МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “УПРАВЛІННЯ ПОЛІТИКОЮ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

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

Єлизавета МЕЛЬНИКОВА
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконала: здобувачка вищої освіти гр. УБД 41

Єлизавета МЕЛЬНИКОВА

Керівник:
К.е.н., доцент Тетяна КАПЕЛЮШНА

Рецензент:
Д.т.н., професор Галина ГАЙДУР

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УІКБ
_____Світлана ЛЕГОМІНОВА
“_____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці Мельниковій Єлизаветі Дмитрівні
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Управління політикою захисту інформаційної безпеки підприємства”

керівник кваліфікаційної роботи КАПЕЛЮШНА Тетяна, к.е.н, доцент
(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “07“ березня 2024 р. №195.

2. Строк подання кваліфікаційної роботи “25” травня 2024 р
3. Вихідні дані до кваліфікаційної роботи: нормативно-правові акти, законодавство щодо інформаційної безпеки, аналітичні звіти компанії про інформаційну безпеку підприємства, наукові статті та публікації українських та зарубіжних вчених.
4. Перелік питань, які потрібно розробити:
    1. Ознайомитися з основними теоретичними положеннями політики інформаційної безпеки та інформаційними активами, що підлягають захисту на підприємствах
    2. Розглянути основні правила оновлення політики захисту інформаційної безпеки на досліджуваному підприємстві
    3. Розробити пропозиції щодо удосконалення політики інформаційної безпеки підприємства та управління нею
    4. Оцінити ефективність пропозицій щодо удосконалення політики інформаційної безпеки підприємства та управління нею.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання “22” лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	13.03.2024	виконано
2.	Збір та аналіз літератури.	30.03.2024	виконано
3.	Проведення огляду та аналізу інформаційної безпеки підприємства	08.04.2024	виконано
4.	Внесення пропозицій щодо удосконалення інформаційної безпеки для поліпшення зальної політики захисту інформації на підприємстві	22.04.2024	виконано
5.	Оцінювання ефективності пропозицій щодо удосконалення політики інформаційної безпеки підприємства та управління нею	09.05.2024	виконано
6.	Формулювання висновків на основі отриманих результатів дослідження.	15.05.2024	виконано
7.	Оформлення роботи.	17.05.2024	виконано
8.	Оформлення презентації.	19.05.2024	виконано
9.	Отримання рецензії на роботу.	03.06.2024	виконано
10.	Захист в ЕК.	___.06.2024	виконано

Здобувачка вищої освіти _____ Єлизавета МЕЛЬНИКОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Мельникова Є.Д. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою)
на тему: "Управління політикою захисту інформаційної безпеки підприємства"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувачка **МЕЛЬНИКОВА Єлизавета** у кваліфікаційній роботі відповідно до обраної теми, визначила напрями, методи дослідження для опрацювання питань за темою та вирішення поставлених завдань. **МЕЛЬНИКОВА Єлизавета** продемонструвала розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довела здібності до опрацювання матеріалів, їх аналізу та побудови висновків, проявила себе як організована, відповідальна виконавиця.

Результати дослідження апробовані на конференції, що доводить практичну значимість отриманих результатів.

Вищевикладене дозволяє оцінити виконану кваліфікаційну роботу здобувачкою **МЕЛЬНИКОВОЮ Єлизаветою** на оцінку "відмінно" та присвоїти їй кваліфікацію "Бакалавр з кібербезпеки" за освітньо-професійною програмою "Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"___"____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Мельникова Є.Д. допускається дозахисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувачки вищої освіти Мельникової Єлизавети Дмитрівни
на тему: "Управління політикою захисту інформаційної безпеки підприємства"

Актуальність. Надскладні умови функціонування, в яких перебувають підприємства, потребують постійного моніторингу та оцінки їх безпеки. Інформаційна безпека підприємств окреслює нове бачення його в системі управління безпекою. Безперечним є зростанні ваги безпеки інформації в часи постійних інформаційних викидів та неправдивої інформації щодо умов функціонування підприємства та результатів діяльності, що суттєво відображається на сприйнятті підприємства клієнтами та оточенням. Тому актуалізується питання захисту інформації, яке має гуртуватися на особливостях роботи підприємства, інформаційних активах, що ним використовуються, від чого залежить побудова політики управління інформаційною безпекою підприємства.

Позитивні сторони

1. Позитивно відзначається послідовність розкриття теми, охоплення теоретичних напрацювань та аналітичних даних щодо функціонування підприємства, що сприяло якісному виконанню роботи. Чітко визначені завдання й їх виконання дозволили досягнути поставленої мети.
2. Аргументовано доцільність пропозицій через оцінку ефективності пропозицій щодо удосконалення політики інформаційної безпеки підприємства та управління нею.
3. Робота оформлена відповідно до вимог, що висуваються до написання кваліфікаційних бакалаврських робіт. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Основні положення роботи представлено у вигляді рисунків, таблиць. Опрацьовано достатню та актуальну інформацію із наукових джерел, статистичних звітів.

Недоліки

1. Варто приділити увагу регуляторним питанням захисту інформації, проте це не є вагомим недоліком та суттєво не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науковому рівні, заслуговує позитивної оцінки, а здобувачка Мельникова Єлизавета Дмитрівна заслуговує присвоєння кваліфікації "Бакалавр кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою"

Рецензент: завідувач кафедри Інформаційної та кібернетичної безпеки, д.т.н, професор — Галина ГАЙДУР

підпис *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра складається з 65 сторінок, включає 14 рисунків, 13 таблиць та базується на 23 джерелах.

Метою роботи є дослідження питань управління політикою захисту безпеки підприємства.

Об'єктом дослідження є політика інформаційної безпеки компанії.

Предметом дослідження **-** політика інформаційної безпеки на цьому підприємстві.

Застосовані методи дослідження включають аналіз, синтез, дедукцію, приведення техніко-економічних характеристик, розрахунок ефективності, прогнозування.

Метою дослідження є розробка пропозицій удосконалення інформаційної безпеки підприємства для поліпшення загальної політики захисту інформації на підприємстві та управління нею.

Короткий зміст роботи. У роботі вивчено політику інформаційної безпеки на підприємстві та її складові, її ключове місце в політиці управління компанією. Проведено аналіз даних підприємства, порівняльний аналіз методів та засобів захисту на підприємстві. Розглянуто шляхи удосконалення управління політикою інформаційної безпеки, включаючи виявлення прогалин, розробку методів та їх застосування до запобігання подальших збитків. Висновки підкреслюють важливість управління політикою інформаційної безпеки підприємства. Кінцеві висновки акцентують актуальність теми та її практичну значущість, додається перелік посилань та демонстраційні матеріали.

Галузь застосування. Запропоновані рекомендації до управління політикою інформації можуть бути використані для дослідження концепції з покращення захисту інформації та для впровадження вдосконаленої політики інформаційної безпеки.

КЛЮЧОВІ СЛОВА: МЕТА ЗАХИСТУ БЕЗПЕКИ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНА БЕЗПЕКА, КОМПАНІЯ, ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ , ІНФОРМАЦІЙНІ АКТИВИ.

ABSTRACT

The textual part of the bachelor's degree qualification work consists of 65 pages, includes 14 figures, 13 tables, and is based on 23 sources.

The aim of the work is to study issues related to managing the company's information security policy.

The object of the study is the company's information security policy.

The subject of the study is the peculiarities of enterprise security management.

The research methods applied include analysis, synthesis, deduction, technical and economic characteristics, efficiency calculation, and forecasting.

forecasting.

Brief content of research is to examine the peculiarities of managing the company's information security policy and develop proposals to eliminate losses and damages.

Summary of the work. This study focuses on analyzing the information security policy within an enterprise and its essential role in the company's management practices. A comprehensive data analysis of the enterprise was conducted, along with a comparative assessment of the methods and tools used for protection. The study also explores strategies for enhancing the management of information security policies, such as identifying gaps, developing methodologies, and implementing preventive measures to minimize future losses. The findings underscore the critical importance of effectively managing the company's information security policy. The concluding remarks reaffirm the relevance and practical significance of the topic, supported by a list of references and accompanying materials for demonstration.

Field of research. The proposed recommendations for managing information policy can be applied to research the concept of improving information protection and

implementing enhanced information security measures.

KEYWORDS: OBJECTIVE OF INFORMATION SECURITY PROTECTION, INFORMATION SECURITY, COMPANY, INFORMATION SECURITY POLICY, INFORMATION ASSETS.

ЗМІСТ

ВСТУП

Актуальність теми. Розвиток новітніх інформаційних технологій та еволюція комп'ютерних систем зберігання та обробки інформації потребують вдосконалення захисту та розробки ефективних механізмів, адаптованих під сучасні методи зберігання даних. Поступово захист інформації стає обов'язковим: розробляються численні документи, що стосуються безпеки інформації, формуються рекомендації з захисту даних, наводиться Закон України "Про інформацію", який розглядає та регулює відносини щодо створення, зберігання, збирання, використання, поширення, охорони, захисту інформації.

Забезпечення безпеки інформації на підприємстві є обов'язковим процесом, який вимагає впровадження новітніх технік для контролю внутрішнього та зовнішнього середовища підприємства, організацію заходів для підтримки стабільної роботи локальної мережі та обчислювальних систем, також мінімізацію ризиків через можливий витік інформації. Для ефективного захисту інформації, як у мережах так і в виробничих системах, підприємство має створити спеціальні правила та нормативні акти. Ці документи мають визначати обов'язки персоналу в сфері безпеки та деталізувати використання технічних і програмних засобів захисту. Сукупність цих документів називають політикою інформаційної безпеки.

Основною метою політики захисту інформації є зменшення ризику витоку інформації, а також забезпечення стабільної праці інформаційних систем підприємства. З урахуванням того, що витік інформації може привести до значних фінансових втрат, слід приділяти належну увагу зміцненню інформаційної безпеки. В умовах збільшення загроз інформаційній безпеці, забезпечення захисту даних стало ключовим елементом стратегії кожного підприємства. Це означає, що захист інформації реалізується з метою відокремлення ефективно працюючих систем від небажаного втручання, та

запобігання несанкціонованого доступу до даних для використання.

Мета роботи розробка пропозицій удосконалення інформаційної безпеки підприємства для поліпшення загальної політики захисту інформації на підприємстві та управління нею.

Об'єктом дослідження політика інформаційної безпеки на підприємстві.

Предметом дослідження особливості забезпечення та управління політикою захисту інформації на підприємстві «Будівельний альянс».

Для досягнення мети потрібно вирішити наступні завдання:

1. Ознайомитися з основними теоретичними положеннями політики інформаційної безпеки та інформаційними активами, що підлягають захисту на підприємствах
2. Розглянути основні правила оновлення політики захисту інформаційної безпеки на досліджуваному підприємстві
3. Розробити пропозиції щодо удосконалення політики інформаційної безпеки підприємства та управління нею
4. Оцінити ефективність пропозицій щодо удосконалення політики інформаційної безпеки підприємства та управління нею.

Практичне значення полягає у тому, що розроблені пропозиції управління політикою інформаційної безпеки можуть бути використані на практиці діючого підприємства.

Апробація результатів. Результати кваліфікаційної роботи було апробовано та оприлюднено на III Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» (тези: «Ключові аспекти політики щодо захисту інформаційної безпеки підприємства»).

РОЗДІЛ 1
АНАЛІЗ СИСТЕМИ ЗАХИСТУ ДАНИХ ПІДПРИЄМСТВА

1.1 Основні положення політики інформаційної безпеки підприємства

Основні принципи політики інформаційної безпеки підприємства відображаються у комплексі документів, що дозволяють відобразити вимоги до забезпечення захисту даних та основні напрямки підприємства забезпечення безпеки.[1] При створенні політики безпеки можна виділити три основні рівні: верхній, середній та нижній.

Верхній рівень політики безпеки даних організації дозволяє:[2]

- сформулювати та демонструвати ставлення адміністрації підприємства до системи захисту інформації та відобразити основні цілі та завдання в цій області;
- розробити індивідуальні політики безпеки, інструкції та правила, за допомогою яких регулюються окремі питання;
- інформувати співробітників організації про основні завдання та пріоритети в області інформаційної безпеки.

Політика інформаційної безпеки середнього рівня служить для відображення відносин та вимог підприємства до: використання інформаційних систем; телекомунікаційних і інформаційних технологій, методів та підходів до обробки інформації; учасників процесів обробки інформації, від яких залежить забезпечення захисту інформації на підприємстві.

Нижній рівень політики безпеки служить для опису конкретних процедур та документів для забезпечення інформаційної безпеки на підприємстві.

Етапи розробки політики безпеки в організації включають:

- виконання оцінки особистого ставлення до загроз безпеки з боку власників та співробітників підприємства;
- проведення аналізу потенційно важливих інформаційних активів підприємства;
- виявлення існуючих загроз безпеки підприємства з подальшою оцінкою ризиків.

При створенні політики безпеки на всіх рівнях необхідно дотримуватися того, що розроблена політика безпеки на нижньому рівні повинна відповідати політиці безпеки, наведеній на верхньому рівні. При цьому в тексті політики безпеки повинні бути викладені правила, які не мають подвійного значення, і вона повинна бути достатньо зрозумілою для співробітників підприємства. Важливе значення для захисту інформації в компанії має політика безпеки, яка представлена у вигляді логічно та семантично пов'язаних, формованих і аналізованих структур даних, що використовуються для захисту інформації на всіх рівнях функціонування підприємства.

