

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА
ФРАНКА

Факультет прикладної математики та інформатики

(повне найменування назва факультету)

кібербезпеки

(повна назва кафедри)

ДИПЛОМНА РОБОТА

**Розробка проекту захисту від несанкціонованого доступу до
інформації на підприємстві**

Виконав: студент групи ПМК-42с
спеціальності

125 «Кібербезпеки»

(шифр і назва спеціальності)

		<u>Скакодуб К.С.</u>
	(підпис)	(прізвище та ініціали)
Керівник		<u>Комар К.В.</u>
	(підпис)	(прізвище та ініціали)
Науковий консультант		<u>Вайганг Г.О.</u>
	(підпис)	(прізвище та ініціали)
Рецензент		<u>Гордєєв Д.О.</u>
	(підпис)	(прізвище та ініціали)



2023

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Факультет Прикладної математики та інформатики

Кафедра Кібербезпеки

Спеціальність 125 «Кібербезпека»

(шифр і назва)

«ЗАТВЕРДЖУЮ»

Завідувач кафедри



"31" серпня 2022 року

З А В Д А Н Н Я

НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

СКАКОДУБА КИРИЛА СЕРГІЙОВИЧА

1. Тема роботи: Розробка проекту захисту від несанкціонованого доступу до інформації на підприємстві

Керівник роботи: Комар Катерина Вячеславівна

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені Вченою радою факультету від "**13**" **вересня 2022 року № 15**

2. Строк подання студентом роботи 13.06.2023р.

3. Вихідні дані до роботи: Аналіз системи інформаційного захисту, вимоги щодо захисту інформації, опис структури та функцій системи захисту, оцінка ефективності проекту захисту.

4. Зміст дипломної роботи (перелік питань, які потрібно розробити)

1. Теоретичні основи захисту інформації
2. Аналіз системи інформаційного захисту
3. Розробка проекту захисту інформації
4. Оцінка ефективності проекту захисту інформації

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

1. Презентація доповіді, виконана в PowerPoint.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Теоретичні основи захисту інформації	01.04.23	10.04.23
2	Аналіз системи інформаційного захисту	10.04.23	20.04.23
3	Розробка проекту захисту інформації	20.04.23	10.05.23
4	Оцінка ефективності проекту захисту інформації	15.05.23	20.05.23

7. Дата видачі завдання 31 серпня 2022 р.

**КАЛЕНДАРНИЙ
ПЛАН**

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Уточнення постановки завдання	28.03.2023 р.	
2	Аналіз літератури	29.03.2023 р.	
3	Обґрунтування вибору рішення	31.03.2023 р.	
4	Збір даних	10.04.2023 р.	
5	Теоретичні основи захисту інформації	01.04.2023 р.	
6	Аналіз системи інформаційного захисту	10.04.2023 р.	
7	Розробка проекту захисту інформації	20.04.2023 р.	
8	Оцінка ефективності проекту захисту інформації	15.05.2023 р.	
9	Оформлення та друк пояснювальної записки	08.06.2023 р.	
10	Оформлення презентацій	09.06.2023 р.	
11	Отримання рецензій	10.06.2022 р.	
12	Захист в ЕК	16.06.2023 р.	

Студент  **Скакодуб К.С.**
(підпис) (прізвище та ініціали)

Керівник роботи  **Комар К.В.**
(підпис) (прізвище та ініціали)

Зміст

ВСТУП	4
Обґрунтування актуальності теми.....	5
Мета та завдання дослідження	7
Об'єкт та предмет дослідження.....	8
РОЗДІЛ 1	11
Теоретичні основи захисту інформації	11
Поняття та класифікація інформації	11
Методи та засоби захисту інформації.....	13
Політика захисту інформації на підприємстві:	15
РОЗДІЛ 2	17
Аналіз існуючої системи захисту інформації на підприємстві	17
Опис існуючої системи захисту інформації на підприємстві XYZ.....	17
Аналіз виявлених недоліків та проблем існуючої системи захисту інформації.....	18
Оцінка потенційних загроз безпеці інформації на підприємстві	22
Визначення критично важливих активів та даних, які потребують особливого захисту.....	25
Розробка рекомендацій щодо поліпшення системи захисту інформації.....	27
РОЗДІЛ 3	28
Розробка проекту захисту інформації на підприємстві	28
Визначення вимог до системи захисту інформації.....	28
Вибір методів та засобів захисту інформації.....	32
Розробка архітектури системи захисту інформації.....	33
Розробка процедур та правил використання системи захисту інформації.....	34
РОЗДІЛ 4	36
Реалізація проекту захисту інформації на підприємстві	
Опис структури та функцій системи захисту інформації:	36
Опис процедур та правил використання системи захисту інформації:	38
Оцінка ефективності проекту захисту інформації на підприємстві:	39
ВИСНОВКИ	41
Рекомендації щодо покращення системи захисту інформації на підприємстві	42
Можливості подальших досліджень	43
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:	45
Нормативно-правова база:.....	45
Вітчизняні та зарубіжні джерела та публікації:	45
ДОДАТКИ	46
Код програмного забезпечення системи захисту інформації	46

Вступ

Обґрунтування актуальності теми

Розробка проекту захисту від несанкціонованого доступу до інформації на підприємстві є надзвичайно актуальною та важливою проблемою в сучасному інформаційному середовищі. З плином часу та зростанням залежності від інформаційних систем, підприємства стають дедалі більш уразливими перед загрозами, пов'язаними з несанкціонованим доступом до конфіденційної та важливої інформації.

Підприємство XYZ повинно бути готовим до виявлення, запобігання і ефективного реагування на такі загрози безпеки даних. Одним із найважливіших аспектів є своєчасне оновлення політик та процедур безпеки інформації, а також навчання співробітників щодо кращих практик та поведінки в цифровому середовищі.

З метою попередження зовнішніх загроз, необхідно забезпечити належний рівень захисту мережі та системи. Це може включати встановлення та оновлення брандмауерів, антивірусного програмного забезпечення, систем виявлення вторгнень, а також регулярне встановлення патчів і оновлень для програмного забезпечення. Крім того, слід розглянути можливість використання системи перевірки безпеки, яка буде сканувати мережу на наявність потенційних вразливостей та допомагати у їх усуненні.

Внутрішні загрози безпеки даних можуть бути складнішими для виявлення, оскільки вони можуть впливати з самого підприємства. Важливо встановити строгі політики доступу до інформації, обмежити привілеї користувачів на основі їх ролей та встановити механізми

моніторингу доступу до критичних ресурсів. Проведення регулярних перевірок безпеки даних, аудитів та журналювання подій можуть допомогти виявити підозрілу активність та вчасно реагувати на можливі випадки порушення безпеки.

Крім того, важливо забезпечити належне навчання співробітників щодо безпеки інформації. Це включає проведення регулярних навчальних програм, організацію тренінгів з в

икористанням реальних сценаріїв атак та надання рекомендацій щодо безпечної роботи з даними. Співробітники повинні бути свідомі ризиків інформаційної безпеки, вміти виявляти підозрілу активність та вживати відповідні заходи безпеки.

