експертної оцінки визначимо дієвість кожного із механізмів захисту p проти визначених загроз a в системі dap та вартість їх реалізації wp (табл. 3.3).

Кожен із механізмів захисту p забезпечує певний рівень захищеності.

Таблиця 3.3

Ймовірності dap знешкодження загрози a механізмом захисту p та вартість введення такого механізму w_p

№	**Механізми захисту *p***	**Індекси загроз інформаційній безпеці *a***								**Вартість реалізації wp**
		1	2	3	4	5	6	7	8	
1	Використання захищених протоколів доступу	0,8	0,9	0,4	0,9	0,7	0,8	0,7	0,8	15
2	Антивірусне ПЗ	0,1	0,9	0,3	0,9	0,3	0,8	0,6	0,1	10
3	Шифрування даних, що передаються	0,8	0,9	0,7	0,8	0,4	0,9	0,9	0,7	20

продовження табл. 3.3

4	Обробка всіх помилок і виключень	0,7	0,3	0,9	0,6	0,9	0,9	0,4	0,4	10
5	Оновлення вразливих версій ПЗ (Vulnerability management)	0,9	0,9	0,9	0,9	0,9	0,4	0,7	0,6	15
6	Екранування вхідних даних	0,8	0,3	0,8	0,8	0,8	0,7	0,9	0,3	20
7	Метод параметризації запитів	0,4	0,5	0,5	0,7	0,4	0,4	0,9	0,5	5
8	Багатофакторна автентифікація	0,7	0,6	0,3	0,6	0,4	0,8	0,3	0,9	10

Після отримання необхідних даних, перейдемо до вирішення поставленого завдання - визначення структури СЗІ, що забезпечить мінімальне значення цільової функції (3.2) при заданих обмеженнях (ресурси на побудову СЗІ).

Безпосередньо синтез СЗІ здійснюється з використанням співвідношення (3.3). Результатом цього є сукупність механізмів захисту {p} для кожної компресорної станції.

Через те що кількість можливих комбінацій, що аналізуються моделлю досягає значного числа, розв’язуючи цю задачу, використовувалися автоматизовані математичні пакети.

В результаті маємо рішення запропонованої задачі для 3 різних випадків - за умови різних витрат на системи захисту інформації W. (табл. 3.4).

Таким чином, на прикладі побудови СЗІ для САК критично важливої інфраструктури було продемонстровано практичну доцільність наведеного підходу. Низка здійснених експериментів засвідчила, що запропонована модель є адекватною для синтезу структури СЗІ та може бути застосована до систем підтримки прийняття рішень інформаційної безпеки.

Таблиця 3.4

Встановлені механізми захисту

Компонент системи c	**Сукупність механізмів захисту** $\{x_{cp}\}$		
Виділені ресурси (W)	500	800	1000
КС «Київ»	1,3,4,5,7,8	1,3,4,5,6,7,8	1,2,3,4,5,6,7,8
КС «Бердичів»	1,3,5,7,8	1,3,4,5,7,8	1,2,3,4,5,7,8
КС «Красилів»	1,3,4,6,7	1,3,4,5,6,7	1,3,4,5,6,7,8
КС «Лубни»	1,3,5,7,8	1,3,4,5,7,8	1,3,4,5,6,7,8
КС «Боярка»	1,4,6,7	1,3,4,6,7	1,3,4,5,6,7
КС «Диканька»	1,4,6,7	1,3,4,6,7	1,3,4,5,6,7
КС «Роменська»	1,3,4,7	1,3,4,6,7	1,3,4,5,6,7
КС «Глушківська»	1,4,7	1,4,6,7	1,3,4,6,7
КС «Гребінківська»	1,4,7	1,3,4,7	1,3,4,5,7
КС «Зіньків»	4,7	1,4,7	1,3,4,7
КС «Решетилівка»	4,7	4,7	1,4,7

Де 1,2,3,4,5,6,7,8 - механізми захисту p, що були визначені в таблиці 3.3.

Відомо, що ДПКС системи диспетчеризації АТ НАК «Нафтогаз України» розподілені територіями Київської, Полтавської, Чернігівської, Хмельницької, Житомирської та Сумської областей і мають представництва у певних населених пунктах.

Центральне відділення, яке контролює роботу всієї системи диспетчеризації розташовано у Києві. Отже, система складається із c = 1,2,...,11 компонентів, які взаємодіють між собою.