Розглянемо основні складові політики інформаційної безпеки підприємства. Під захистом у даному випадку розуміється використання наведених у політиці безпеки організаційних заходів захисту інформації. За допомогою політики інформаційної безпеки на підприємствах здійснюють зовнішній і внутрішній аудит захисту даних, результати якого використовуються для визначення рівня ефективності, використовуваних методів та засобів захисту. Зокрема, покращення виражається у вигляді налаштування заходів політики безпеки з використанням отриманих результатів проведення тестування та моніторингу.[3] Політика безпеки в процесі функціонування підприємства повинна постійно оновлюватися. При цьому внесені зміни підлягають постійному порівнянню з тими методами та засобами, які вже використовуються. Основні складові політики інформаційної безпеки підприємства можна представити у вигляді схеми, наведеної на рисунку 1.1.

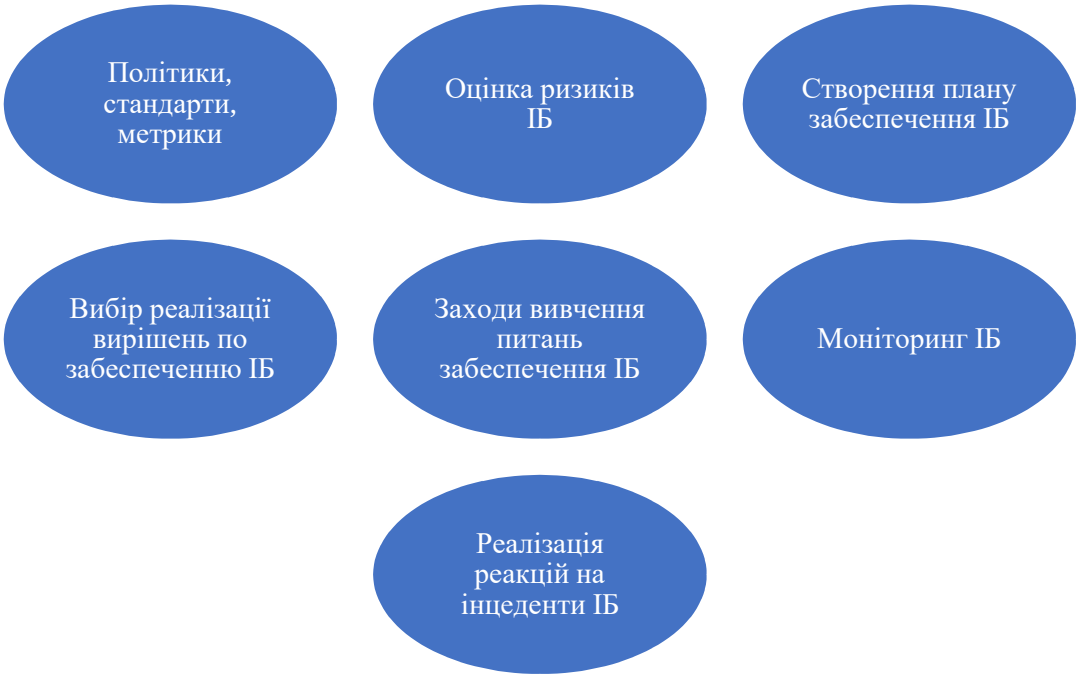

Рис. 1.1. Основні складові політики інформаційної безпеки підприємства

Як видно з рисунка 1.1, політика інформаційної безпеки відображає взаємопов'язані етапи організації інформаційної безпеки підприємства, які представлені процедурами, що дозволяють систематизувати та ефективно розв'язувати поставлені завдання для досягнення вимог захисту даних.

На першому етапі необхідно визначити межі, в рамках яких буде функціонувати політика інформаційної безпеки підприємства, сформулювати критерії для оцінки результатів.

На етапі аналізу ризиків інформаційної безпеки описується склад і визначаються пріоритети обраних засобів захисту з розподілом їх за ступенем важливості для підприємства, ідентифікуються вразливості активів підприємства та визначається збиток. Результати аналізу ризиків інформаційної безпеки підприємства будуть використовуватися у вигляді основи для планування роботи системи інформаційної безпеки, вибору найбільш ефективної стратегії та тактики. Для підвищення ефективності політики безпеки застосовуються такі методи як групове визначення об'єктів безпеки, опосередковане визначення з використанням довірених атрибутів та мандатне

керування доступом.

Багато підприємств використовують глобальні та локальні політики безпеки, що базуються на принципах управління безпекою інформації. Глобальна політика інформаційної безпеки спрямована на забезпечення захисту інформації на рівні бізнес-процесів компанії, а локальна політика формується на рівні захисту даних підприємства. У загальному вигляді глобальну політику безпеки можна представити у вигляді структури, наведеної на рисунку 1.2.

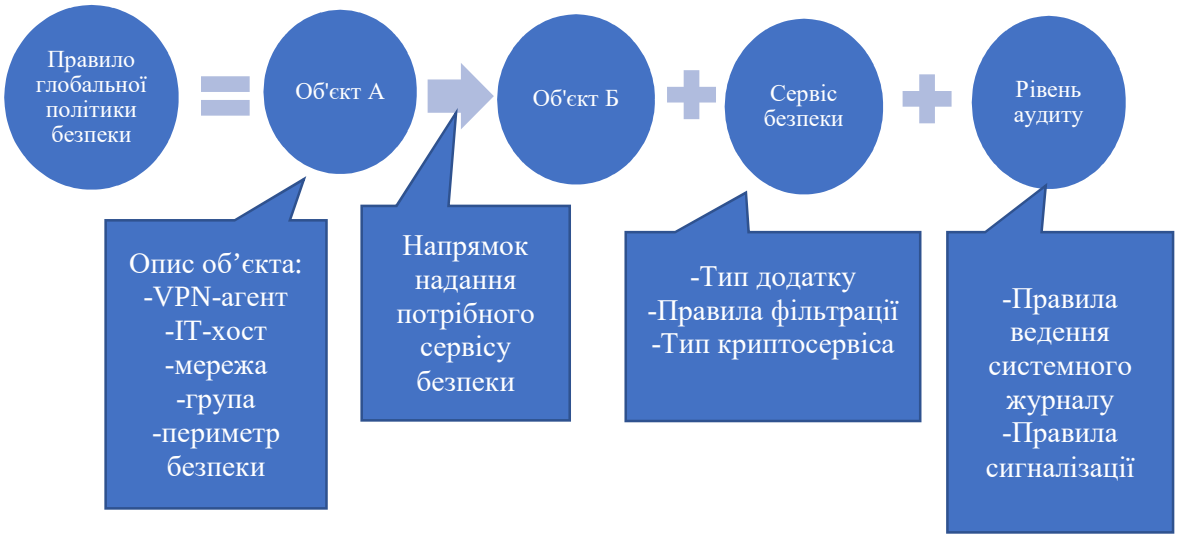

Рис. 1.2. Загальна структура глобальної політики безпеки підприємства

За допомогою глобальної політики безпеки, зазначеної на рисунку 1.2, забезпечуються правила аутентифікації об'єктів, обмін ключами, ведеться запис результатів подій безпеки у спеціальний журнал і відбувається облік ризиків безпеки даних. Об'єктами для глобальної політики безпеки виступають окремі робочі станції та підмережі, що включають у свій склад структурні підрозділи підприємства.

У глобальній політиці безпеки компанії правила за функціями розділяються на такі групи:

– правила VPN, що реалізовані з використанням протоколів IPSec. В

якості агенту виконання цих правил виступає драйвер VPN, встановлений у стеках клієнтських пристроїв або шлюзах безпеки;

- правила пакетної фільтрації, що дозволяють забезпечити фільтрацію пакетів типів stateless і stateful;
- проксі-правила, з включенням антивірусного захисту, які відповідають за фільтрацію трафіку, що передається через прикладні протоколи. У цьому випадку в якості виконавчого агенту виступає проксі-агент;
- правила авторизованого доступу, з використанням правил одноразового входу, що дозволяють забезпечити роботу користувачів за паролями. Ці правила виконуються агентами різних рівнів від VPN-драйвера до проксі-агентів. В якості агентів виконання таких правил захисту інформації виступають системи авторизації;
- правила, що відповідають за протоколювання подій, вразливостей у системі захисту інформації. У компанії політика ведення журналів подій виконується агентом протоколювання, а в якості виконавців виступає повністю вся інформаційна система.

За допомогою локальної політики безпеки підприємства здійснюється налаштування засобів захисту інформації і синхронізуються налаштування для вузлів з подальшим коригуванням. Загалом в локальній політиці безпеки підприємства розміщені правила, за допомогою яких регламентуються з'єднання, змінюються налаштування використовуваних мережевих пристроїв.

При роботі з великим обсягом конфіденційних даних у компанії стоїть першочергове завдання організації захисту інформації, тобто визначення заходів, спрямованих на створення, забезпечення та підтримку інформаційної безпеки. Об'єкт захисту інформації представляє собою інформацію або інформаційний процес, який потребує забезпечення захисту від несанкціонованого доступу, порушення цілісності та структурованості даних.

Мета захисту інформації - це отримання результатів від уникнення

збитків, спричинених витоком або несанкціонованим впливом на інформацію.[4] Ефективність захисту інформації дозволяє визначити рівень відповідності результатів використаної системи захисту даних поставленим цілям.

Виділяють наступні основні види захисту інформації:

1. Захист інформації від витіку – це заходи, спрямовані на збереження та цілісність конфіденційних даних, використовуваних у внутрішньому та зовнішньому документообігу підприємства.

2. Захист даних від розголошень – це заходи, спрямовані на запобігання необережних або умисних дій співробітників або інших осіб, які розкрили конфіденційну інформацію, що може призвести до подальшої передачі даних.

3. Захист даних від несанкціонованого доступу – це заходи, спрямовані на запобігання доступу до комп'ютерної мережі шляхом застосування комплексу інженерно-технічних, програмних та організаційних засобів.[5]

Крім того, необхідно розробити систему захисту даних, яка включає в себе технічні, програмні, криптографічні та організаційні засоби, що забезпечують безпеку мережі у будь-який момент часу від випадкового чи умисного впливу, а також несанкціонованого використання.

Безпека даних – це стан захищеності даних, при якому забезпечена цілісність, конфіденційність та доступність.

Проблеми захисту інформації на сьогодні пов'язані з дестабілізуючим впливом зовнішніх та внутрішніх загроз, що виникають у компанії та впливають на її функціонування. В свою чергу, поняття проблеми безпеки даних пов'язано з поняттям загрози безпеки. Це призвело до того, що в діяльності підприємств все більше виникає проблем, які мають негативний вплив на систему управління, а також технологічну підтримку у питаннях зберігання та обробки даних.[6]

Проблеми інформаційної безпеки розділяють на три основних види[7]:

1. Перехоплення даних, пов'язане з порушенням конфіденційності інформації.

2. Модифікація або зміна даних, пов'язана з зміною початкового повідомлення або його повною підміною з подальшим пересиланням адресату.
3. Порушення авторства інформації, тобто передача інформації не від імені автора, а від імені зловмисника.

Для здійснення перехоплення конфіденційної інформації зловмисниками використовуються віруси, троянські програми, шкідливе та шпигунське програмне забезпечення. Проблеми захисту мережі пов'язані з тим, що не кожна антивірусна програма може вчасно виявити виниклі загрози в мережі, що створює можливість для зловмисника використовувати мережу для досягнення поставлених цілей. Однак можливість перехоплення інформації не завжди створює можливості отримання доступу до захищених даних з подальшою модифікацією. Як приклад перехопленням інформації може виступати аналіз мережевого трафіку в мережі. У цьому випадку зловмисник отримує інформацію про мережу підприємства, але можливості спотворення цієї інформації не має.

Проблеми безпеки даних також пов'язані з розвитком глобальної мережі інтернет, яка користується популярністю серед різних категорій користувачів. Зміцнення глобалізації, а разом з тим і інформатизації створює можливості для зловмисника з будь-якої точки світу створювати загрози безпеки для комп’ютерної мережі.

До основних завдань інформаційної безпеки даних відносяться[8]: забезпечення конфіденційності, цілісності та структурованості інформації; організація своєчасного виявлення та запобігання зовнішнім та внутрішнім загрозам; впровадження організаційних, інженерно-технічних, апаратно-програмних методів, що дозволяють зміцнити захист даних; розробка та вдосконалення політики безпеки з урахуванням сучасних тенденцій розвитку апаратного та програмного забезпечення.

Для підприємств завдання забезпечення захисту даних є одними з найважливіших, оскільки вони завжди перебувають під постійним наглядом

зловмисників. Тому інформаційна безпека спрямована на забезпечення достатнього та необхідного рівня захисту інформації, що в значній мірі визначається платіжними, інформаційними та іншими процесами. Виникнення помилок в роботі інформаційної структури підприємства може завдати значний збиток у сфері отримання інформації для забезпечення стабільності основних бізнес-процесів.

Тому інформаційна безпека постійно контролюється, приймаються заходи для управління ризиками, розробляються документи, які є основою стандартизації управління захистом інформації. Особливе значення при забезпеченні інформаційної безпеки приділяється формальним методам захисту інформації, на основі яких здійснюється стандартизація.[9] Головною метою стандартизації є підвищення довіри, виконання необхідних заходів щодо захисту інформації від виникаючих загроз та впровадження методів зменшення ризиків.