Нарешті, важливо мати ефективні механізми відновлення після інцидентів безпеки. Це включає регулярні резервне копіювання даних, створення планів відновлення після інциденту та проведення тестування цих планів. У разі виникнення порушення безпеки важливо швидко реагувати, ізолювати інцидент, відновлювати систему та проводити аналіз інциденту для попередження подібних ситуацій у майбутньому.

Загальним підходом до безпеки даних на підприємстві повинна бути системна стратегія, що поєднує технологічні заходи, політики та процедури, а також навчання та свідоме ставлення співробітників до безпеки інформації. Тільки такий комплексний підхід дозволить забезпечити належний рівень захисту даних і підтримувати впевненість клієнтів та партнерів в безпековості підприємства.

Отже, розробка ефективного проекту захисту від несанкціонованого доступу до інформації на підприємстві є необхідною для забезпечення конфіденційності, цілісності та доступності даних. Це стає невід'ємною складовою успішного функціонування підприємства в сучасному цифровому світі.

Мета та завдання дослідження

Метою даної дипломної роботи є розробка проекту захисту від несанкціонованого доступу до інформації на підприємстві з метою забезпечення високого рівня безпеки та конфіденційності даних.

Основним завданням дослідження є:

- Провести аналіз існуючих систем захисту від несанкціонованого доступу до інформації на підприємстві. Вивчити методи та практики, використовувані для захисту даних в різних організаціях.
- Визначити уразливості та загрози, що можуть виникнути при несанкціонованому доступі до інформації на підприємстві. Розібратися з можливими сценаріями атак та виявити слабкі місця в системі безпеки.
- Розробити концепцію проекту захисту, яка включатиме стратегії та методи захисту, що відповідають виявленим загрозам і вимогам підприємства.
- Розробити архітектуру та складові проекту захисту. Визначити необхідні апаратні та програмні компоненти, механізми аутентифікації, шифрування, контролю доступу та моніторингу.
- Реалізувати розроблений проект захисту від несанкціонованого доступу до інформації на підприємстві та провести його тестування та оцінку ефективності.

- Зробити висновки щодо ефективності та придатності розробленого проекту та надати рекомендації щодо його впровадження на підприємстві.
- Дослідження цих завдань дозволить створити надійну та ефективну систему захисту від несанкціонованого доступу до інформації на підприємстві, що сприятиме забезпеченню безпеки та конфіденційності даних, а також зниженню ризику витоку та недоброзичливого використання інформації.
- Розробити план впровадження проекту захисту. Визначити етапи реалізації, враховуючи ресурси, бюджет та терміни.
- Оцінити ефективність та результативність реалізованого проекту. Порівняти його з попередніми показниками безпеки та виявити поліпшення, що були досягнуті.
- Проаналізувати потенційні ризики та виклики, пов'язані з використанням розробленого проекту та запропонувати стратегії постійного покращення безпеки інформації.
- Зробити висновки з проведеного дослідження та дати рекомендації з подальшого вдосконалення системи захисту від несанкціонованого доступу до інформації на підприємстві.
- Сформулювати заключні висновки та підсумки роботи, підкреслити значення розробленого проекту та його внесок у сферу інформаційної безпеки підприємства.

Об'єкт та предмет дослідження

Об'єктом дослідження є компанія «XYZ». Компанія "XYZ" - це середнього розміру підприємство, що активно діє у сфері надання послуг (або виробництва товарів) в конкретній галузі. Залежно від галузі, в якій вона працює, компанія може забезпечувати інформаційні технології для

підтримки бізнесу, фінансові послуги для клієнтів, медичні рішення для покращення здоров'я та багато іншого.

У сучасному цифровому світі підприємства стикаються з різноманітними викликами, пов'язаними з безпекою інформації, тому компанія "XYZ" приділяє велику увагу захисту своїх даних і дотриманню вимог безпеки. Враховуючи важливість збереження конфіденційності, цілісності та доступності інформації, компанія активно розробляє та впроваджує системи та процедури безпеки, які допомагають уникнути можливих загроз та зберегти довіру своїх клієнтів та партнерів.

Однією з основних метою компанії "XYZ" є захист конфіденційної інформації від несанкціонованого доступу. Для досягнення цієї мети компанія використовує різні технічні і організаційні заходи, такі як аутентифікація користувачів, контроль доступу до ресурсів, шифрування даних та інші. Це дозволяє забезпечити високий рівень безпеки інформації та уникнути можливих порушень безпеки.

Крім того, компанія "XYZ" активно вдосконалює свою систему виявлення та реагування на загрози безпеки. Вона встановлює моніторингові системи, які допомагають виявляти незвичайну активність, аналізувати журнали подій та швидко реагувати на можливі інциденти. Це дозволяє компанії вчасно виявляти та реагувати на потенційні загрози, зменшувати ризик втрати даних та забезпечувати непереривну роботу бізнесу.

Компанія "XYZ" також враховує внутрішні загрози безпеки, пов'язані зі своїми співробітниками. Вона проводить навчання та свідомо ставиться до вимог безпеки серед свого персоналу. Регулярні школи безпеки та нагадування про правила використання інформації допомагають

забезпечити, що співробітники розуміють важливість захисту даних і свою відповідальність у цьому питанні.

Усі ці заходи посилюють довіру клієнтів та партнерів до компанії "XYZ" та її здатність забезпечувати безпеку їхніх даних. Компанія продовжує вдосконалювати свою систему захисту інформації, слідує за останніми тенденціями в галузі інформаційної безпеки та завжди готова адаптуватися до нових загроз та викликів. В цілому, компанія "XYZ" ставить безпеку даних на перше місце та прагне забезпечити найвищий рівень захисту для всієї своєї інформації.

Вона зберігає значну кількість конфіденційної та важливої інформації, включаючи персональні дані клієнтів, фінансові дані, інтелектуальну власність та інші види чутливої інформації.

Предметом дослідження є розробка проекту захисту від несанкціонованого доступу до інформації на компанії «XYZ».

Дослідження передбачає аналіз існуючих систем захисту на підприємстві, виявлення потенційних загроз та уразливостей, розробку концепції та архітектури системи захисту, впровадження необхідних апаратних та програмних компонентів, а також тестування та оцінку ефективності розробленого проекту.

Метою дослідження є забезпечення високого рівня безпеки, конфіденційності та доступності інформації на компанії «XYZ», а також запобігання можливим загрозам, витоку даних та несанкціонованому використанню інформації. Дослідження спрямоване на розробку та впровадження ефективних стратегій, методів та технологій захисту, що враховують специфіку компанії «XYZ» та її потреби в безпеці інформації.

Розділ 1

Теоретичні основи захисту інформації

Поняття та класифікація інформації

Інформація є необхідною складовою сучасного світу, де величезна кількість даних генерується, обмінюється та зберігається щодня. Вона виступає в різних формах і має велике значення для спілкування, прийняття рішень і розуміння оточуючого середовища. Інформація може бути у текстовому вигляді, представлена зображеннями, звуком, відео та іншими форматами, які дозволяють нам отримати певні знання і сприйняти світ більш повно.