Завдання полягає в побудові системи захисту інформації для описаної КВОІ, яка забезпечить здійснення функцій інформації: цілісність, конфіденційність та доступність даних.

Висновки за розділом 3

Отже, було здійснено оцінку цінностей компонентів системи диспетчеризації АТ НАК «Нафтогаз України», яка в подальшому буде використовуватися для оцінки можливих збитків.

Успішна реалізація загрози проти одного із компонентів системи призведе до зупинки постачання газу користувачам (відмова в обслуговуванні), що еквівалентна цінності цього компонента для функціонування системи в цілому.

За відсутності статистичних даних та фінансових звітів, припустимо, що завданий збиток пропорційний кількості населення району атакованої КС в якості споживачів газу.

Далі було сформовано модель зловмисника та загроз. Володіючи інформацією про мету та характерні особливості зловмисника, є можливість обрати найбільш вірогідні загрози ІБ а, застосовуючи які, він, ймовірно, досягне поставленої мети. Базуючись на цьому та на вразливостях нашої САК було отримано ймовірності реалізації цих загроз.

Для побудови цільової функції визначаються змінні. В розділі була здійснена побудова цільової функції для моделі системи захисту інформації «захисник-зловмисник» А саме – визначено множина загроз, множина профілів захищенності в якості змінних. Було приведено і описано етапи проведення атаки зловмисником як кроки позиційної гри:

- Зловмисник проводить розвідку.
- Зловмисник проводить атаку.
-Зловмисник приховує сліди.

Отримано кінцеву цільову функцію для заданих обмежень (обмеження на кількість одночасно реалізованих загроз, обмеження на ресурси захисника).

Вибір механізмів захисту, з орієнтацією на архітектуру обчислювального середовища та модель загроз є наступним етапом розробки політики безпеки.

За допомогою методу експертної оцінки визначили дієвість кожного із механізмів захисту *p* проти визначених загроз a в системі $\boldsymbol{dap}$ та вартість їх реалізації $\boldsymbol{wp}$.

І, нарешті, було визначено структуру системи захисту інформації, яка забезпечить мінімальне значення цільової функції (3.2) при заданих обмеженнях (ресурси на побудову СЗІ).

ВИСНОВКИ

Отже, інформаційна безпека підприємства полягає у здійсненні цілеспрямованої діяльності органів управління та посадових осіб підприємства з використанням дозволених сил та засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування та динамічний розвиток

Вибудовуючи інформаційну систему та роблячи конкретні кроки, спрямовані на попередження загроз інформаційній безпеці, необхідно опрацьовувати заходи прямого захисту від відомих загроз та забезпечувати можливість оперативного реагування на ті загрози, котрим заходи захисту передбачені базовим регламентом. Для обох випадків існує низка загальних методів захисту, які забезпечують зниження шкоди, що завдається інформаційній системі внаслідок порушення інформаційної безпеки, дозволяють знизити ймовірність реалізації максимального широкого спектру загроз та убезпечити підприємство від різних зовнішніх атак та помилок внутрішніх користувачів. Відповідно до концепції інформаційної безпеки вони поділяються на апаратні, програмні та комунікаційні.

Забезпечення інформаційної безпеки має бути спрямоване насамперед на запобігання ризикам, а не на ліквідацію їх наслідків. Саме вжиття запобіжних заходів щодо забезпечення конфіденційності, цілісності, а також доступності інформації є найбільш правильним підходом у створенні системи інформаційної безпеки.

Сьогодні спостерігається критично високе значення інформаційних активів підприємств у контексті їх превалюючого значення стосовно вартості матеріальних ресурсів організації.

Враховуючи рівень сучасного розвитку інформаційних технологій, питання забезпечення захисту інформації стають однією з фундаментальних детермінантів економічної безпеки компанії. Інформаційна безпека є єдино можливим напрямом для запобігання завданню шкоди економічним інтересам компанії шляхом організації захисту від існуючих та потенційних загроз інформаційних ресурсів підприємства.

Група Нафтогаз - найбільша державна компанія в Україні. Це провідна компанія в паливно-енергетичному секторі України. Офіційна назва: Національна акціонерна компанія "Нафтогаз України" Група "Нафтогаз України" – вертикально-інтегрована нафтогазова компанія, яка займається розвідкою, розробкою, експлуатацією та облаштуванням родовищ, транспортуванням, зберіганням нафти і газу та постачанням їх споживачам.