Для забезпечення захисту даних підприємство повинно виконувати наступні завдання[10]:

- забезпечувати високий рівень організації та функціонування підрозділів у сфері інформаційної безпеки підприємства;

- здійснювати корекцію у сфері функціонування системи захисту даних;

- розробляти плани управління ризиками порушення інформаційної безпеки та забезпечувати високий рівень організації впровадження цих планів у основні бізнес-процеси підприємства;

- проводити корекцію внутрішнього документообігу у сфері захисту даних;

- приймати управлінські рішення у сфері вдосконалення системи захисту даних, а також розробляти та організовувати програми навчання співробітників, заходи підвищення обізнаності співробітників підприємства у сфері захисту даних;

- здійснювати постійний моніторинг виявлення загроз та вдосконалювати заходи їх ліквідації;

- впроваджувати сучасні методи захисту даних, проводити внутрішній та зовнішній аудит інформаційної безпеки;

- приймати рішення у сфері вдосконалення політики безпеки підприємства, коригувати концепцію та стратегію у сфері інформаційної безпеки.

1.2 Інформаційні активи підприємства як об‘єкти захисту при формуванні інформаційної безпеки підприємства

Вивчення сфери діяльності організації дозволило виявити наступні інформаційні активи:

- Інформація (включаючи секретну документацію генеральних планів міських комунікацій, проектну документацію організацій, особисті дані клієнтів та інше);
- Апаратне забезпечення (комп'ютери, сховища даних, оргтехніка);
- Програмне забезпечення, включаючи прикладні програми (зокрема, САП);
- Документи у паперовому вигляді (включаючи договори, скани генпланів, виписки з державних реєстрів та інше);
- Конфіденційність та довіра при наданні послуг.

Рис. 1.3. Інформаційні активи підприємства

Усі активи компанії можна розглянути з погляду цінності та розташувати їх у порядку зростання:

1. прикладне програмне забезпечення (зокрема, САП, CMS, ERP, CRM та інше);
2. системне програмне забезпечення;
3. особисті дані про співробітників;
4. Особисті дані клієнта;
5. проектна документація, плани комунікацій, включаючи стратегічного призначення;
6. проектна документація, отримана від замовника;
7. проєктна документація, розроблена організацією.

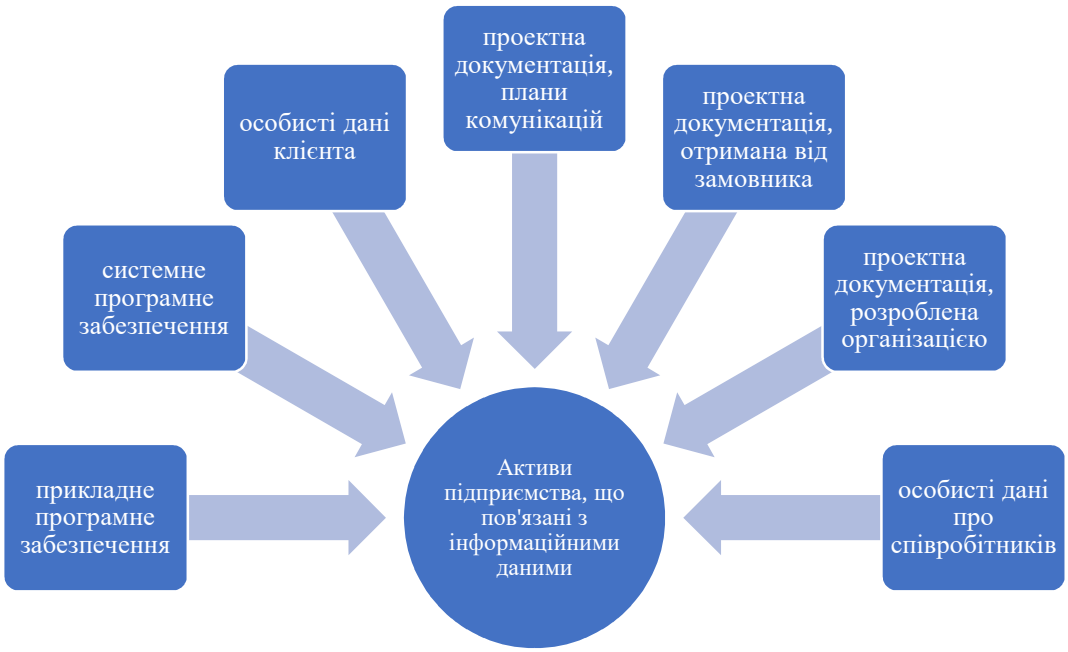

Рис.1.4. Активи підприємства, що пов’язані з інформаційними даними

Отже, в компанії виявлено багато активів, пов'язаних з інформаційними даними. Відповідно до них можуть бути виділені наступні вразливості: дії зловмисників; вихід з ладу апаратного забезпечення (АО); недостача ресурсів АО; конструктивні недоліки програмного забезпечення (ПО); вихід з ладу ПО; недостача ресурсів ПО; викрадення під час передачі по лініям зв'язку (ЛЗ); підміна під час передачі по ЛЗ; відмова у обслуговуванні ЛЗ; помилки

користувача; розголошення конфіденційної інформації; недбале ставлення до інформаційної безпеки; саботаж; виникнення надзвичайних ситуацій; обставини непереборної сили.

Загрози безпеки підприємства можуть мати природний або людський фактор, вони можуть виникати як випадково, так і навмисно. Для підприємства важливо не пропустити жодної загрози інформаційної безпеки, оскільки можливі збитки можуть бути дуже значними, але також не варто звертати увагу на незначні загрози, оскільки може бути задіяно надто багато засобів, і шкода для підприємства може не бути завдана. Після виявлення можливого джерела загрози та сектору, який є цільовим для загрози (об'єкт загрози), потрібно визначити можливість та масштаби реалізації загрози. Для цього необхідно врахувати аналітичні дані, такі як:

- частоту виникнення загрози;

- мету загрози, використовувані ресурси та можливості реалізації цієї або іншої загрози;

- наскільки привабливий ресурс, на який впливає загроза;

- наскільки можливі випадкові загрози, пов'язані з географічним фактором, реалізація яких може бути природною або техногенною катастрофою.

Для проведення аналізу по виникненню загрози необхідно скористатися статистичними даними, якщо такі існують. Статистичні дані дозволять визначити, як часто виникає загроза і на що вона спрямована, які збитки вона може завдати. З цього пункту можна зробити висновок, що в цій компанії є вразливі інформаційні активи, які необхідно захищати. І для більш правильного впровадження політики інформаційної безпеки необхідно визначити основні проблеми та завдання захисту інформації в будівельній компанії.

1.3. Обґрунтування доцільності оновлення політики інформаційної безпеки підприємства

Під час загального аналізу можливих загроз підприємству можна зробити висновок, що поточний стан інформаційної безпеки організації є невтішним і вимагає повної реорганізації. Таким чином, у межах розробки комплексної інформаційної безпеки було прийнято рішення розвивати роботу у трьох напрямках.

1. Розробка адміністративних методів забезпечення інформаційної безпеки.
2. Розробка програмно-апаратних методів забезпечення інформаційної безпеки.
3. Розробка інженерно-технічних методів забезпечення інформаційної безпеки.

Перше напрямок передбачає встановлення трудового розпорядку на підприємстві; введення пропускного режиму; встановлення регламенту перебування сторонніх осіб на території підприємства та регламенту роботи працівників на робочих місцях.

Розробка даного напрямку передбачає організацію стратегії інформаційної безпеки узгоджено з керівником організації. Контроль за виконанням методики буде покладено на працівників відділів та службу охорони.

При розробці другого напрямку особлива увага буде приділятися: централізованому встановленню антивірусного програмного забезпечення; організації міжмережевого екрана; організації засобів розподілу інтернет-трафіку; організації засобів централізованої автентифікації користувача; забороні на використання зовнішніх носіїв; організації обміну інформацією між комп’ютерами; організації розподілу доступу; оновленні програмного забезпечення до актуальних стабільних версій; організації резервного

копіювання даних.

Виконання інструкцій цього напрямку буде покладено на IT-персонал організації.

Розробка інженерно-технічних засобів передбачає впровадження:

- датчиків руху;
- відеокамер спостереження;
- “тривожних кнопок”.

Виконання цих рекомендацій буде покладено на підрядні організації та організації, що займаються приватним охоронним бізнесом. Контроль за виконанням заходів буде здійснювати директор організації та завгосп офісного центру (не є працівником компанії).

У підсумку розробка всіх трьох напрямків сходиться до єдиних вимог:

1. Усунути можливі загрози інформаційної безпеки всередині підприємства.

2. Усунути можливі загрози в віртуальному просторі глобальної мережі.

3. Усунути можливі загрози вільного проходу на підприємство та доступу до інформації.

До поточного моменту на об'єкті не проводилося цілеспрямоване розроблення та впровадження політики інформаційної безпеки. Використання методів захисту інформації було епізодичним і зводилося до встановлення безкоштовних антивірусних програм та фізичного захисту (закривання приміщень на ніч). Дана халатність з боку інформаційно-технічного персоналу призвела до кількох інцидентів, які становили загрозу для діяльності організації. Тому було прийнято рішення про необхідність розроблення комплексної політики інформаційної безпеки.

Нижче буде розглянуто існуючий захист інформаційної безпеки з точки зору: програмного забезпечення; технічного забезпечення.

Результати обстеження об'єкта на предмет наявності інформаційної безпеки внесені в таблицю 1.1.

Таблиця 1.1

Аналіз основних завдань забезпечення інформаційної безпеки

Основні завдання забезпечення інформаційної безпеки	Ступінь виконання
Забезпечення безпеки діяльності, захисту інформації та даних, що є комерційною таємницею. Забезпечення безпеки діяльності, захисту інформації та даних, що є комерційною таємницею	Низька
Організація роботи з правової, організаційної та інженерно-технічної (фізичної, апаратної, програмної та математичної) захисту комерційної таємниці.	Відсутня
Організація спеціального справочно-документального обігу, який виключає несанкціоноване отримання даних, що є комерційною таємницею.	Відсутня
Попередження необґрунтованого доступу та відкритого доступу до інформації та документів, що становлять комерційну таємницю.	Відсутня
Забезпечення режиму безпеки під час здійснення різних видів діяльності, таких як зустрічі, переговори, наради, засідання та інші заходи, пов'язані з діловим співробітництвом на національному та міжнародному рівні.	Не відбувається

Продовження таблиці 1.1

Виявлення та локалізація можливих каналів витоку конфіденційної інформації під час повсякденної виробничої діяльності та в екстремальних ситуаціях (аварії, пожежі та інші).	Не забезпечує
Забезпечення охорони території, будівель і приміщень з інформацією, яка підлягає захисту.	Вахтер без ліцензії та охоронну діяльність

З таблиці 1.1 видно, що положення компанії відносно стандартів захисту інформації дуже низьке, тобто у разі крадіжки даних компанія може понести величезні втрати. Дані, вказані в таблиці, показують, що обрана спрямованість розробки інформаційної безпеки є актуальною й надзвичайно необхідною.

Отже, можна зробити висновок, що компанія потребує розробки нової моделі управління політики інформаційної безпеки, і обрані рішення є актуальними для цього підприємства.

У першому розділі надані визначення основним термінам і поняттям, пов'язаним із політикою захисту інформації, наведено опис підприємства, проведено порівняльний аналіз системи безпеки, можна зробити наступні висновки:

- основною проблемою є необхідність забезпечення потрібного рівня захисту, при цьому необхідно враховувати, що інформація, яка передається по комп'ютерній мережі, може бути отримана зловмисником та передана по каналах зв'язку;
- головною метою стандартизації є підвищення довіри, рівня стабільності роботи мережі, виконання необхідних заходів з захисту інформації від виникаючих загроз та впровадження методів для зниження ризиків;
- також необхідно розробити документи, які стануть основою політики інформаційної безпеки.

РОЗДІЛ 2
ПРОПОЗИЦІЇ ЩОДО УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПОЛІПШЕННЯ ЗАЛЬНОЇ ПОЛІТИКИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

2.1 Техніко-економічна характеристика будівельної компанії

Компанія з обмеженою відповідальністю "Будівельний альянс" пропонує повний комплекс загально будівельних робіт - від створення проектної документації до виконання чистових робіт та комплектації об'єктів матеріалами за оптовими цінами. Діяльність фірми зосереджена на повному забезпеченні процесу будівництва від вибору проекту до здачі реалізованого будівельного об'єкту «під ключ». Поєднання найкоротших термінів виконання замовлень і прийнятних цін, використання сучасних матеріалів та дотримання високої якості робіт роблять фірму з обмеженою відповідальністю "Будівельний альянс" досить конкурентоспроможною у сфері будівництва.

Будівельна фірма з обмеженою відповідальністю "Будівельний альянс" має значний досвід у монтажі та виконанні робіт з облаштування інженерних систем та обладнання, використовує в роботі сучасні передові технології та обладнання. Робочі бригади, що займаються монтажем, мають високу кваліфікацію та значний досвід, що дозволяє виконувати замовлення в найкоротших термінах без зайвих затримок, а також прокладати інженерні системи в місцях, до яких досить складно забезпечити нормальний доступ. Досвідчені співробітники фірми надають якісні консультації з монтажу, заміни або модернізації інженерних мереж, а також розповідають про нові тенденції у розвитку інженерних систем, про найбільш оптимальні, якісні та економічні рішення завдань, які необхідно реалізувати.

У таблиці 1.2 наведено загальні технічні характеристики підприємства.

Таблиця 1.2

Характеристика підприємства

№	Назва характеристики	Значення показника	Одиниця виміру
1	Річний обіг	142,26млн.	грн.
2	Вартість підприємства	20,500млн.	грн.
3	Річний фонд заробітної плати	22,644млн	грн.
4	Кількість співробітників	306	люд.
5	Кількість партнерів підприємства	>24	шт.
6	Рентабельність підприємства	>15,3%	

Джерело: [11]

До основних напрямків діяльності ТОВ «Будівельний альянс» відносяться:

- будівництво будівель та споруд;
- підготовка будівельної ділянки;
- монтаж інженерного обладнання, будівель та споруд;
- облаштування підлогових покриттів та оздоблення стін;
- виробництво інших будівельних робіт.