Для передачі, зберігання та обробки інформації використовуються різні засоби та технології. В цифрову епоху інформація передається через комп'ютерні мережі, Інтернет та інші зв'язкові системи. За допомогою електронних засобів, таких як комп'ютери, смартфони, планшети, ми можемо обмінюватися інформацією в режимі реального часу, ділитися файлами, спілкуватися через електронну пошту, соціальні мережі та інші комунікаційні канали.

Однак, важливо зрозуміти, що інформація потребує захисту, оскільки велика кількість даних може бути чутливою та приватною. Зловмисники можуть намагатися зламати системи, отримати незаконний доступ до інформації, викрасти особисті дані або пошкодити їх. Тому безпека інформації стає особливо важливою в сучасному цифровому світі. Підприємства та організації вкладають значні зусилля у розробку та

впровадження систем захисту даних, шифрування, аутентифікації користувачів та інших методів для забезпечення конфіденційності, цілісності та доступності інформації.

Загрози безпеці інформації постійно змінюються і еволюціонують разом із розвитком технологій. Суттєві виклики включають хакерські атаки, віруси, фішинг, крадіжку даних та інші форми кіберзлочинності. Крім того, внутрішні загрози, такі як несанкціонований доступ співробітників або недбале використання ресурсів, також можуть призвести до витоку чутливої інформації.

Оскільки інформація є цінним активом, компанії повинні приділяти належну увагу захисту даних, розробляти стратегії безпеки, впроваджувати заходи контролю доступу, шифрування та журналювання подій. Це допомагає забезпечити конфіденційність, цілісність та доступність інформації, а також підтримувати довіру клієнтів та бізнес-партнерів. Постійне вдосконалення системи захисту інформації та свідомість персоналу становлять важливу частину загальної стратегії безпеки даних компанії, дозволяючи їй протистояти сучасним загрозам і забезпечувати високий рівень захисту.

За міжнародними стандартами інформацію можна класифікувати залежно від рівня конфіденційності, цілісності та доступності. Класифікація допомагає встановити рівень захисту, який потрібно застосовувати до кожного типу інформації.

Основні рівні класифікації інформації включають:

1. Секретна інформація: Інформація, яка має найвищий рівень конфіденційності та потребує особливого захисту. Це можуть бути

комерційні таємниці, важливі дані про проектування, стратегічні плани, персональні дані клієнтів тощо.

2. Інформація обмеженого доступу: Інформація, яка має помірний рівень конфіденційності та обмежений доступ. Вона може включати конфіденційні дані про внутрішню структуру підприємства, фінансові звіти, договори з партнерами тощо.

3. Інформація загального доступу: Інформація, яка не має обмежень стосовно доступу або конфіденційності. Це можуть бути публічно доступні дані, інформація про продукти та послуги підприємства, публічні заяви тощо.

Класифікація інформації допомагає визначити необхідні заходи та політику захисту для кожного типу інформації з метою забезпечення конфіденційності, цілісності та доступності даних на підприємстві.

Методи та засоби захисту інформації:

Фізичний захист

Фізичний захист передбачає використання різноманітних заходів для захисту фізичних ресурсів, що містять інформацію. Ці заходи включають:

- **Контроль доступу до приміщень:** Встановлення систем контролю доступу, таких як електронні картки, біометричні системи або кодові замки, щоб обмежити фізичний доступ до приміщень, де знаходиться інформація.
- **Використання систем відеоспостереження:** Встановлення камер відеоспостереження для моніторингу та запису дій, що відбуваються у приміщеннях, що містять інформацію.

- Використання замків та бар'єрів: Застосування фізичних бар'єрів, таких як металеві двері, решітки, сейфи та замки, для запобігання несанкціонованому доступу до об'єктів зберігання інформації.

Логічний захист

Логічний захист передбачає застосування технологій та методів для захисту інформації в цифровому форматі. До методів логічного захисту входять:

- Використання паролів: Встановлення сильних паролів та політик щодо їх використання для обмеження доступу до систем та даних.
- Шифрування даних: Використання шифрування для захисту конфіденційності даних під час їх передачі та зберігання.
- Використання брандмауерів: Встановлення брандмауерів, які контролюють мережевий трафік та фільтрують небезпечні з'єднання.
- Використання антивірусного програмного забезпечення: Встановлення та оновлення антивірусного програмного забезпечення для виявлення та запобігання шкідливим програмам.
- Використання систем виявлення вторгнень: Встановлення систем, які моніторять мережеву активність та виявляють незвичайну або підозрілу поведінку для запобігання вторгнень.

Адміністративний захист

Адміністративний захист передбачає встановлення політик, процедур та стандартів, а також забезпечення належної управлінської практики для забезпечення безпеки інформації. Це включає:

- Встановлення політики безпеки: Розробка та впровадження політики безпеки, яка визначає правила та вимоги щодо захисту інформації.

- Контроль виконання заходів захисту: Моніторинг та перевірка дотримання заходів безпеки, включаючи періодичні аудити безпеки та оцінку ризиків.
- Навчання персоналу: Здійснення навчання та свідомого підходу до безпеки інформації для всього персоналу підприємства.
- Реагування на інциденти: Встановлення процедур реагування на інциденти безпеки, включаючи ідентифікацію, аналіз та відновлення після інцидентів.
- Управління загрозами безпеки: Оцінка ризиків та управління загрозами безпеки для забезпечення ефективного захисту інформації.

Ці методи та засоби захисту інформації використовуються на підприємстві XYZ з метою забезпечення високого рівня безпеки інформації та запобігання несанкціонованому доступу та втраті даних.

Політика захисту інформації на підприємстві:

Підготовка до розробки політики захисту інформації на підприємстві включає оцінку існуючої мережевої інфраструктури та інформаційних систем. Цей етап передбачає детальне вивчення архітектури мережі, ідентифікацію ризиків та вразливостей, аналіз управління доступом, засобів і методів резервного копіювання даних, а також виявлення слабких місць у захисті інформації.

Після розробки політики захисту інформації, важливим етапом є її виконання на підприємстві. Цей процес включає наступні кроки:

- Розповсюдження політики серед працівників: Політика повинна бути офіційно оприлюднена і доступна для всього персоналу

підприємства. Це може бути зроблено шляхом розміщення політики на внутрішньому порталі, висвітлення її на зборах або надання копій працівникам.

- Навчання щодо виконання політики: Працівники повинні отримати достатню підготовку та навчання щодо виконання політики захисту інформації. Це може включати проведення навчальних семінарів, тренінгів або онлайн-курсів, де пояснюються правила та вимоги політики.
- Встановлення механізмів контролю: Для забезпечення відповідності політиці захисту інформації необхідно встановити механізми контролю. Це може включати моніторинг систем безпеки, перевірку дотримання політики, аудити безпеки та інші заходи для виявлення порушень і забезпечення виконання політики.

Ефективна політика захисту інформації є важливим елементом системи захисту інформації на підприємстві. Вона допомагає забезпечити відповідність законодавству, регуляторним вимогам та бізнес-потреbam, а також зменшити ризик витоку інформації та несанкціонованого доступу до даних.