За результатами оцінки, відповідно до переліку показників критеріїв значущості, масштабу можливих наслідків у разі виникнення комп'ютерних інцидентів на об'єктах критичної інформаційної інфраструктури об'єкту АТ НАК «Нафтогаз України» було присвоєно категорію значимості із найвищим значенням – 3 категорія значимості.

Для нашої системи ми будемо застосовувати модель «захисник-зловмисник».

Для побудови цільової функції визначаються змінні. В розділі була здійснена побудова цільової функції для моделі системи захисту інформації «захисник-зловмисник» А саме – визначено множина загроз, множина профілів захищенності в якості змінних. Було приведено і описано етапи проведення атаки зловмисником як кроки позиційної гри:

- Зловмисник проводить розвідку.

- Зловмисник проводить атаку.

-Зловмисник приховує сліди.

І, нарешті, отримано кінцеву цільову функцію для заданих обмежень (обмеження на кількість одночасно реалізованих загроз, обмеження на ресурси захисника).

Отже, було здійснено оцінку цінностей компонентів системи диспетчеризації АТ НАК «Нафтогаз України», яка в подальшому буде використовуватися для оцінки можливих збитків.

Успішна реалізація загрози проти одного із компонентів системи призведе до зупинки постачання газу користувачам (відмова в обслуговуванні), що еквівалентна цінності цього компонента для функціонування системи в цілому.

За відсутності статистичних даних та фінансових звітів, припустимо, що завданий збиток пропорційний кількості населення району атакованої КС в якості споживачів газу.

Далі було сформовано модель зловмисника та загроз. Володіючи інформацією про мету та характерні особливості зловмисника, є можливість обрати найбільш вірогідні загрози ІБ a, застосовуючи які, він, ймовірно, досягне поставленої мети. Базуючись на цьому та на вразливостях нашої САК було отримано ймовірності реалізації цих загроз.

Вибір механізмів захисту, з орієнтацією на архітектуру обчислювального середовища та модель загроз є наступним етапом розробки політики безпеки.

За допомогою методу експертної оцінки визначили дієвість кожного із механізмів захисту *p* проти визначених загроз a в системі $\boldsymbol{dap}$ та вартість їх реалізації $\boldsymbol{wp}$.

І, нарешті, було визначено структуру системи захисту інформації, яка забезпечить мінімальне значення цільової функції (3.2) при заданих обмеженнях (ресурси на побудову СЗІ).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бірюков Д.С. «Про доцільність та особливості визначення критичної інфраструктури в Україні». Аналітична записка. URL: http://www.niss.gov.ua/articles/1026/

2. Баскаков В. Ю. Інформація з обмеженим доступом: поняття та ознаки. Актуальні проблеми державотворення (Імперативи розвитку юридичної та безпекової науки ; № 9): матеріали наук.-практ. конф., м. Київ, 28 черв. 2021 р. Київ, 2021. – С. 47–49.

3. Баскаков В. Ю. Адміністративно-правовий режим інформації з обмеженим доступом : автореферат дис. ... канд. юрид. наук : 12.00.07. Київ, 2016. 24 с.

4. Біла книга. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні. Матеріал для обговорення (Policy Paper) - UPL: parlament.org.ua › 2017/12 › au_White-book-on-cybersecurity-draft_

5. Бакалинський О.О. «Інформаційний бліцкриг». Правова інформатика, № 2(42)/2017, UPL.: http://ippi.org.ua/sites/default/files/14booib.pdf.

6. Бобро Д.Г., Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети, № 4 (37), 2015 р., Серія «Економіка», стор. 83-93. URL:http://sp.niss.gov.ua/content/articles/files/10-1457002140.pdf

7. Гізун А.І. Сучасні підходи до захисту інформаційних ресурсів для забезпечення безперервності бізнесу / А.І. Гізун, В.О. Гнатюк, О.П. Дуксенко, А.О. Корченко // Матеріали X Міжнародної науково-технічної конференції «АВІА-2011». - К.: НАУ, 2021. - Т1 - с. 2.5-2.9. URL: http://avia.nau.edu.ua/doc/2021/2/avia2011_2_2.pdf

8. Дімчогло М. І. Консолідація інформаційного законодавства України : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2017. 18 с.

9. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки». 27.12.2016. № 448 http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128

10. Золотар О. О. Обмеження доступу до інформації: інформаційно-правовий аспект. URL: http://archive.nbuv.gov.ua/portal/soc_gum/iblsd/2012_1/_private/13zooala.pdf.

11. Зелена книга з питань захисту критичної інфраструктури в Україні. 2015 р. URL:http://www.niss.gov.ua/public/File/2015_nauk_an_rozrobku/Green%20Paper% 20-%20dopovid.pdf

12. Корченко А. О. Метод оцінки рівня критичності для систем управління кризовими ситуаціями / А. О. Корченко, В. А. Козачок, А. І. Гізун // Захист інформації. - 2017. - Т. 17, № 1. - С. 86-98. URL:http://nbuv.gov.ua/UJRN/Zi_2015_17_1_14.

13. Компанія [Електронний ресурс]. – 2012. URL:http://www.naftogaz.com/www/3/nakweb.nsf/0/3A25D65C2606A6C9C22570D800 3 18869?OpenDocument.

14. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. ... д-ра юрид. наук : 12.00.07. Харків, 2018. 31 с.

15. Ліпкан В. А, Капінус Л. І. Доступ до інформації з обмеженим доступом: Проблеми вироблення уніфікованих дефініцій. Науково-практичний юридичний журнал «Публічне право» Київ, 2013. № 4. С 45–53.

16. Марущак А. І. Слова свободи та інформація з обмеженим доступом: співвідношення понять. Наукове фахове видання «Бюлетень міністерства юстиції України». Київ, 2018. № 6. С. 44–49

17. Нафтогаз України URL:https://uk.wikipedia.org/wiki/%D0%9D%D0%B0%D1%84%D1%82%D0%BE%D0 %B3%D0%B0%D0%B7_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%B D%D0%B8

18. Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи, Постанова Кабінету Міністрів України; Концепція від 20.01.1997 № 40. URL: https://zakon.rada.gov.ua/laws/term/40-97-%D0%BF.

19. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. № 537-V. Відомості Верховної Ради України (ВВР), 2007, № 12, ст.102

20. Про Стратегію кібербезпеки України: Указ Президента №96/2016 від 15.03.2016. UPL: https://zakon.rada.gov.ua/laws/show/96/2016

21. Про основні засади забезпечення кібербезпеки України: Закон України № № 2163-VIII від 05.10.2017 р. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403

22. Про кіберзлочинність. Конвенція Ради Європи від 21.11.2001. //Офіційний вісник України від 10.09.2007р., № 65, стор. 107, стаття 2535, код акту 40846/2007.

23. Про захист прав людини і основних свобод. Європейська конвенція. від 04.11.1950. Офіційний вісник України від 16.04.1998., № 13, / № 32 від 23.08.2006 / стор. 270.

24. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 07.11.2018, № 2155-VIII. Відомості Верховної Ради України (ВВР), 2006, № 30, ст.258

25. Про Національний банк України. Закон України від 20.5.1999 № 679 – XIV. Відомості Верховної Ради України (ВВР), 1999, № 29, ст.238.

26. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Постанови Кабінету Міністрів України № 518 від 19 червня 2019 року.Офіційний вісник України від 02.07.2019. 2019, № 50, стор. 53, стаття 1697, код акту 94896/2019.

27. Службова інформація: порядок віднесення та доступу. Практичний посібник ; за ред. Д. М. Слизьконіс. Київ : Центр політичних студій та аналітики, 2014. 76 с.

28. Серьогін В. О. Конституційний принцип гласності у діяльності органів державної влади України : автореф. дис. ... канд. юрид. наук : 12.00.02. Харків, 2019. 18 с.

29. Угода про Асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27.06.2014./Офіційний вісник України від 26.09.2014 — 2014, № 75, том 1, стор. 83, стаття 2125.

30. Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity

certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union. L 151/15, 7.6.2019

31. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88

32. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. OJ L 194, 19.7.2016, p. 1–30

33. Risk assessment methodologies for critical infrastructure protection. Part I: a state of the art / G.Giannopoulos, R.Filippini, M. Schimmer. – Luxembourg: Joint Research Centre of Institute for the Protection and Security of the Citizen, 2012. – 70 p.

34. Lewis T.G., Critical infrastructure protection in homeland security: defending a networked nation. - John Wiley & Sons, Inc., 2016. – 474 p.