Місією ТОВ «Будівельний альянс» є розвиток діяльності компанії за рахунок високої якості виконання будівельних робіт, оптимальної цінової політики та новітніх технологій.

Для підтримки свого іміджу компанією виконуються наступні завдання: встановлюються єдині критерії підтримки іміджу серед працівників компанії, бізнес-середовища, органів державної влади та громадських організацій; формується та підтримується середовище взаємного поваги, відкритості і довіри з гарантією захисту їх прав; зміцнюється імідж компанії за рахунок репутації ефективного, соціально відповідального та надійного партнера.

Для підтримки іміджу серед працівників, пріоритетами компанії є життя і здоров'я, підтримка соціального забезпечення та постійне підвищення професіоналізму співробітників.

Структура управління підприємством побудована за ієрархічним принципом і зображена на рисунку 2.1.

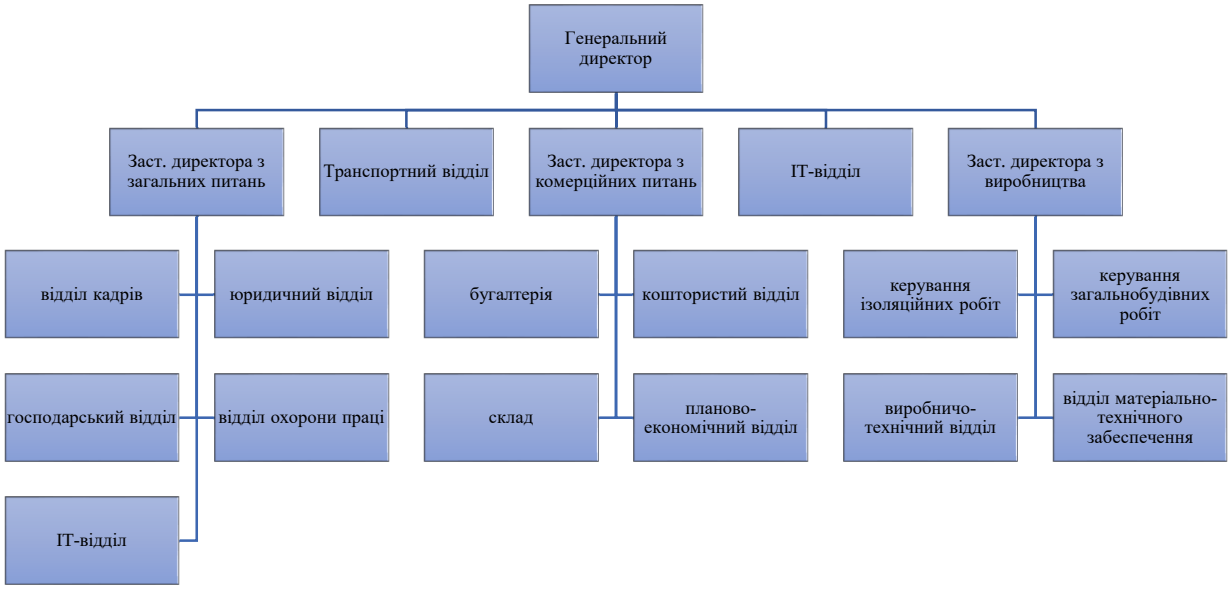

Рис. 2.1. Організаційна структура компанії «Будівельний альянс»

Будівельна фірма ТОВ «Будівельний альянс», що складається з численних структурних підрозділів, надає всім відділам однаковий доступ до всіх даних, що знаходяться в базі даних (БД), що призводить до неправильної роботи самої БД, а також можливості надання закритої інформації особам, яким не повинен бути доступ, тобто до неправильної організації політики інформаційної безпеки. Відповідно можна зробити висновок, що дана схема організації доступу до даних має велику кількість потенційних загроз інформаційної безпеки, і для покращення захисту даних необхідно розмежувати доступ до цієї системи.

На рис. 2.2 наведено схему обробки заявки від клієнта.

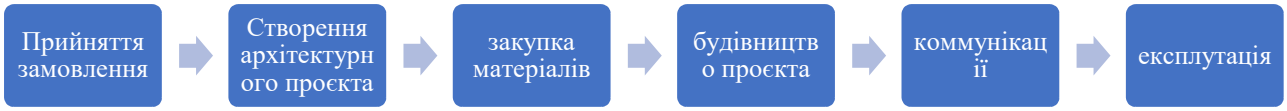

Рис. 2.2. Структурна схема обробки заявки клієнта

З рисунку 2.2 ми можемо бачити, що інформація від прийняття замовлення від клієнта до здачі в експлуатацію відбувається загальним потоком

і для всіх однакова. Це підтверджує фактор загрози інформаційної безпеки.

2.2 Загальні правила оновлення політики інформаційної безпеки підприємства

При побудові системи інформаційної безпеки підприємства використовуються міжнародні стандарти інформаційної безпеки ISO/IEC 27002:2015 “ Інформаційні технології .Технології безпеки. Практичні правила менеджменту інформаційної безпеки.”. Ці стандарти містять рекомендації загального характеру щодо забезпечення інформаційної безпеки, які забезпечують основний рівень безпеки інформаційних систем. У стандарті ДСТУ ISO/IEC 27002:2015 “Інформаційні технології .Технології безпеки. Практичні правила менеджменту інформаційної безпеки.” описані норми, які необхідно вивчити та врахувати при розробці політики інформаційної безпеки та проектуванні конкретних заходів забезпечення захисту даних.

- Стандарт ISO ISO/IEC 27002:2015 складається з розділів, які регламентують багато напрямків забезпечення безпеки інформаційних систем:
- політика інформаційної безпеки регламентує важливість підтримки керівництвом компанії затвердженої системи організації інформаційної безпеки;
- рекомендації з політики інформаційної безпеки підприємства описуються в розділі організаційні питання;
- заходи забезпечення інформаційної безпеки описані в розділі класифікація інформаційних ресурсів;
- вплив людського фактору та норми, розроблені для зменшення ризику безпеки, описані в розділі управління персоналом;
- реалізація фізичної безпеки регламентує дії забезпечення безпеки компонентів інформаційної системи;
- дії при роботі з серверами, робочими станціями тощо описані в

розділі адміністрування інформаційних систем;

- необхідність розмежування прав при роботі з інформацією регламентує управління доступом;
- основні рушії інформаційної безпеки систем описує розділ розробки та супроводу інформаційних систем;
- постійна робота підприємства без перерв описує термін забезпечення неперервності бізнесу;
- загальні вимоги до політики інформаційної безпеки описує термін забезпечення відповідності вимогам. [12]

Політика інформаційної безпеки повинна бути доведена до відома всіх користувачів організації у формі, яка є актуальною, доступною та зрозумілою для читачів, яким вона призначена. Політика інформаційної безпеки повинна бути частиною більш загальної документованої політики. Якщо політика інформаційної безпеки поширюється за межі організації, мають бути прийняті заходи для запобігання розголошенню конфіденційної інформації.

Ступінь інформаційної безпеки підприємства визначається відповідно до правил дотримання політики інформаційної безпеки. Для компанії політика інформаційної безпеки представлена наступними нормативними документами в галузі технічного захисту інформації:

1. Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».[13]
2. Указ Президента України від 27.09.1999 № 1229 «Про Положення про технічний захист інформації в Україні».[14]
3. Наказ Адміністрації Держспецзв’язку від 22.03.2007 № 36 «Про затвердження Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації», зареєстрований в Міністерстві юстиції України 04.04.2007 за № 312/13579.[15]
4. Постанова Кабінету Міністрів України від 08.10.1997 № 1126 «Про

затвердження Концепції технічного захисту інформації в Україні».[16]

5. Закон України «Про платіжні послуги»; [17]

6. Закон України «Про захист персональних даних»; [18]

Ці нормативні документи повністю регламентують правила використання комп'ютерної техніки та інформаційних ресурсів з точки зору політики інформаційної безпеки підприємства. [19]

2.3 Пропозиції щодо удосконалення політики інформаційної безпеки підприємства та управління нею

Електронні та електронно-механічні пристрої, що входять до складу технічних засобів охорони, є апаратними засобами забезпечення інформаційної безпеки. Апаратні засоби, які працюють разом із програмними або самостійно, виконують завдання, необхідні для побудови інформаційної безпеки. Електронні та електронно-механічні пристрої є апаратними засобами забезпечення інформаційної безпеки, а не інженерно-технічними засобами, якщо вони обов'язково входять до складу технічних засобів політики інформаційної безпеки.

До апаратних засобів політики інформаційної безпеки відносяться:

- пристрої введення біометричних даних визначення;
- пристрої ідентифікації співробітника;
- пристрої шифрування інформації;
- електронні замки та блокатори, що не дозволяють безконтрольно вмикають робочі станції.
- До допоміжних засобів захисту інформації відносяться:
- засоби знищення магнітних носіїв та інформації на них;
- засоби сигналізації, що попереджують про несанкціоновані дії користувачів.

До програмних засобів захисту інформації відносяться програми, що

входять до складу програмного забезпечення, необхідного для захисту даних. До цих засобів захисту інформації можна віднести:

- програми визначення користувачів;
- програми визначення зони доступу до ресурсу;
- програми криптографічного захисту інформації;
- програмне забезпечення: баз даних, комп'ютерних засобів;
- програми, що захищають інформацію від незаконного доступу та копіювання.

Ідентифікація користувачів у політиці інформаційної безпеки розуміється як 100% визначення індивідуального та унікального імені користувача, а аутентифікація служить для того, щоб визначити 100% належність користувачу представленого ним імені.

Як приклад програм, які допомагають у захисті інформації, можуть виступати:

- програми видалення залишеної інформації (у тимчасових файлах, оперативній пам'яті тощо);
- аудиторські програми подій, які описують виникненні загрози, журнали реєстрації подій, які можуть бути доказом виниклих загроз;
- програми, що створюють можливі події, при яких здійснюється імітація роботи з порушником;
- програми тестування захищеності.

Для захисту локальної обчислювальної мережі необхідно розділити користувачів на групи з відповідними правами:

1. Адміністратор (Administrator) - адміністратори мережі (створення та управління політикою інформаційної безпеки, глобальні налаштування мережі і т. д.).
2. Менеджер (Manager) - обліковий запис для щоденного обслуговування інформаційно-обчислювальної техніки.
3. Користувач (User) - обліковий запис звичайного користувача (співробітника компанії) з обмеженими правами.

4. Безпека (Security) - обмежений обліковий запис (у випадку необхідності доступу не співробітників організації).

Для ідентифікації користувача потрібна Active Directory на базі мережевої операційної системи, де для кожного користувача повинен бути створений унікальний запис, а кожний запис повинен бути включений в відповідну групу. Таким чином, здійснюється розподіл доступу.

Таблиця 2.1

Групи користувачів та їх права

Дії	Безпека	Користувач	Менеджер	Адміністратор
Створення та зміна груп користувачів	ні	ні	ні	так
Зміна налаштувань мереж	ні	ні	ні	так
Підключення нових робочих станцій до мережі	ні	ні	ні	так
Зміна налаштувань серверів	ні	ні	ні	так
Зміна прав доступу до каталогів та резервних копій	ні	ні	ні	так
Встановлення програм	ні	ні	так	так
Доступ до Інтернету	ні		так	так
Обсяг трафіку (на місяць)	0	100	1000	1000
Можливість завантажувати файли	ні	ні	так	так
Запис	Тільки в "Мої документи"	"Мої документи", "Робочий стіл", "Для всіх", "Мережева"	Будь-яка папка на локальному комп'ютері	Будь-яка папка на будь-якому комп'ютері в мережі
Підключення зовнішніх флеш-дисків, зовнішніх дисків	ні	ні	так	так
Підключення CD/DVD-ROM	ні	ні	так	так
Використання ICQ	ні	так	так	так
Доступ до FTP	ні	ні	ні	так
Доступ до POP3	ні	так	так	так
Доступ до SMTP	не	так	так	так
Доступ до SSL	ні	так	так	так
Доступ до SOCKS	ні	ні	ні	так

Для зменшення вразливості програмного забезпечення було вирішено

оцінити рівень готовності операційних систем. Для цього були прийняті наступні заходи:

1. Проведена заміна застарілих операційних систем на нові операційні системи.
2. Там, де заміна операційних систем не є доцільною, проведено оновлення існуючих операційних систем шляхом встановлення сервіс-паків останніх версій.

Для підвищення якості антивірусного захисту було прийнято рішення впровадити більш сучасний антивірус. Контроль інтернет-трафіку буде здійснюватися за допомогою проксі-сервера, який одночасно буде виступати як брандмауер.

Можна зробити висновок, що окремо програмний комплекс та апаратний комплекс мало ефективні. Тому необхідно використовувати обидва цих засоби захисту інформації разом, тим самим отримавши програмно-апаратний комплекс. Отже, вважаю за необхідне розглянути структуру програмно-апаратного комплексу, який використовується для забезпечення інформаційної безпеки даних в організації.

Програмно-апаратний комплекс - це набір технічних та програмних засобів, які співпрацюють для виконання одного або декількох схожих завдань.[20]

Програмний комплекс на даному підприємстві включає наступні складові: операційна система Windows XP, антивірус Dr. Web Enternet Security. У програмному комплексі захист пароля організований стандартним розділенням доступу користувачів Windows, передача даних здійснюється в Інтернеті без використання захищеного з'єднання за технологією VPN. Для розширеного функціонування комплексу на сервері необхідно провести: налаштування мережевого екрана, встановлення проксі-сервера, встановлення поштового сервера.