Розділ 2

Аналіз існуючої системи захисту інформації на підприємстві

Опис існуючої системи захисту інформації на підприємстві XYZ

Існує встановлена система захисту інформації, яка має на меті забезпечити безпеку цінної корпоративної інформації. Опис системи захисту включає наступні аспекти:

- **Мережева інфраструктура:** Підприємство XYZ має розгалужену мережу, яка забезпечує зв'язок між всіма відділами та підрозділами. Мережеві пристрої, такі як маршрутизатори та комутатори, належно налаштовані для забезпечення безпеки мережі.
- **Сервери та бази даних:** Підприємство використовує сервери та бази даних для зберігання та обробки інформації. Ці сервери мають належні заходи безпеки, такі як доступ з обмеженими правами, резервне копіювання даних та захист від несанкціонованого доступу.
- **Контроль доступу:** Підприємство використовує систему контролю доступу, що базується на різних рівнях автентифікації та авторизації. Це включає використання паролів, ідентифікаторів, біометричних даних та інших методів для перевірки прав користувачів на доступ до конфіденційної інформації.
- **Шифрування даних:** Для забезпечення конфіденційності та цілісності даних підприємство використовує методи шифрування, такі як симетричне та асиметричне шифрування. Це дозволяє захистити дані від несанкціонованого доступу та забезпечити їх безпеку під час передачі та зберігання.

- Політика безпеки: На підприємстві існує встановлена політика безпеки, яка включає правила та процедури, що регулюють використання системи, доступ до інформації, захист паролів, обмеження фізичного доступу та інші аспекти безпеки інформації.

Описана система захисту інформації є складним інтегрованим підходом, що поєднує технології, процедури та політику безпеки. Це дозволяє забезпечити захист інформації від можливих загроз та зберегти конфіденційність та цілісність даних.

Аналіз виявлених недоліків та проблем існуючої системи захисту інформації

Однією з найважливіших проблем, виявлених під час аналізу, є недостатня освіта та свідомість співробітників підприємства щодо безпеки інформації. Часто співробітники можуть не мати належного розуміння ризиків, пов'язаних з неправильним використанням і обробкою даних, не знати процедур безпеки, які їм потрібно дотримуватись. Для вирішення цієї проблеми варто провести систематичні навчальні курси, тренінги та інформаційні кампанії, спрямовані на підвищення обізнаності співробітників щодо безпеки інформації, правил використання системи та можливих загроз.

Другою проблемою є недостатня реактування на потенційні загрози безпеки. Виявлення загроз та атак може бути обмеженим або відбуватись затримкою, що збільшує ризик компрометації інформації. Для поліпшення цього аспекту варто розглянути впровадження системи моніторингу, яка забезпечуватиме постійний аналіз мережевої активності, виявлення аномалій, вторгнень та інших потенційних загроз. Також варто розглянути

автоматичну систему реагування, яка надасть можливість швидко реагувати на виявлені загрози, блокувати атаки та запобігати подальшому пошкодженню або витоку інформації.

Третьою проблемою є відсутність чітких політик і процедур управління доступом. Відсутність централізованої системи управління доступом та слабкі політики доступу можуть призвести до недостатнього контролю над доступом до різних ресурсів і інформації. Для вирішення цієї проблеми рекомендується впровадження системи управління доступом, яка дозволяє централізовано керувати правами доступу, встановлювати рівні доступу на основі ролей та виконувати аудит доступу для відстеження активності користувачів.

Крім того, було виявлено, що система шифрування та розшифрування даних, яка використовується на підприємстві, потребує оновлення. Шифрування є важливим аспектом захисту інформації, і важливо мати сучасні та надійні алгоритми шифрування. Рекомендується провести огляд та оновлення системи шифрування, використовуючи сучасні алгоритми та методи шифрування, що відповідають найвищим стандартам безпеки.

Враховуючи ці недоліки та можливості для покращення, рекомендується розробити та впровадити план дій з вдосконалення системи захисту інформації на підприємстві XYZ.

Цей план повинен включати в себе необхідні кроки щодо навчання співробітників, впровадження систем моніторингу та реагування на загрози, встановлення системи управління доступом та оновлення системи шифрування. Послідовне виконання цих кроків допоможе підприємству

забезпечити більш високий рівень безпеки та конфіденційності своєї інформації.

Нижче наведено деякі з них:

- Слабкі паролі: Встановлені паролі на різних системах та облікових записах можуть бути недостатньо складними та легко піддаються підлогам. Це створює ризик несанкціонованого доступу до інформації. Рекомендується встановити політику сильних паролів та використовувати двофакторну аутентифікацію для забезпечення більшої безпеки.
- Відсутність регулярних оновлень: Деякі програмні продукти та системи на підприємстві не отримують регулярних оновлень, що може призвести до вразливостей безпеки. Важливо мати механізм оновлення програмного забезпечення та систем, а також використовувати патчі безпеки для заповнення потенційних дір в безпеці.
- Недостатня освіта та свідомість персоналу: Деякі співробітники можуть бути недостатньо ознайомлені з правилами та процедурами безпеки інформації. Це може призводити до ненавмисних порушень безпеки або створювати можливість для соціального інжинірингу. Рекомендується проводити регулярну освіту та навчання персоналу з питань безпеки інформації.
- Недостатня моніторинг та аудит: Відсутність системи моніторингу та аудиту може ускладнити виявлення потенційних загроз та вторгнень в систем
- у. Рекомендується встановити механізми моніторингу, аналізу журналів подій та аудиту активності для вчасного виявлення та реагування на безпекові події.

- Недостатня фізична безпека: Важливо забезпечити адекватний рівень фізичної безпеки на підприємстві, такий як обмежений доступ до серверних приміщень, використання системи контролю доступу та відеоспостереження. Недостатні заходи фізичної безпеки можуть відкрити шлях для фізичного доступу до інформації.

Аналіз виявлених недоліків та проблем існуючої системи захисту інформації дозволяє ідентифікувати області, які потребують подальшого вдосконалення та впровадження заходів для забезпечення вищого рівня безпеки інформації. Це важливий етап дослідження, оскільки виявлені недоліки та проблеми створюють потенційні ризики для безпеки інформації. За допомогою аналізу цих недоліків можна розробити конкретні рекомендації та стратегії для вдосконалення системи захисту інформації.

На основі отриманих результатів аналізу буде можливо встановити пріоритетність вдосконалення окремих аспектів системи захисту інформації. Наприклад, звернення уваги на поліпшення парольної політики та використання двофакторної аутентифікації може зменшити ризик несанкціонованого доступу до системи.

Вдосконалення процедур оновлення програмного забезпечення та систем дозволить заповнити можливі дірки в безпеці та зменшити вразливості. Крім того, впровадження навчальних програм та тренінгів з питань безпеки інформації може підвищити свідомість персоналу та зменшити ризик соціального інжинірингу.

Отримані результати аналізу слугуватимуть основою для розробки рекомендацій з поліпшення системи захисту інформації на підприємстві

XYZ. Ці рекомендації враховуватимуть конкретні потреби та характеристики підприємства з метою забезпечення оптимального рівня безпеки інформації та запобігання можливим загрозам.

Оцінка потенційних загроз безпеці інформації на підприємстві

Оцінка потенційних загроз безпеці інформації є невід'ємною частиною досліджень в галузі безпеки даних. Цей етап включає комплексний аналіз та оцінку різних факторів, які можуть становити загрозу для безпеки інформації в системі.