Апаратний комплекс на підприємстві представлений:

- персональні електронні обчислювальні машини Office Cor 2 duo E7500, a

також Celeron 430;

- Hub Dlink DES - 1005D/E;
- принтери HP DeskJet 2050;
- сканери Genius G Pen.

Програмний та апаратний комплекс є одним робочим комплексом, який надалі називається програмно-апаратним комплексом. Для зрозуміння сутності програмно-апаратного комплексу, запропонованого для будівельної організації, розглянемо його структуру, представлену на рисунку 2.3.

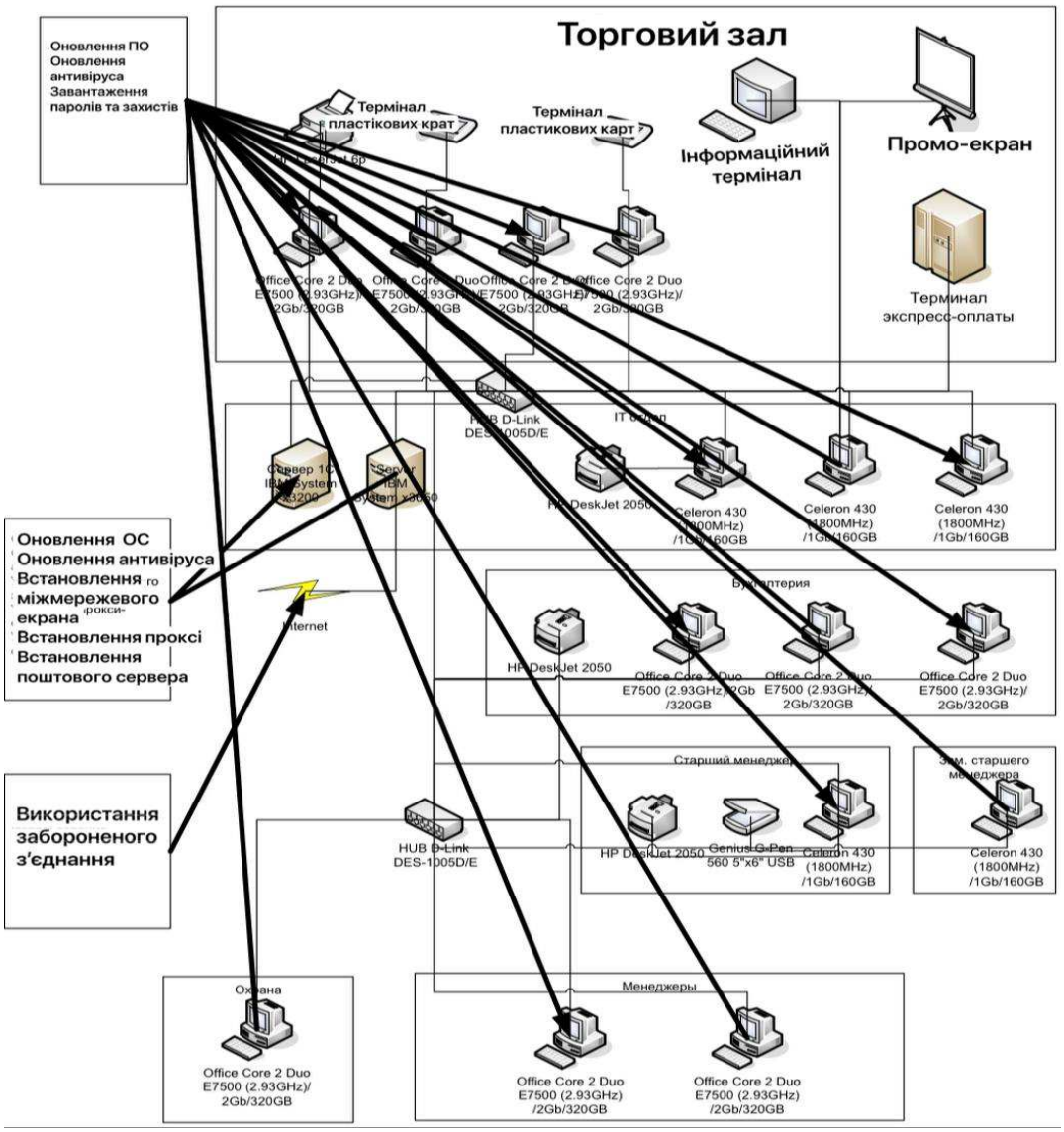

Рисунок 2.3 Структура програмно-апаратного комплексу

На основі наданої схеми видно, що для підвищення інформаційної

безпеки були проведені заходи з посилення безпеки мережі підприємства, які представлені в таблиці 2.2.

Таблиця 2.2

Проведені заходи з посилення безпеки мережі підприємства

Об’єкт	Заходи
Сервер	Оновлення ос Оновлення антивірусу Встановлення міжмережевого екрану Встановлення проксі-серверу Встановлення поштового сервера
Робочі станції	Оновлення ОС Оновлення антивірусу Встановлення паролів
З’єднання	Використання захищеного інтернет з’єднання

Комплексна політика захисту інформації включає інженерно-технічне забезпечення комп'ютерної безпеки, яке розглядається як елемент запобігання комп'ютерним злочинам. Інженерно-технічний захист розглядається як комплекс заходів, важелів, технічних засобів і заходів забезпечення інформаційної безпеки.

Для протистояння технічним засобам розвідки на підприємствах використовують криптографічні, апаратні, апаратно-програмні, фізичні та програмні засоби захисту інформації.

Під фізичними методами захисту інформації розуміється охорона приміщень і будівель компанії, приміщень з робочими станціями, а також засобів комп'ютерної техніки та носіїв інформації.

Під апаратними методами захисту інформації розуміється обладнання у вигляді окремих технічних засобів, комп'ютерної техніки, які використовуються для захисту цих систем.

Отже, змінюється структура інженерно-технічного комплексу інформаційної безпеки та захисту інформації підприємства, зображена на рисунку 2.4.

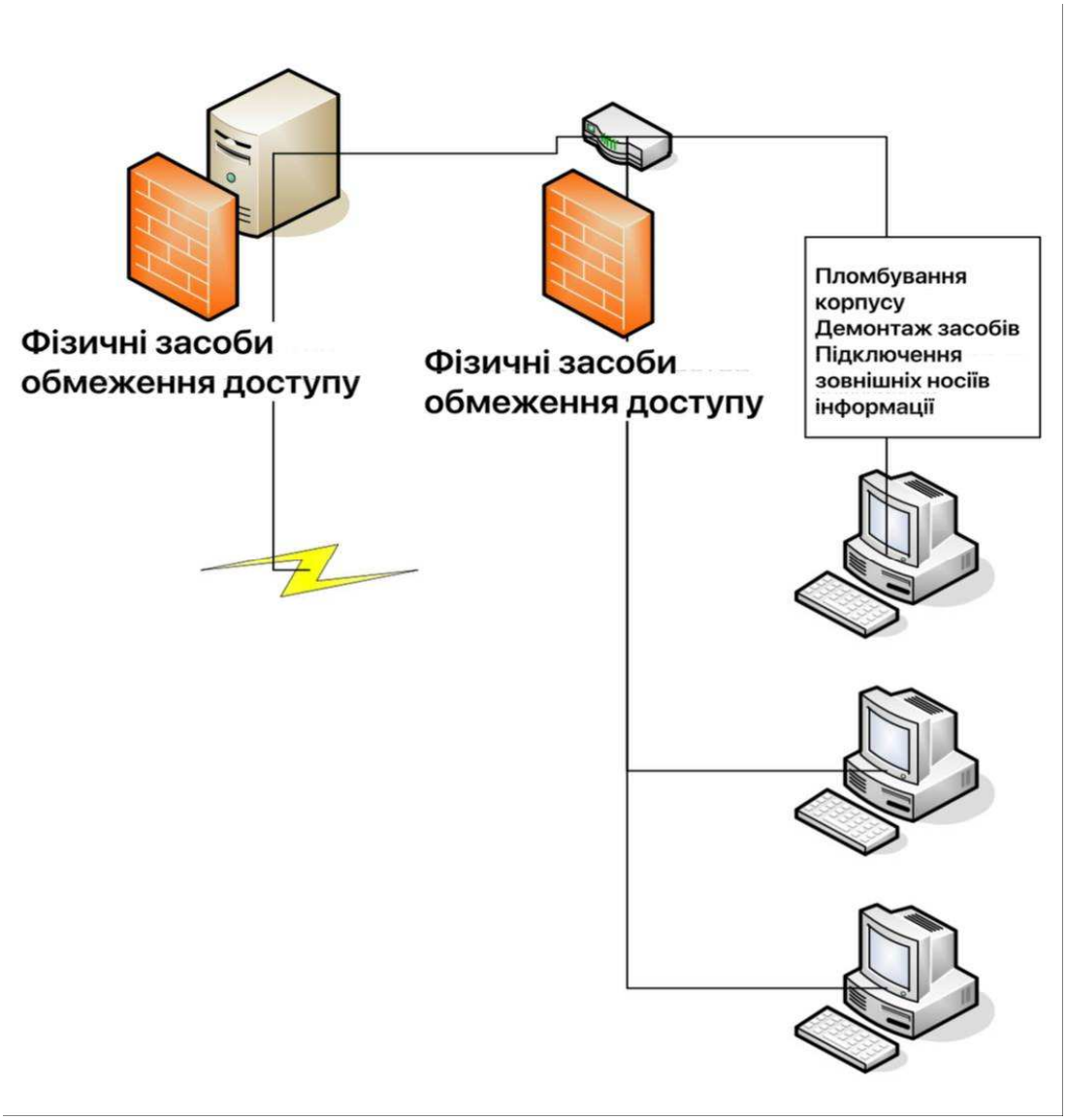

Рис. 2.4. Структура інженерно-технічного комплексу

Використовуючи інженерно-технічний комплекс на підприємстві, ми обмежуємо доступ до мережі та проводимо розмежування доступу до бази даних. Щоб уникнути копіювання даних на зовнішні носії інформації на всіх персональних робочих станціях, необхідно здійснити опломбування корпусу та демонтаж засобів підключення зовнішніх носіїв. Для цього, з метою забезпечення інформаційної безпеки комп'ютерної мережі були проведені наступні заходи (див. табл. 2.3).

Таблиця 2.3

Проведенні заходи забезпечення інформаційної безпеки

Об’єкт	Заходи
Сервер	Фізичні засоби обмеження доступу
Вузли мережи	Фізичні засоби обмеження доступу
Робочі станції	Пломбування корпусу з застосуванням спеціальних пристроїв Демонтаж засобів підключення зовнішніх носіїв інформації

Обов’язковими завданнями при представленні комплексу інженерно-технічних засобів є наступне [21]:

1. Запобігання проникненню зловмисника до джерел інформації з метою її знищення, крадіжки або зміни.

2. Захист носіїв інформації від знищення внаслідок впливу стихійних сил, перш за все, від пожежі та води (піни) під час її гасіння.

3. Запобігання витоку інформації через різноманітні технічні канали.

Для забезпечення ефективного інженерно-технічного захисту інформації необхідно визначити:

1. Що захищати технічними засобами в даній організації, будівлі, приміщенні.

2. Яким загрозам піддається захищена інформація з боку зловмисників і їх технічних засобів.

3. Які способи та засоби доцільно застосовувати для забезпечення інформаційної безпеки з урахуванням як величини загрози, так і витрат на її запобігання.

4. Як організувати та реалізувати технічний захист інформації в організації [21].

Для організації були виділені наступні об'єкти інженерно-технічного захисту, які були розділені за класами захисту:

1. Об'єкти першого (найвищого класу) захисту. До цих об'єктів захисту були віднесені всі носії інформації, знищення або крадіжка яких призведе до

припинення діяльності фірми, понесення великих фінансових збитків, виникнення конфліктів з законом та ін.

2. Об'єкти другого класу захисту. До цих об'єктів були віднесені об'єкти, знищення або крадіжка яких призведе до ускладнень у роботі компанії, спричинить тимчасові зупинки.

3. Об'єкти третього класу захисту. До цих об'єктів були віднесені об'єкти, знищення або крадіжка яких мало вплине або не відобразиться на діяльності фірми.

Таблиця 2.4

Дані про важливість захищених об'єктів

№	Клас	Назва об’єкту
1	1	Комп’ютер керівника
2	1	Комп’ютер секретаря
3	1	Комп’ютер гол. бухгалтера
4	1	Документи керівника
5	1	Документи бухгалтерії
6	1	Документи секретаря
7	1	Сервер
8	2	Документи виробничого відділу
9	2	Документи бухгалтерії
10	2	Інші документи
11	3	Комп’ютери програмісту, системного адміністратора
12	3	Комп’ютери бухгалтерії
13	3	Комп’ютери виробничого відділу
14	3	Комп’ютери відділу кадрів
15	3	Інші носії інформації

Для забезпечення інформаційної безпеки було вирішено використовувати такі інженерно-технічні методи:

1) встановлення відеокамер спостереження;

2) встановлення детекторів руху;

3) встановлення систем оповіщення про пожежу;

4) встановлення систем автоматичного загасання пожежі;

5) встановлення засобів пасивного захисту від вогню.

Ці засоби дозволяють зменшити ризик втрати як інформації, так і цінного майна внаслідок спроби умисного викрадення інформаційних носіїв або матеріальних цінностей, а також у разі виникнення пожежі. Вирішено відмовитися від використання засобів захисту від прослуховування та інших засобів шпигунства, оскільки їх придбання, встановлення та обслуговування є дорогими для підприємства.