Першим кроком в оцінці потенційних загроз є ідентифікація можливих джерел загроз. Це можуть бути зовнішні загрози, такі як хакерські атаки, віруси, фішинг або соціальний інжиніринг, а також внутрішні загрози, пов'язані з недоброзичливими діями співробітників, недбале використання ресурсів або крадіжкою даних. Важливо проаналізувати різноманітні сценарії загроз та визначити їх потенційні наслідки для безпеки інформації.

Другим кроком є оцінка ризику, пов'язаного з кожною потенційною загрозою. Це включає аналіз ймовірності виникнення загрози та величини можливого збитку, який може бути завданий в результаті інциденту. Для цього можуть використовуватися різні методи, такі як кількісна аналітика ризику, експертні оцінки, статистичні дані та інші методи оцінки.

Після оцінки ризиків можна розробити стратегії та заходи для управління та зменшення ризиків безпеки інформації. Це можуть бути технічні заходи, такі як встановлення протипожежного брандмауера, шифрування даних, системи виявлення вторгнень, а також організаційні заходи, такі як

політики безпеки, навчання та свідомість персоналу, контроль доступу та інші заходи для забезпечення безпеки інформації.

Оцінка потенційних загроз безпеці інформації є постійним процесом, оскільки технології, загрози та ризики постійно змінюються. Подальші дослідження можуть спрямовуватися на вдосконалення методів оцінки ризиків, розробку нових технологій для виявлення та запобігання загрозам, а також розробку стратегій управління ризиками, що відповідають сучасним викликам та тенденціям в галузі безпеки інформації.

Для проведення оцінки використовуються різноманітні методи та підходи, такі як:

- Аналіз зовнішніх загроз: Включає вивчення потенційних загроз, що можуть походити з зовнішнього середовища, таких як зловмисники, хакери, конкуренти, соціальний інжиніринг тощо. Це дозволяє визначити, які види атак можуть бути спрямовані на підприємство та які можливі наслідки ці атаки можуть мати.
- Аналіз внутрішніх загроз: Включає вивчення можливих загроз безпеці, які можуть походити зсередини самого підприємства, таких як несанкціонований доступ співробітників, недоброчливі дії, виток інформації внаслідок недбалості або недостатньої освіти персоналу. Це допомагає визначити внутрішні слабкі місця та вразливості, які потребують уваги та заходів для запобігання.
- Оцінка ризику: Включає оцінку ймовірності виникнення загрози та визначення потенційних наслідків. Це дозволяє приділити пріоритети тим загрозам, які можуть мати найбільший вплив на безпеку інформації підприємства. Оцінка ризику допомагає

прийняти обґрунтовані рішення стосовно вдосконалення системи захисту інформації.

- Аудит безпеки: Включає перевірку ефективності існуючих заходів захисту, виявлення можливих слабкі місць та вразливостей. Аудит безпеки допомагає оцінити відповідність системи захисту інформації встановленим стандартам та рекомендаціям.

Результати оцінки потенційних загроз безпеці інформації на підприємстві XYZ нададуть важливу інформацію для подальшого розроблення та впровадження стратегій та заходів з покращення системи захисту інформації.

Оцінка потенційних загроз безпеці інформації буде виконуватися за допомогою наступних методів:

1. Аналіз зовнішніх загроз:

- Дослідження потенційних загроз з боку зловмисників, хакерів, конкурентів та інших зовнішніх акторів.
- Виявлення вразливостей, які можуть бути використані для несанкціонованого доступу до інформації.
- Оцінка ризиків, пов'язаних з цими загрозами та визначення потенційних наслідків.

2. Аналіз внутрішніх загроз:

- Вивчення можливих загроз безпеці, що виникають зсередини підприємства, таких як несанкціонований доступ співробітників або виток інформації через людський фактор.
- Виявлення внутрішніх слабких місць та недоліків у політиці безпеки та процесах.

3. Оцінка ризику:

- Визначення ймовірності виникнення загрози та потенційних наслідків, що вона може мати на безпеку інформації.
- Приділення пріоритетів тим загрозам, які можуть мати найбільший вплив на підприємство.

4. Аудит безпеки:

- Перевірка ефективності наявних заходів захисту і виявлення можливих слабких місць та вразливостей.
- Оцінка відповідності системи захисту інформації встановленим стандартам та рекомендаціям.

Ці методи допоможуть отримати повну картину про потенційні загрози безпеці інформації та визначити необхідні заходи для покращення системи захисту інформації. Результати оцінки ризиків будуть використовуватися для розроблення стратегій та планування майбутніх заходів з покращення безпеки інформації.

Визначення критично важливих активів та даних, які потребують особливого захисту

У рамках аналізу існуючої системи захисту інформації на підприємстві XYZ проводиться визначення критично важливих активів та даних, які вимагають особливого рівня захисту. Цей етап дослідження має на меті ідентифікувати активи та дані, які є ключовими для успішного функціонування підприємства, а також можуть бути піддані ризику зловживання, втрати або пошкодження.

Процес визначення критично важливих активів та даних включає наступні кроки:

- **Ідентифікація активів:** Проводиться докладний аналіз всіх видів активів, що знаходяться на підприємстві XYZ. Це можуть бути фінансові ресурси, клієнтська база даних, інтелектуальна власність, конфіденційна інформація, технічне обладнання тощо. Кожен актив ідентифікується та детально описується.
- **Оцінка значущості активів:** Для кожного ідентифікованого активу проводиться оцінка його важливості для підприємства. Важливість може визначатися через такі критерії, як фінансова цінність, стратегічне значення, вплив на конкурентоспроможність, дотримання законодавства, репутація підприємства тощо.
- **Визначення рівня захисту:** На основі значущості активів встановлюється рівень захисту, який відповідає їхньому потенційному ризику. Критично важливі активи і дані, які мають найвищу важливість та піддаються найбільшому ризику, потребують більш високого рівня захисту. Це можуть бути заходи технічного характеру (шифрування даних, біометрична автентифікація), організаційні заходи (політики безпеки, контроль доступу) та процедурні заходи (резервне копіювання, інструкції з безпеки).
- **Розробка стратегій захисту:** На основі визначених критично важливих активів і даних розробляються стратегії захисту, які включають в себе комплекс заходів для забезпечення безпеки цих активів. Це можуть бути технічні заходи, наприклад, встановлення міцних файрволів і систем виявлення вторгнень, організаційні заходи, такі як регулярні огляди політики безпеки та перевірка дотримання процедур, а також навчання персоналу з питань безпеки інформації.

Визначення критично важливих активів та даних є важливим кроком у покращенні системи захисту інформації на підприємстві. Це дозволяє підприємству зосередитися на найбільш цінних елементах та вжити відповідних заходів для їх ефективного захисту, забезпечуючи високий рівень безпеки інформації.

Розробка рекомендацій щодо поліпшення системи захисту інформації

На основі проведеного аналізу існуючої системи захисту інформації та виявлених недоліків і проблем, розробляються рекомендації щодо поліпшення системи захисту інформації. Цей етап є важливим кроком у забезпеченні вищого рівня безпеки інформації та захисту активів підприємства. Рекомендації можуть стосуватися технічних, організаційних та процедурних аспектів системи захисту інформації. Розробка включає такі кроки:

- Впровадження передових технологій: Рекомендації можуть включати в себе впровадження новітніх технологій захисту інформації, таких як продукти кібербезпеки, системи моніторингу та виявлення вторгнень, шифрування даних тощо. Це допоможе підвищити ефективність захисту інформації та зменшити ризик зловживання.
- Створення політик і процедур: Рекомендації можуть включати розробку політик та процедур безпеки інформації. Це включає в себе створення правил доступу до інформації, регулярне оновлення паролів, контроль доступу до приміщень та комп'ютерних систем, навчання персоналу з питань безпеки інформації тощо. Ці політики та процедури допоможуть створити культуру безпеки інформації на підприємстві.

- Підвищення освітнього рівня персоналу: Рекомендації можуть включати організацію навчальних програм та тренінгів з питань безпеки інформації для персоналу підприємства XYZ. Це допоможе зрозуміти загрози та ризики, пов'язані з інформаційною безпекою, і навчити персонал ефективно застосовувати заходи захисту інформації у своїй роботі.
- Регулярні аудити та оцінка ефективності: Рекомендації можуть включати проведення регулярних аудитів системи захисту інформації та оцінку її ефективності. Це дозволить виявляти слабкі місця, коригувати заходи безпеки та забезпечувати постійне покращення системи захисту інформації.

Розробка рекомендацій щодо поліпшення системи захисту інформації на підприємстві є важливим етапом у процесі забезпечення безпеки інформації та захисту активів підприємства. Ці рекомендації спрямовані на вдосконалення технічних, організаційних та процедурних аспектів системи захисту, забезпечуючи більш ефективний та надійний захист інформації в сучасному інформаційному середовищі.

Розділ 3

Розробка проекту захисту інформації на підприємстві

Визначення вимог до системи захисту інформації

Процес встановлення вимог до системи захисту інформації на підприємстві є критичним етапом, оскільки він визначає основні принципи та цілі, які мають бути досягнуті для забезпечення високого рівня безпеки даних. Цей етап вимагає глибокого аналізу потреб організації, враховуючи

її специфіку, розмір, галузь діяльності та особливості інформаційних ресурсів.

Перший крок у встановленні вимог - це докладний аналіз потенційних загроз, ризиків та вразливостей, з якими може стикнутися підприємство. Це може включати зовнішні загрози, такі як хакерські атаки, соціальний інжиніринг, фішинг, а також внутрішні загрози, пов'язані з недоброзичливими діями співробітників або недбалим використанням ресурсів.

Далі, проводиться детальний аналіз потреб організації з точки зору безпеки інформації. Це охоплює виявлення критичних активів, конфіденційності, цілісності та доступності даних, а також вимог щодо їх зберігання, обробки та передачі. Також враховуються правові та регуляторні вимоги, що стосуються безпеки даних, зокрема в галузі захисту персональних даних, фінансової звітності та інших аспектів.

На цьому етапі також проводяться консультації з експертами з безпеки, які допомагають оцінити потреби та ризики організації. Вони можуть рекомендувати оптимальні заходи, процедури та технології для забезпечення безпеки інформації, враховуючи бюджетні обмеження та ефективність впровадження.

Після аналізу, консультацій та узгодження з усіма зацікавленими сторонами, формулюються конкретні вимоги до системи захисту інформації. Ці вимоги визначають набір заходів, процедур і технологій, необхідних для забезпечення конфіденційності, цілісності та доступності даних. Вони можуть включати вимоги до аутентифікації користувачів, контролю доступу, шифрування даних, журналювання подій, резервного

копіювання та відновлення, а також навчання персоналу щодо безпеки інформації.

Встановлення вимог до системи захисту інформації вимагає уважного підходу та комплексного аналізу, щоб забезпечити ефективний та надійний захист даних підприємства. Це важливий крок у процесі розробки безпечної інформаційної системи, яка допомагає забезпечити конфіденційність, цілісність та доступність важливої інформації.

Для забезпечення надійного захисту інформації на підприємстві, будуть визначені оптимальні процедури та технології. Перш за все, важливо встановити механізми ідентифікації, аутентифікації та авторизації користувачів. Це забезпечить контроль доступу до інформаційних ресурсів та унеможливить несанкціонований доступ до конфіденційної інформації.

Крім того, впровадження шифрування є ключовим елементом захисту інформації. Використання сучасних криптографічних алгоритмів та методів шифрування дозволить забезпечити конфіденційність даних під час їх передачі та зберігання. Шифрування забезпечує захист інформації від несанкціонованого доступу, навіть якщо дані потраплять у недоброчесні руки.

Для ефективного моніторингу та виявлення потенційних загроз безпеки, на підприємстві будуть впроваджені системи моніторингу і аналізу інформаційних ресурсів. Ці системи дозволять вчасно виявляти незвичну або підозрілу активність, а також реагувати на потенційні загрози безпеки. Вони забезпечать постійний контроль за інформаційними потоками та швидку реакцію на можливі інциденти.

Аналіз та визначення вимог щодо процедур та технологій захисту інформації дозволить підприємству побудувати комплексну систему безпеки, що відповідає найвищим стандартам. Враховуючи специфіку підприємства та його інформаційних потреб, будуть впроваджені оптимальні заходи забезпечення безпеки, що гарантують захист цінної інформації та запобігають можливим загрозам.

Для визначення вимог до системи захисту інформації, потрібно врахувати наступні аспекти:

- **Класифікація даних:** Визначення рівнів конфіденційності та важливості різних типів даних. Це допоможе встановити пріоритети та визначити необхідні рівні захисту для кожного типу даних.
- **Ідентифікація загроз:** Аналіз потенційних загроз безпеці інформації, таких як несанкціонований доступ, крадіжка даних, атаки зловмисників і т.д. Визначення загроз дозволяє встановити, які заходи захисту потрібно впровадити для їх запобігання або пом'якшення наслідків.
- **Аналіз потенційних вразливостей:** Виявлення слабких місць в існуючій системі захисту інформації, які можуть стати джерелом загроз. Це можуть бути технічні, організаційні або процедурні вразливості, які необхідно врахувати при розробці поліпшеної системи захисту.
- **Законодавчі вимоги:** Врахування вимог, що стосуються захисту інформації, які встановлені законодавством або регуляторними органами. Наприклад, це можуть бути вимоги щодо збереження персональних даних, вимоги щодо забезпечення конфіденційності важливих даних тощо.
- **Бізнес-потреби:** Врахування потреб бізнесу та вимог, що стосуються доступу до інформації. Наприклад, встановлення правил доступу до

даних для забезпечення ефективності бізнес-процесів та недопущення перешкод у роботі співробітників.

В результаті визначення вимог до системи захисту інформації, будуть сформульовані чіткі та конкретні вимоги, які будуть використовуватись під час розробки та впровадження поліпшеної системи захисту інформації на підприємстві XYZ.

Вибір методів та засобів захисту інформації

В рамках розробки системи захисту інформації були вибрані певні методи та засоби для забезпечення безпеки даних. Основні методи та засоби, що були використані, включають:

1. Аутентифікація користувачів:

- Використання хеш-функцій для зберігання та порівняння хешів паролів.