Для забезпечення інформаційної безпеки було визначено три класи об'єктів, які потребують захисту, як обов'язковий список заходів та перелік дій для вирішення проблем безпеки у системі підприємства. Однак було прийнято рішення відмовитися від засобів захисту від прослуховування та інших засобів шпигунства.

Таблиця 2.5

Реалізація розроблених заходів інформаційної безпеки з використанням конкретних засобів

Об’єкт	Заходи	Зміст проведення
Сервер	Оновлення ОС	Встановлення оновлень операційних систем для усування вразливостей захисту, налаштування автоматичних оновлень
Сервер	Оновлення антивірусу	Встановлення сучасної ліцензійної версії NOD-32
Сервер	Встановлення міжмережевого екрану	Встановлення міжмережевого екрану Microsoft ISA Server
Сервер	Встановлення проксі-серверу	Встановлення проксі-серверу Microsoft ISA Server
Сервер	Встановлення поштового серверу	Встановлення поштового серверу Microsoft Exchange
Робоча станція	Оновлення ОС	Для машин з Windows XP та Windows 2000 заміна ОС на Windows8 , налаштування автоматичних оновлень

Продовження таблиці 2.5

Робоча станція	Оновлення антивірусу	Встановлення сучасної ліцензійної версії NOD-32
Робоча станція	Використання паролів	Налаштування груп користувачів в з подальшою генерацією індивідуальних паролів
З’єднання	Використання захищеного інтернет з’єднання для обміну інформацією з головним офісом	Для безпечного обміну даними з головним офісом використовується VPN з'єднання з локальною мережою офіса

Отже, застосування розроблених заходів безпеки дозволить організувати політику інформаційної безпеки, а також скоригувати структуру реалізованого апаратно-програмного комплексу.

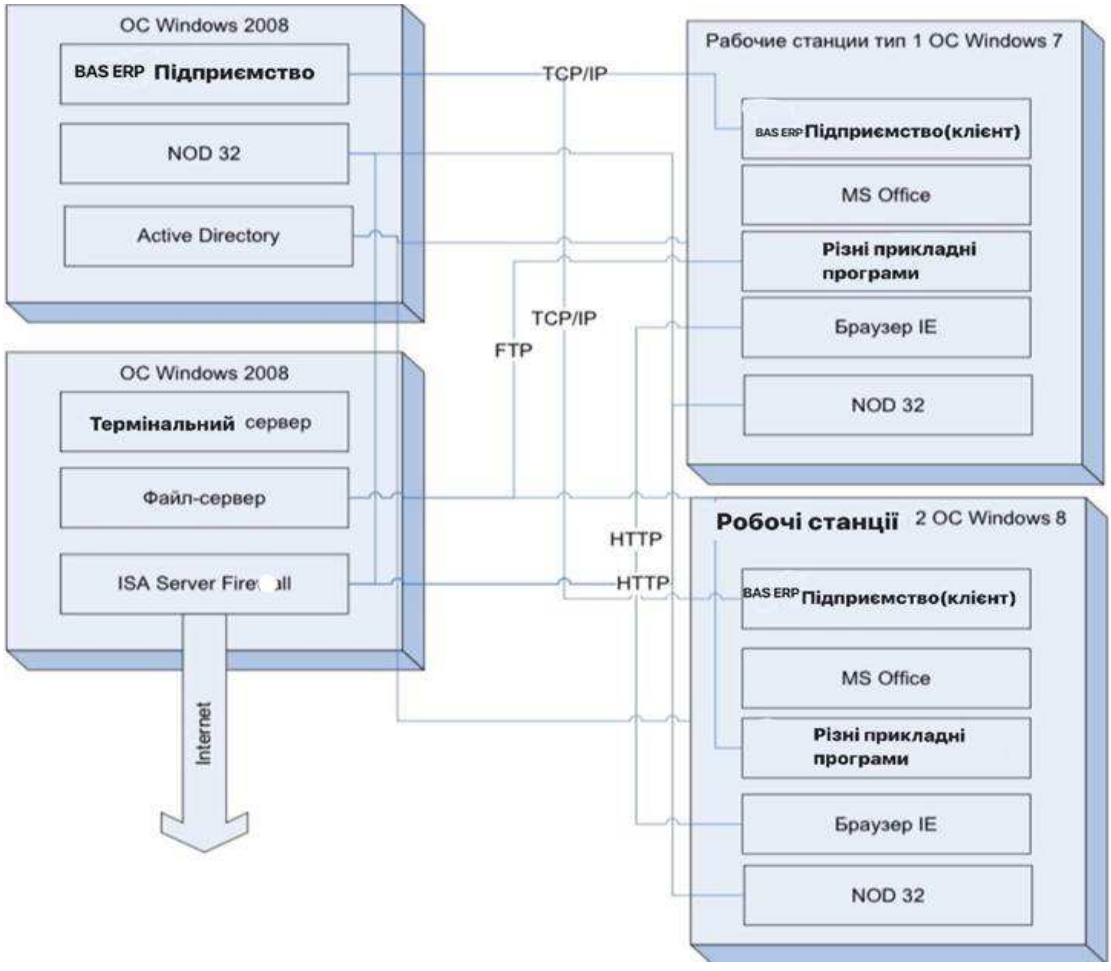

Рис 2.5. Структура програмного складу комплексу

У склад оновленого програмного комплексу включено:

1) сервер BAS ERP: працює на операційній системі Windows Server 2008, на ньому розташована база програми BAS ERP Підприємство 8.1; антивірус, встановлений на цьому сервері NOD 32. Через службу каталогів Active Directory здійснюється розподіл доступу;

2) сервер IBM - працює на операційній системі Windows Server 2008, на ньому розташований файл-сервер, а також Firewall. Доступ в Інтернет здійснюється через Firewall, на файл-сервер збігається інформація від прикладних програм з робочих станцій;

3) робочі станції першого типу працюють на операційній системі Windows 7, на них встановлено: програма BAS ERP Підприємство (клієнт), Microsoft Office 2013, а також браузер Internet Explorer 11, антивірус NOD 32;

4) робочі станції другого типу працюють на операційній системі Windows 8, на них встановлено: програма BAS ERP Підприємство (клієнт), Microsoft Office 2013, а також браузер Internet Explorer 11, антивірус NOD 32.

Реалізація розроблених заходів і створення захищеного Інтернету, а також обмеження доступу до сервера вузлам мережі та робочим станціям потребує проведення заходів щодо реалізації розроблених заходів обмеження доступу. Опис реалізації розроблених заходів щодо обмеження доступу та засобів контролю доступу до ресурсу наведено в таблиці 2.6.

Таблиця 2.6

Реалізація розроблених заходів щодо обмеження доступу та засобів контролю доступу до ресурсу

Об’єкт	Заходи	Зміст проведення
Сервер	Обмеження фізичного доступу	Обладнання приміщення для розташування серверів. Обладнання приміщення системами сигналізації.
Вузли мережі	Обмеження фізичного доступу	Розташування мережевих кабелів в спеціальних каналах для виключення можливості вільного доступу. Розташування важливого мережевого обладнання на території серверної або в спеціальних замкнених контейнерах.

Продовження таблиці 2.6

Робочі станції	Опломбування корпусів та використання спеціальних захисних пристроїв	Опломбування корпусів всієї комп'ютерної техніки з метою своєчасного виявлення спроб несанкціонованого доступу або вилучення пристроїв. Використання замикаючих пристроїв у корпусах, де це передбачено конструкцією.

Реалізація інженерно-технічного захисту інформації передбачає такі завдання:

- встановлення камер відеонагляду;
- встановлення детекторів руху;
- встановлення систем оповіщення про пожежу;
- встановлення систем автоматичного пожежогасіння;
- встановлення засобів пасивного захисту від вогню.

Встановлення камер відеонагляду в офісі продемонстровано наступним планом (див. рис. 2.6).

У даному випадку в офісі компанії були встановлені 4 відеокамери Vision Hi-Tech VB32BS-HVF49 в місцях потенційного входу відвідувачів:

- камера № 1 встановлена на протилежній стіні коридору, в поле її огляду потрапляють всі люди, які входять або виходять з ліфта;
- камера № 2 встановлена так, щоб в її поле огляду потрапляли люди, які входять в приміщення офісу по сходах;
- камера № 3 встановлена так, щоб в поле її огляду потрапляли всі люди, які входять в приймальню і кабінет директора;
- камера № 4 фіксує всіх людей, які намагаються потрапити в приміщення через балкон.

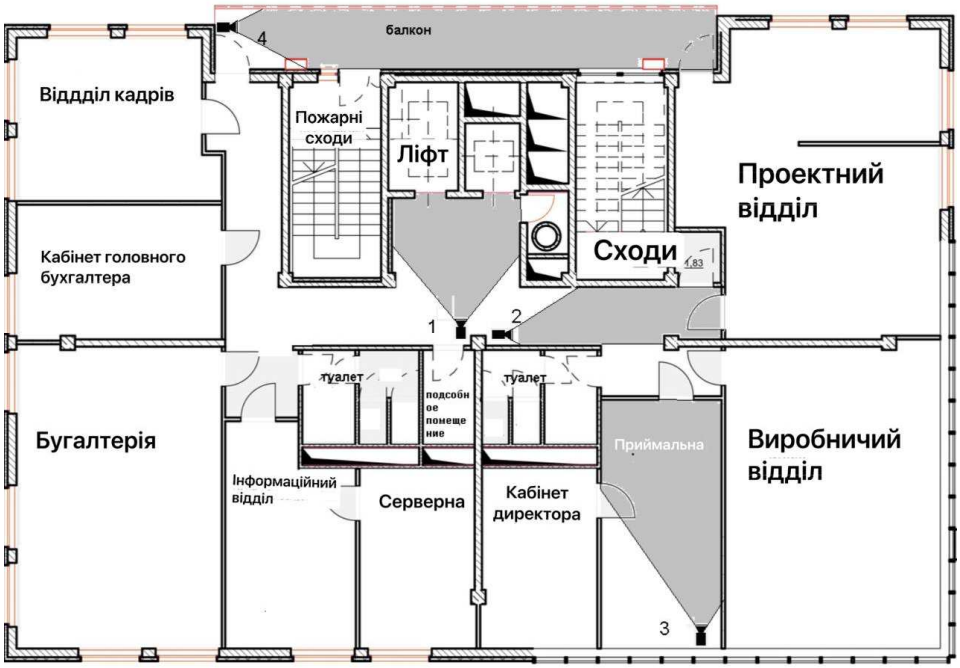

Рис. 2.6. План установки відеокамер

Отже, камери фіксують обличчя кожної людини, яка входить в офіс. Відеодані з камер виводяться на монітор охорони і записуються на спеціальний носій інформації з періодичністю перезапису 14 днів.

Для захисту офісу в нічний час від проникнення зловмисників через двері та вікна в офісі було встановлено 11 детекторів руху в наступних місцях:

- відділ кадрів;
- кабінет головного бухгалтера;
- бухгалтерія;
- інформаційний відділ;
- серверна;
- кабінет директора;
- приймальна;
- виробничий відділ;
- проектний відділ;
- коридор.

Були обрані детектори IS215T (Ademco) з наступними технічними

характеристиками:

- зона виявлення 12 х 12 м з контролем "під собою";
- діаграма напрямленості типу "широкий кут";
- два рівні чутливості;
- висока стійкість до впливу білого світла понад 6000 люкс;
- діапазон робочих температур -10°С– +55°С;
- розміри 87 х 62 х 40 мм.

Схема розташування детекторів зазначена на плані (див. рис. 2.7), де кольорами показані зони покриття.

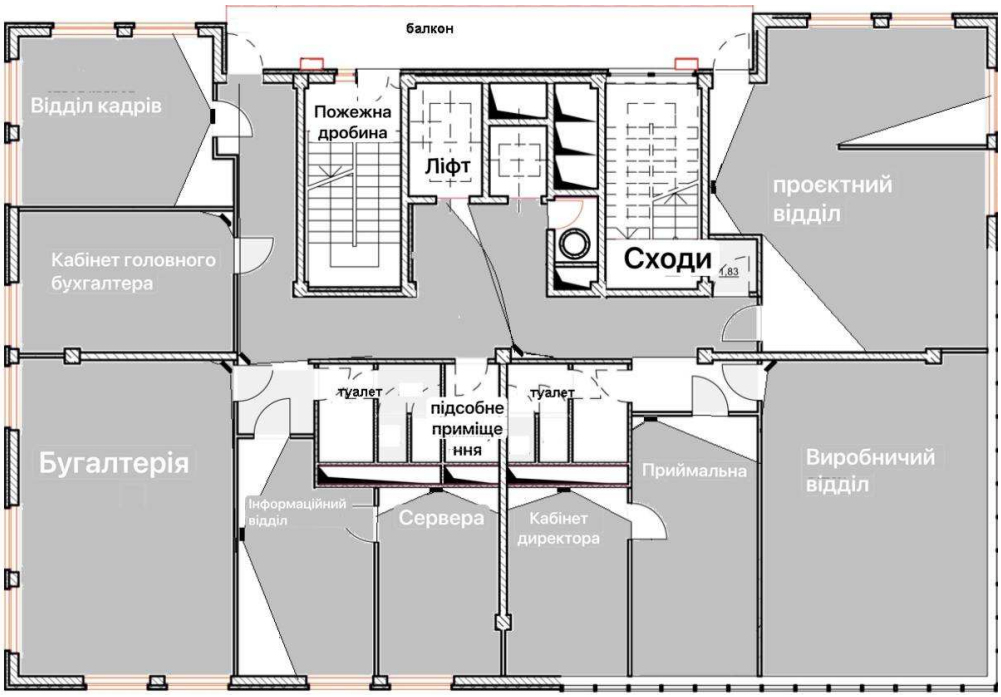

Рис. 2.7. Схема розташування детекторів

Як видно з плану, практично весь офіс при такому розташуванні є охоронною зоною.