- Додатковий сіль (salt) для ускладнення процесу зламу паролів.

2. Контроль доступу:

- Визначення ролей користувачів та обмежень доступу на основі ролей.

- Перевірка доступу до ресурсів на основі ролей користувачів.

3. Журналювання подій:

- Запис подій у журнал для аналізу та виявлення вразливостей або несанкціонованої діяльності.

4. Шифрування даних:

- Застосування алгоритмів шифрування для забезпечення конфіденційності даних.

- Захист даних під час їх передачі та зберігання.

5. Використання логічних та фізичних засобів захисту:

- Встановлення фізичних бар'єрів та контроль доступу до приміщень, де знаходиться інформація.

- Використання брандмауерів, антивірусного програмного забезпечення та інших засобів для захисту мережі та системи.

Зазначені методи та засоби є ефективними для захисту інформації. Однак, варто враховувати, що безпека інформації - постійний процес, і рекомендується постійно оновлювати та аналізувати використовувані методи та засоби, враховуючи нові загрози та ризики.

Розробка архітектури системи захисту інформації.

При розробці архітектури системи захисту інформації можуть бути враховані наступні аспекти:

- Ідентифікація захисних шарів: Розподіл системи захисту інформації на рівні або шари, що включають фізичний, мережевий, системний та захист даних. Кожен шар має свої функції та заходи захисту, які співпрацюють для забезпечення загальної безпеки інформації.
- Вибір технологій та інструментів: Визначення технологій, програмного забезпечення та інструментів, які будуть використовуватись для реалізації архітектури системи захисту. Це можуть бути файрволи, антивіруси, системи контролю доступу, шифрування даних та інші засоби захисту.

- **Управління доступом:** Розробка політик та механізмів для контролю та управління доступом до інформації на різних рівнях. Це включає встановлення ролей та прав доступу, аутентифікацію та авторизацію користувачів, аудит доступу та інші механізми контролю доступу.
- **Захист даних:** Розробка стратегій та механізмів для захисту конфіденційності, цілісності та доступності даних. Це можуть бути шифрування даних, резервне копіювання, контроль цілісності даних та інші методи захисту.
- **Моніторинг та виявлення інцидентів:** Розробка системи моніторингу, яка дозволяє відстежувати події та виявляти можливі інциденти безпеки. Це може включати системи журналювання подій, системи виявлення вторгнень та інші інструменти моніторингу.
- **Навчання та свідомість персоналу:** Розробка програми навчання та підвищення свідомості персоналу щодо важливості захисту інформації та правил безпеки. Це можуть бути тренінги, посібники, інструкції та інші освітні матеріали.

Після розробки архітектури системи захисту інформації, будуть визначені основні компоненти та засоби захисту, які будуть використовуватись для забезпечення безпеки інформації. Це стане основою для подальшої реалізації та впровадження системи захисту інформації на підприємстві.

Розробка процедур та правил використання системи захисту інформації

Розробка процедур та правил використання системи захисту інформації є важливою складовою частиною впровадження поліпшеної системи захисту інформації на підприємстві. Цей етап передбачає докладну

розробку і документування інструкцій та рекомендацій, що охоплюють всі аспекти використання системи, з метою забезпечення її ефективності та надійності. Процедури використання системи захисту інформації включають розгортання та налаштування системи, доступ до інформації, зміну налаштувань, виконання резервного копіювання, встановлення оновлень та усунення неполадок. Кожна процедура повинна бути описана докладно, зазначаючи послідовність кроків, параметри і налаштування, необхідні для коректної роботи системи.

Важливо також включити рекомендації щодо часто виникаючих ситуацій, помилок та способів їх вирішення. Правила використання системи захисту інформації встановлюють набір обов'язкових вимог, які повинні дотримуватись всіма користувачами системи. Ці правила можуть включати вимогу до складності паролів, обмеження доступу до конфіденційної інформації лише для авторизованих осіб, заборону використання несанкціонованих програм або пристроїв, вимогу щодо регулярного змінювання паролів, обов'язкову двофакторну аутентифікацію та збереження конфіденційності, цілісності та доступності інформації.

При розробці процедур та правил використання системи захисту інформації необхідно враховувати специфіку підприємства XYZ, його потреби у захисті інформації та вимоги щодо дотримання внутрішніх та зовнішніх стандартів безпеки даних. Крім того, слід звернути увагу на законодавчі та регуляторні вимоги, що стосуються конкретної сфери діяльності підприємства, наприклад, GDPR (Загальний регламент про захист персональних даних) або інших регулятивних положень, які стосуються захисту конфіденційної інформації. Крім того, важливим аспектом розробки процедур та правил є організація навчання і

підвищення свідомості користувачів щодо правильного використання системи захисту інформації. Це може включати проведення навчальних семінарів, тренінгів, підготовку інформаційних матеріалів та документації, щоб забезпечити зрозуміле і відповідне використання системи всіма співробітниками.

Остаточні процедури та правила повинні бути документовані і доступні всім зацікавленим сторонам, зокрема співробітникам, керівництву та внутрішнім аудиторам. Вони повинні підлягати періодичному огляду та оновленню з урахуванням змін у технологічному оточенні, вимог безпеки та досвіду з використання системи

Загальний успіх системи захисту інформації, значно залежить від ефективної розробки процедур та правил використання, їх впровадження та підтримки на всіх рівнях організації. Це забезпечить зменшення ризиків, збільшення надійності та захищеності інформації, а також забезпечить довіру співробітників та клієнтів в ефективність застосованої системи захисту.

Розділ 4

Реалізація проекту захисту інформації на підприємстві

Опис структури та функцій системи захисту інформації:

Система захисту інформації на підприємстві складається з різних компонентів, модулів та їх взаємозв'язків, які спільно працюють для забезпечення безпеки інформації. Вона включає апаратні засоби,

програмне забезпечення та людський фактор, які допомагають уникнути загроз і зберегти конфіденційність, цілісність та доступність інформації.

Апаратні засоби є важливою складовою частиною системи захисту інформації на підприємстві XYZ. Вони забезпечують необхідну інфраструктуру для ефективного функціонування заходів безпеки. Сервери є основою для зберігання та обробки даних, забезпечуючи надійність та доступність інформації.

Мережеві пристрої, такі як мережеві фаєрволи, відіграють важливу роль у контролі та фільтрації мережевого трафіку. Вони дозволяють встановлювати правила доступу, блокувати небажані з'єднання та забезпечувати безпеку мережі.

Додатково, інтрузійні системи виявлення та системи моніторингу мережі використовуються для виявлення потенційно шкідливої активності та незвичних подій в мережі. Вони надають реальний аналіз та сповіщення про можливі загрози, що допомагає оперативно реагувати на потенційні інциденти та забезпечувати безпеку мережевих ресурсів.

Важливо враховувати, що вибір і конфігурація апаратних засобів повинні відповідати конкретним потребам підприємства та бути вирішеними в контексті загальної стратегії захисту інформації. Комплексне поєднання апаратних та програмних засобів допоможе створити надійну та ефективну систему захисту інформації.