Усі запропоновані засоби захисту інформації є актуальними і необхідними для підприємства.

Криптографія є науковим напрямком, що досліджує методи забезпечення конфіденційності, цілісності інформації, аутентифікації, а також безумовності авторства. Криптографія поділяється на два напрямки:

1. Шифрування інформації, пов'язане з оборотнім перетворенням даних для

вчасного виявлення неавторизованих користувачів та дотримання конфіденційності переданих даних.

2. Створення алгоритмів електронного цифрового підпису.

Застосування електронного цифрового підпису в підприємствах передбачає виконання трьох основних правил[22]:

1. Підписання документа за допомогою електронного підпису може виконувати особа, уповноважена відповідними повноваженнями.
2. У випадку виникнення позаштатної ситуації повинна бути передбачена можливість встановлення автентичності електронного підпису.
3. Електронний підпис у мережі обов'язково повинен бути закріплений штампом підприємства.

Застосування секретного ключа для цифрового підпису є надійним методом захисту інформації. Однак, якщо зловмисник увійшов у довіру абоненту, то отримуючи дані про шифрування підписів, він може їх використовувати для передачі іншим абонентам. Для виключення цієї ситуації необхідно використовувати правило підпису лише контрольної суми повідомлення, навіть якщо воно має незначний розмір.

Методи, що дозволяють здійснити ефективне шифрування і дешифрування даних, наведені на рисунку 2.8.

Рис. 2.8. Методи, які дозволяють здійснити ефективне шифрування і дешифрування даних, де а) ефективне шифрування повідомлення, а б) дешифрування зашифрованого повідомлення

Перевагами апаратних методів криптографічних функцій захисту даних є:

1. Можливість забезпечення цілісності даних при реалізації алгоритму криптографічний захист.

2. Шифрування та зберігання ключів у платі апаратного забезпечення, а не у оперативній пам'яті комп'ютера.

3. Створення системи захисту інформації від несанкціонованого доступу до інформації.

Слід зауважити, що криптографічні механізми застосовують для управління ідентичністю, реалізації технології довіреної платформи, розділення доступу, управління авторством, побудови мереж VPN. На відміну від інших методів вони дозволяють забезпечити гарантоване знищення даних та забезпечити високий рівень захисту від фізичної крадіжки носія інформації.

Між переваг криптографічних методів захисту варто відзначити високий рівень захисту даних, економічність у реалізації та ефективність у швидкодії.

Недоліками криптографічних методів захисту є складність у реалізації, що вимагає залучення криптографічних фахівців для забезпечення необхідного рівня захисту даних.

Криптографічні методи захисту інформації відносяться до програмного комплексу захисту інформації, проте в тенденціях сучасного бізнесу це напрямок захисту інформації стає все актуальнішим. Оскільки вся звітність та багато торгових операцій з удосконаленням інформаційних технологій переходять на електронний документообіг, і автентичність документів та підписів необхідно підтверджувати, а також захищати документи від редагування або доступу до них сторонніх осіб, то криптографія як метод захисту інформації на мій погляд є окремим методом у політиці інформаційної безпеки. І криптографічні методи захисту інформації є дуже ефективними.

Висновки до другого розділу

У другому розділі роботи наведено характеристику організаційних, програмно-апаратних, криптографічних методів і засобів захисту, і на основі цього отримано такі висновки: організаційні заходи забезпечення політики інформаційної безпеки підприємства - регламентують документально використання засобів інформаційного захисту, що регламентує роботу всієї політики інформаційної безпеки; апаратні і програмні засоби забезпечення інформаційної безпеки в будівельній компанії дуже ефективні в комплексі, що надає найбільший захист даних і більше відповідає необхідним нормам політики інформаційної безпеки; в даний час серед криптографічних методів і засобів, використовуваних на підприємствах, найбільш ефективними є криптографічний метод захисту створення цифрового або електронного підпису.

РОЗДІЛ 3
ОЦІНКА ЕФЕКТИВНОСТІ ПРОПОЗИЦІЙ ЩОДО УДОСКОНАЛЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ТА УПРАВЛІННЯ НЕЮ

3.1 Метод оцінки доцільності пропозицій щодо удосконалення політики інформаційної безпеки

Економічна ефективність заходів з захисту інформації базується на очевидному факті: з одного боку, порушення захищеності інформації призводить до збитків, а з іншого - забезпечення захисту інформації вимагає витрат. Повна очікувана вартість захисту може бути виражена як сума витрат на захист та втрат від порушення захищеності. Зрозуміло, що оптимальним рішенням було б виділення коштів на захист інформації, що мінімізує загальну вартість робіт з захисту.

Також, економічна ефективність заходів з захисту інформації може бути визначена через обсяг відвернутих збитків або ризиків для інформаційних активів організації. Оскільки оптимальне рішення щодо рівня витрат на захист полягає в тому, що цей рівень повинен дорівнювати рівню очікуваних збитків в разі порушення захищеності, досить визначити лише рівень збитків. Одним із методів визначення рівня витрат може бути використання наступної емпіричної залежності очікуваних збитків (ризиків) від загрози інформації (і-загрози)[23]:

$$R_i = 10^{S_i V_i - 4} \tag{3.1}$$

де, S_i - коефіцієнт, що відображає можливу частоту виникнення відповідної загрози;

V_i- коефіцієнт, який відображає значення можливої шкоди при її виникненні.

Таблиця 3.1

Значення коефіцієнтів S_i та V_i

Очікувана (можлива) частота появи загроз	**Передбачуване значенняS_i**
Майже ніколи	0
1 раз в 1000 років	1
1 раз в 100 років	2
1 раз в 10 років	3
1 раз в рік	4
1 раз на місяць (приблизно 10 разів на рік)	5
1-2 разів на тиждень (приблизно 100 разів на рік)	6
3 рази на день (приблизно 1000 разів на рік)	7
Можливий збиток при прояві загроз (грн.)	**Передбачуване значення V_i**
30	0
300	1
3000	2
30000	3
300000	4
3000000	5
30000000	6
300000000	7

Сумарна вартість втрат визначається формулою:

$$R = {}_{i=1}^{N} R_i \qquad (3.2)$$

де, N – кількість загроз інформаційним активам

При розрахунку загального показника рекомендується вважати, що загрози конфіденційності, цілісності та доступності реалізуються зловмисником незалежно одна від одної. Це означає, що якщо в результаті дій

зловмисника може бути порушена цілісність інформації, але її зміст залишається для нього невідомим (конфіденційність не порушена), а авторизовані користувачі все ще мають доступ до активів, навіть якщо вони спотворені.

Таблиця 3.2

Величини втрат (загроз) для критичних інформаційних ресурсів до запровадження модернізації захисту інформації

Актив	**Загроза**	**Величина втрат (тис. грн.)**
Проектна документація розроблена підприємством	конфіденційності	100
Проектна документація розроблена підприємством	цілісності	500
Проектна документація розроблена підприємством	доступності	20
Проектна документація отримана від замовника	конфіденційності	100
Проектна документація отримана від замовника	цілісності	100
Проектна документація отримана від замовника	доступності	20
Проектна документація, плани комунікацій зокрема стратегічного призначення	конфіденційності	500
Проектна документація, плани комунікацій зокрема стратегічного призначення	цілісності	100
Проектна документація, плани комунікацій зокрема стратегічного призначення	доступності	20
Особисті дані клієнта	конфіденційності	300
Особисті дані клієнта	цілісності	20
Особисті дані клієнта	доступності	20
Особисті дані співробітників	конфіденційності	100
Особисті дані співробітників	цілісності	10
Особисті дані співробітників	доступності	10
Системне програмне забезпечення	конфіденційності	0
Системне програмне забезпечення	цілісності	100
Системне програмне забезпечення	доступності	100
Прикладне програмне забезпечення (зокрема САПР, CMS, ERP, CRM тощо)	конфіденційності	0
Прикладне програмне забезпечення (зокрема САПР, CMS, ERP, CRM тощо)	цілісності	100
Прикладне програмне забезпечення (зокрема САПР, CMS, ERP, CRM тощо)	доступності	100
Загальна величина втрат		2320

Після проведення розрахунків і побудови таблиці 3.2 ми визначили ризик фінансових втрат для підприємства, який може становити приблизно 2 320 000 гривень. З цього можна зробити висновок, що для підприємства це буде дуже значною втратою. Для оцінки того, наскільки ефективна отримана політика інформаційної безпеки, необхідно здійснити розрахунок показників економічної ефективності нової моделі управління безпекою.

3.2. Економічна ефективність пропозицій щодо покращення політики захисту інформації та управління нею на підприємств

Ризик власника інформації залежить від рівня інженерно-технічного захисту інформації, який, в свою чергу, визначається ресурсами системи.

Ресурс може бути визначений у вигляді кількості людей, залучених до захисту інформації, інженерних конструкцій та технічних засобів, що використовуються для захисту, грошових сум для оплати праці людей, будівництва, розробки та покупки технічних засобів, їх експлуатації та інших витрат. Найбільш загальним способом вираження ресурсу є грошова міра. Ресурс, виділений на захист інформації, може мати одноразовий і постійний характер.

Одноразові ресурси витрачаються на закупівлю, установку та налагодження дорогих технічних засобів.

Постійні ресурси - на заробітну плату працівникам служби безпеки та підтримку певного рівня безпеки, передусім шляхом експлуатації технічних засобів та контролю ефективності захисту.

Отже, для визначення економічної ефективності захисту інформації підприємства необхідні наступні дані (показники):

- витрати (виділені ресурси) на створення/модернізацію даного та його підтримання в робочому стані;

- величини втрат (ризиків), обумовлених загрозами інформаційним

активам після впровадження/модернізації захисту інформації.

Дані щодо змісту та об'єму разового ресурсу, який виділяється на захист інформації, зазначені в Додатку А в таблиці 3.3. [21]

Таблиця 3.4

Зміст та об’єм постійного ресурсу, який виділяють на захист інформації

Організаційні заходи				
№	Виконані дії	Середня погодинна заробітна плата спеціаліста (грн.)	Трудомісткість дії (людини на годину)	Вартість всього(тис. грн.)
1	Проведення тренінгів, інструктажів	300	100	300
Вартість проведення організаційних заходів всього				300
Заходи інженерно-технічного захисту				
№	Номенклатура витратних матеріалів	Вартість одиниці (тис. грн.)	Кількість матеріалу (одиниця виміру)	Вартість всього (тис. грн.)
2	Оновлення ПО	150	10	150
3	Обслуговування відео нагляду	3	100	30
4	Обслуговування детекторів руху	3	100	30
5	Обслуговування протипожежної системи	3	200	60
Вартість проведення заходів інженерно-технічного захисту				270

Отже, для розробки системи інформаційної безпеки потрібно 3556,4 тисяч гривень, а для щорічного обслуговування - 570 тисяч гривень. Для проведення розрахунків необхідно отримати прогнозовані дані про розмір втрат (ризиків) для критичних інформаційних ресурсів після впровадження/модернізації захисту інформації. Результати формуються на основі експертного опитування.

Таблиця 3.5

Величини втрат (ризиків) для критичних інформаційних ресурсів після модернізації захисту інформації

Актив	**Загроза**	**Величина втрат (тис. грн.)**
Проектна документація розроблена підприємством	конфіденційності	10
Проектна документація розроблена підприємством	цілісності	50
Проектна документація розроблена підприємством	доступності	2
Проектна документація отримана від замовника	конфіденційності	10
Проектна документація отримана від замовника	цілісності	10
Проектна документація отримана від замовника	доступності	20
Проектна документація, плани комунікацій зокрема стратегічного призначення	конфіденційності	50
Проектна документація, плани комунікацій зокрема стратегічного призначення	цілісності	10
Проектна документація, плани комунікацій зокрема стратегічного призначення	доступності	2
Особисті дані клієнта	конфіденційності	30
Особисті дані клієнта	цілісності	2
Особисті дані клієнта	доступності	2
Особисті дані співробітників	конфіденційності	10
Особисті дані співробітників	цілісності	1
Особисті дані співробітників	доступності	1
Системне програмне забезпечення	конфіденційності	0
Системне програмне забезпечення	цілісності	10
Системне програмне забезпечення	доступності	10
Прикладне програмне забезпечення (зокрема САПР, CMS, ERP, CRM тощо)	конфіденційності	0
Прикладне програмне забезпечення (зокрема САПР, CMS, ERP, CRM тощо)	цілісності	10
Прикладне програмне забезпечення (зокрема САПР, CMS, ERP, CRM тощо)	доступності	10
Загальна величина втрат		232

Таблиця 3.6

Оцінка динаміки величини втрат за певний період (2 роки)

	1 кв.	2 кв.	3 кв.	1 рік	1 кв.	2 кв.	3 кв.	2 рік
До запровадження СЗІ	580	1160	1740	2320	2900	3480	4060	4640
Після впровадження СЗІ	58	116	174	232	290	348	406	464
Зниження втрат	522	1044	1566	2088	2610	3132	3654	4176

Після прийняття обов'язкових припущень про незмінність частоти появи загроз, а також про незмінний рівень надійності створеного захисту інформації, можливо визначити строк окупності (T_{ok}). Це виконується аналітичним методом за допомогою наведеної нижче формули:

$$T_{Ok} = \frac{R_{\Sigma}}{(\mathrm{R_{ср}} - \mathrm{R_{прогн}})} \tag{3.3}$$

та графічно, як приведено нижче:

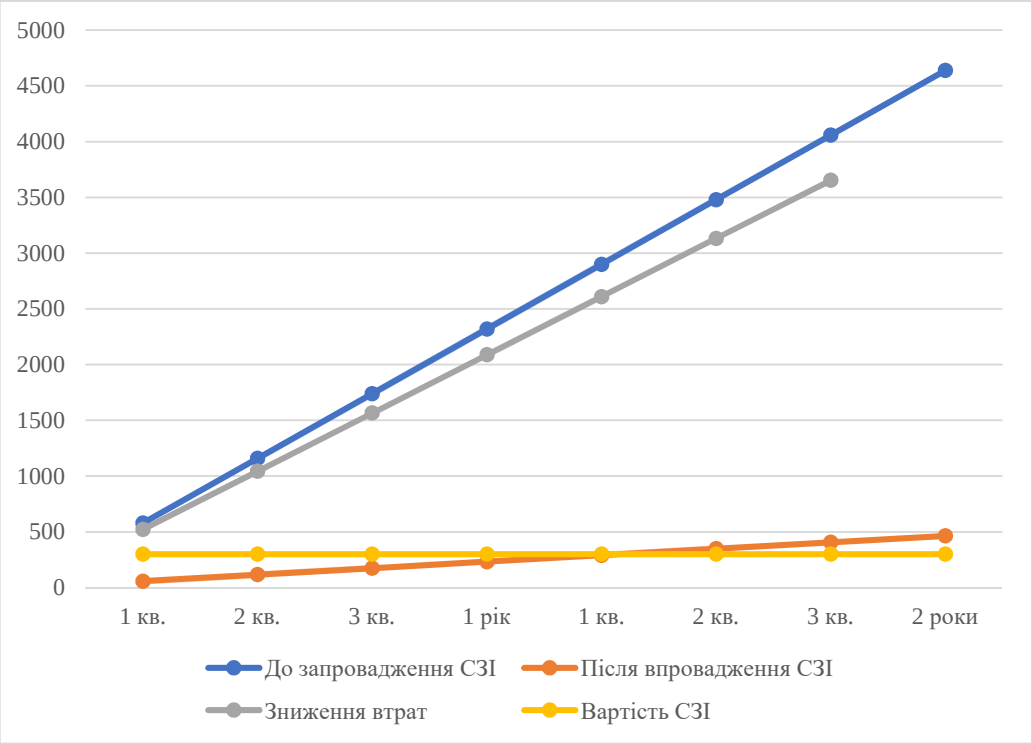

Рис. 3.1. Графічне визначення терміну окупності

Висновки до третього розділу

Отже, економічні розрахунки показують ефективність впровадження комплексу заходів інформаційного захисту. Згідно проведених розрахунків, відшкодування витрат на інформаційну безпеку відбудеться ще в першому кварталі її використання. Це для підприємства є дуже мінімальним фінансовим навантаженням.

У цьому розділі були проведені розрахунки, з яких можемо бачити, що передбачений збиток є досить значним для підприємства, а одноразові витрати на впровадження політики інформаційної безпеки менше, ніж припущений фінансовий збиток. Це свідчить про те, що реалізація політики інформаційної безпеки допоможе захистити дані, і це буде ефективний захист, який допоможе запобігти фінансовим втратам компанії від можливих загроз. І через 2 роки політика інформаційної безпеки, реалізована в компанії, допоможе захистити приблизно чотири мільйони гривень. Відповідно можна зробити висновок, що розроблена політика інформаційної безпеки є дуже ефективною

ВИСНОВКИ

У процесі виконання випускної кваліфікаційної роботи була розроблена політика інформаційної безпеки підприємства. Проведений аналіз основних положень теорії захисту інформації показав, що для створення політики інформаційної безпеки необхідно розробити цілий ряд документів та інструкцій, спрямованих на захист інформації. Не можна зупинятися лише на одному методі захисту інформації, оскільки це може поставити під загрозу захист даних. Захист даних повинен бути комплексним. Комплексна політика інформаційної безпеки включає розробку, виробництво та встановлення технічних засобів захисту, а також регулярне проведення перевірки використовуваного інформаційного обладнання. В даний час багато підприємств здійснюють роботу з атестації інформатизованих об'єктів на відповідність вимогам інформаційної безпеки.

У межах цього проекту була розроблена комплексна система захисту інформації на підприємстві. Розробка цього проекту включала наступне:

- виявлення недоліків діючого інформаційного захисту підприємства;

- виявлення типів загроз, які можуть виникнути внаслідок недоліків у захисті інформаційних систем підприємства;

- вибір методів та способів вирішення існуючих проблем.

В якості рішення був розроблений комплекс заходів, що складається з:

- адміністративних рішень, які регулюють можливості витоку інформації внаслідок впливу людського чинника;

- програмно-апаратних рішень, які дозволили мінімізувати ризик виникнення атак на інформаційні канали зовнішнього середовища або з використанням різних пристроїв зберігання інформації;

- інженерно-технічних рішень, які дозволять запобігти пошкодженню або крадіжці різних сховищ інформації, мінімізувати ризик виникнення атак на інформаційні канали зовнішнього середовища або з використанням різних

пристроїв зберігання інформації, а також пошкодженню їх внаслідок різних форс-мажорних обставин.

На основі аналізу основних методів та засобів захисту інформації встановлено, що організаційно-правові методи та засоби захисту інформації повинні спрямовуватися на протидію загрозам інформаційної безпеки, знижувати ризики та ефективно обробляти інциденти з метою тривалого забезпечення достатнього рівня захисту даних. Інженерно-технічні методи захисту інформації базуються на захисті інформації на контрольованій території, всередині приміщень, мережі, програмному забезпеченні та наявних базах даних. Апаратно-програмні методи захисту спрямовані на забезпечення мережевої безпеки на рівні мережі, користувача, включаючи рівень додатків. На сьогодні серед криптографічних методів та засобів, які використовуються на підприємствах, найбільш ефективним є криптографічний метод створення цифрового або електронного підпису. На основі проведеного аналізу найбільш ефективними методами та засобами захисту інформації є комплекс заходів як інженерно-технічні методи та засоби, що дозволяють забезпечити комплексний захист даних на підприємстві, так і апаратно-програмні та криптографічні. Політика інформаційної безпеки розроблена і її ефективність доведена. Оцінка ефективності запропонованих заходів показала їх доцільність впровадження в організаціях. На кінцевому етапі проекту було дано економічне обґрунтування ефективності та окупності захисту інформації, в результаті якого було встановлено, що окупність захисту настає протягом кількох років, при цьому час окупності прямо пропорційний кількості відбитих атак, а ефективність буде зростати з кожним роком. Ураховуючи, що всі поставлені завдання повністю вирішені, можна обґрунтовано стверджувати, що головна мета дослідження досягнута.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Економіка та управління АПК: Зб. наук. праць / Білоцерк. нац. аграр. ун-т – Біла Церква, 2013.– Вип. 10 (102).– 204 с. с.65.
2. Учасники проектів Вікімедіа. Апаратне забезпечення – Вікіпедія. Вікіпедія. URL: https://uk.m.wikipedia.org/wiki/Апаратне_забезпечення (дата звернення: 14.05.2024).
3. Матеріали VII Міжнародної науково-практичної конференції “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення: тези доповідей, 1 листопада 2023 р. – Кропивницький: ЦНТУ, 2023. – 135 с . с.43.
4. Залізняк В.К. Захист інформації від витоку по технічним каналам: Навчальний посібник. – 188 с. (с 46)
5. ТЗІ - інформаційна безпека та захист інформації. URL: https://tzi.com.ua/downloads/3.7-001-99.pdf дата звернення: 14.05.2024).
6. Чи існує в Україні інформаційна безпека? - Мережа UPLAN. Мережа UPLAN. URL: https://uplan.org.ua/analytics/chy-isnuie-v-ukraini-informatsiina-bezpeka/ (дата звернення: 14.05.2024).
7. Безпека інформації : конспект лекцій / укладач О. С. Кушнерьов. – Суми : Сумський державний університет, 2021. – 99 с.с 43.
8. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
9. Федулова С. О. Інформаційна безпека та захист інтелектуальної власності на бази даних. *Економічний вісник ДВНЗ "Український державний хіміко-технологічний університет"*. 2016. № 2 (4). С. 189–193.
10. НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ АСПЕКТИ БЕЗПЕКИ Настанови щодо їх включення до стандартів. Вид. офіц.
11. Звіт незалежного аудитора. Щодо річної фінансової звітності ТОВ Будівельний Альянс. 31.12.2021. 41 с.

12. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT). *БУДСТАНДАРТ Online - нормативні документи будівельної галузі України*. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=66911 (дата звернення: 19.05.2024).
13. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Каб. Міністрів України від 29.03.2006 р. № 373 : станом на 21 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text (дата звернення: 14.05.2024).
14. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 р. № 1229/99 : станом на 4 трав. 2008 р. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text (дата звернення: 14.05.2024).
15. Про затвердження Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації : Наказ Адмін. Держ. служби спец. зв'язку та зах. інформації України від 22.03.2007 р. № 36 : станом на 27 черв. 2013 р. URL: https://zakon.rada.gov.ua/laws/show/z0312-07#Text (дата звернення: 14.05.2024).
16. Про затвердження Концепції технічного захисту інформації в Україні : Постанова Каб. Міністрів України від 08.10.1997 р. № 1126 : станом на 13 жовт. 2011 р. URL: https://zakon.rada.gov.ua/laws/show/1126-97-п#Text (дата звернення: 14.05.2024).
17. Про платіжні послуги : Закон України від 30.06.2021 р. № 1591-IX : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text (дата звернення: 19.05.2024).
18. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 19.05.2024).

19. Бервено С. Л. Застосування методології теорії управління у сфері технічного захисту інформації. *Держава і право*. 2006. Вип. 32. С. 222–227.
20. Ужгородський національний університет. Організація та технологія захисту інформації URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186 (дата звернення: 14.05.2024).
21. Hulkov M., Tolkachov V. Технічний захист інформації, як складова інформаційної безпеки, у контексті євроатлантичної інтеграції України. Сучасні інформаційні технології у сфері безпеки та оборони. 2019. Т. 36, № 3. С. 59–64. URL: https://doi.org/10.33099/2311-7249/2019-36-3-59-64 дата звернення: 14.05.2024).
22. Потій О., Лєншин А., "Методика оцінки відповідності поточної зрілості цільовим орієнтирам", Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник, Вип. 1(12), с. 31 – 43, 2006.
23. Sk F. Journal Vol – 15 No -7, July 2020 Journal > Journal > Journal Vol – 15 No -7, July 2020 > Page 6 PERFORMANCE AND EMISSION CHARACTERISTICS OF GASOLINE-ETHANOL BLENDS ON PFI-SI ENGINE Authors: D.Vinay Kumar ,G.Samhita Priyadarsini,V.Jagadeesh Babu,Y.Sai Varun Teja, DOI NO: https://doi.org/10.26782/jmcms.2020.07.00051 admin July 26, 2020 Abstract: Alcohol based fuels can be produced from ren. *JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES*. 2020. Т. 15, № 7. URL: https://doi.org/10.26782/jmcms.2020.07.00056 (дата звернення: 14.05.2024).

ДОДАТОК А

Таблиця А.1

Зміст та об’єм разового ресурсу, який виділяється на захист інформації

Організація заходів				
№	Виконавчі дії	Середньо погодинна заробітна плата спеціалістів (грн.)	Трудомісткість дії (людини за годину)	Вартість всього (тис. грн.)
1	Розробка методики та наказів	220	5	1100
2	Доведення інформації до співробітників, навчання, тренінги	220	2	440
Вартість проведення організаційних заходів всього				1540
Заходи інженерно-технічного захисту				
№	Номенклатура витратних матеріалів	Вартість одиниці (тис. грн.)	Кількість (одиниця виміру)	Вартість всього (тис. грн.)
1	Лліцензійна версія TrafficQuota	3	1	3
2	Лліцензійна версія TrafficInspector	3,5	1	3,5
3	Лліцензійна версія ISA Server	5,2	1	5,2
4	комплексне рішення в комплекті з антиспамом, фаерволом, захистом електронної пошти	2	16	32
5	Ліцензія на ОС Windows 10 з можливістю дунґрейда до 7	9,2	16	147,2
6	Установка та обновлення програмного забезпечення люд./год.	0,3	40	12
7	Пломби та інструменти опломбування	12	1	12

Продовження таблиці А.1

8	Опломбування люд./год	0,3	8	2,4
9	Зачинні пристрої	1	5	5
10	Монтаж запірних пристроїв	0,2	5	1
11	Камери відеоспостереження	5,2	4	20,8
12	Проводи, з'єднувачі, роз'єми тощо	3,5	1	3,5
13	Система архівування записів відеоспостереження	7	1	7
14	Монтаж відеоспостереження люд./год.	0,3	10	3
15	Детектор руху	1	11	11
16	Проводи, з'єднувачі, роз'єми тощо	3,5	1	3,5
17	Пульт контролю та оповіщення	6	1	6
18	Монтаж датчиків руху люд./год.	0,3	12	3,6
19	Датчики задимлення	0,8	26	20,8
20	Проводи, з'єднувачі, роз'єми тощо	3,5	1	3,5
21	Монтаж протипожежної системи оповіщення	0,3	12	3,6
22	Засоби річні протипожежні	0,5	10	5
23	Засоби автоматизованого пожежогасіння	30	1	30
24	Проводи, з'єднувачі, роз'єми тощо	3,5	1	3,5
25	Монтаж протипожежний люд./год.	0,3	20	6
Вартість проведення заходів інженерно технічного захисту				354,1