Програмне забезпечення включає різні інструменти та програми, які використовуються для захисту інформації. Це можуть бути антивірусні програми, програми шифрування, системи ідентифікації та автентифікації,

програми моніторингу та аудиту, а також програми для керування доступом та резервного копіювання.

Людський фактор є невід'ємною частиною системи захисту інформації. Включає навчання працівників щодо правил безпеки і використання системи захисту, встановлення ролей та відповідальності, а також організацію процедур та політики безпеки на рівні підприємства.

Опис процедур та правил використання системи захисту інформації:

Використання системи захисту інформації, базується на встановлених процедурах та правилах, які забезпечують безпеку інформації та ефективне функціонування системи. Нижче наведені деякі з них:

- Автентифікація та авторизація: Кожен користувач системи повинен пройти процедуру автентифікації, щоб підтвердити свою ідентичність. Після цього система призначає права доступу, враховуючи ролі та обов'язки користувача. Користувачі повинні дотримуватися правил використання своїх облікових записів та не розголошувати свої облікові дані третім особам.
- Захист паролів: Користувачі повинні використовувати міцні паролі, які важко вгадати, і регулярно їх змінювати. Також можуть встановлюватися вимоги щодо довжини паролів та використання різних типів символів.
- Класифікація та маркування інформації: Інформація повинна бути класифікована відповідно до її важливості та чутливості. Класифікація може включати рівні, такі як "секретна", "конфіденційна" або "загальнодоступна". Правила маркування допомагають користувачам розпізнавати інформацію та встановлювати необхідні обмеження доступу.

- **Захист від зловмисних програм:** Користувачам слід уникати відкривання ненадійних поштових вкладень та завантаження програм з невідомих джерел. Антивірусне програмне забезпечення повинно бути встановлено на всіх комп'ютерах та регулярно оновлюватися.

Оцінка ефективності проекту захисту інформації на підприємстві:

Оцінка ефективності проекту захисту інформації на підприємстві вимагає проведення регулярних аудитів та оцінок, які дозволяють оцінити стан безпеки і знайти шляхи для покращення. Для досягнення цієї мети використовуються різні засоби та методи, які спрямовані на перевірку відповідності, виявлення загроз, оцінку ефективності контролів та підвищення свідомості та навчання працівників.

Першим інструментом є перевірка відповідності системи захисту інформації підприємства встановленим нормативним вимогам та стандартам безпеки, таким як ISO 27001. Це включає аналіз наявних політик, процедур та технологій, щоб виявити потенційні недоліки та пропозиції щодо покращення системи.

Другий інструмент - виявлення загроз - включає аналіз потенційних загроз безпеці інформації на підприємстві. Це може включати використання пенетраційних тестів, щоб перевірити систему на наявність слабких місць, а також використання систем виявлення і запобігання інтрузіям для виявлення недоброзичливої активності.

Третій інструмент - оцінка ефективності контролів - дозволяє оцінити, наскільки добре встановлені контролі безпеки функціонують. Це включає оцінку механізмів контролю доступу, шифрування, резервного копіювання та інших заходів, що спрямовані на забезпечення безпеки інформації. За допомогою цього інструменту можна виявити прогалини та рекомендації щодо подальшого удосконалення системи захисту.

Четвертий інструмент - свідомість та навчання - орієнтований на підвищення рівня знань та усвідомленості працівників щодо правил безпеки, використання системи захисту та виявлення потенційних загроз. Це можуть бути навчальні заходи, тренінги або інформаційні матеріали, що допомагають працівникам бути більш пильними та реагувати на потенційні проблеми безпеки.

Усі результати оцінок та аудитів використовуються для вдосконалення системи захисту інформації на підприємстві XYZ. Регулярні перевірки та оновлення системи є важливим етапом для забезпечення найвищого рівня безпеки та відповідності нормативним вимогам у сфері захисту інформації.

Висновки

У ході реалізації проекту захисту інформації на підприємстві були проведені різні дії для забезпечення безпеки та конфіденційності інформації. Було розроблено систему захисту інформації, яка включає в себе структуру та функції. Були визначені процедури та правила використання системи захисту інформації. Також була проведена оцінка ефективності проекту захисту інформації на підприємстві.

За результатами реалізації проекту було виявлено, що система захисту інформації на підприємстві, виконує свої функції і допомагає забезпечити безпеку і конфіденційність важливих даних. Проте, під час аналізу були виявлені деякі недоліки та можливості для покращення системи.

Одним з недоліків, виявлених під час аналізу, є використання статичного солі для хешування паролів в класі `User`. Статична сіль означає, що всі паролі будуть хешуватись з використанням однакової солі, що може зробити систему більш вразливою до атак зламу хешу паролів.

Рекомендовано використовувати унікальну сіль для кожного користувача або використовувати алгоритми хешування з вбудованою сіллю, які забезпечують додатковий рівень безпеки.

Крім того, було виявлено, що система контролю доступу в класі `AccessControlModule` має обмежену функціональність. Наразі вона базується на приналежності користувача до ролей для надання доступу до ресурсів. Однак, для більш гнучкого управління доступом можна розглянути використання додаткових механізмів, таких як динамічні права доступу, контроль доступу на основі атрибутів, політики безпеки тощо. Це

дозволить більш точно визначати, які користувачі мають доступ до яких ресурсів та які дії вони можуть виконувати.

Для покращення безпеки системи також можна розглянути впровадження додаткових заходів безпеки, таких як механізми двофакторної аутентифікації, обмеження спроб авторизації, моніторинг та виявлення аномалій, шифрування збереження паролів та конфіденційних даних, резервне копіювання тощо.

Крім того, можна розширити функціональність системи, додавши можливості аудиту безпеки, виявлення та реагування на загрози, моніторинг доступу та подій, аналіз журналів тощо. Це допоможе вчасно виявляти потенційні загрози та забезпечити відповідне реагування на них.

Наслідком вдосконалення системи захисту інформації буде забезпечення більш високого рівня безпеки, конфіденційності та доступності важливих даних на підприємстві.

Рекомендації щодо покращення системи захисту інформації на підприємстві

- Провести аудит системи захисту інформації з метою виявлення потенційних слабких місць і вразливостей. Застосувати найновіші методи тестування на проникнення для оцінки стійкості системи до атак.
- Розширити функціональність системи захисту інформації, включаючи додаткові можливості шифрування, контролю доступу та виявлення вторгнень.

- Постійно оновлювати програмне забезпечення системи захисту інформації, включаючи встановлення патчів та оновлення безпекових апаратних засобів.
- Забезпечити регулярне навчання та свідомість персоналу щодо безпеки інформації, включаючи навчання процедурам безпеки, обізнаність щодо соціального інжинірингу та методів атак.

Можливості подальших досліджень

Можливості подальших досліджень у галузі безпеки інформації включають широкий спектр напрямків, спрямованих на поліпшення та розширення заходів захисту даних. Деякі з цих можливостей включають:

1. Дослідження нових методів шифрування і розшифрування даних:
Запровадження нових алгоритмів шифрування може сприяти забезпеченню вищого рівня конфіденційності даних. Дослідники можуть вивчати нові криптографічні протоколи, ключові обміни та методи шифрування, що дозволяють покращити безпеку передачі та зберігання інформації.
2. Вивчення нових методів виявлення і реагування на вторгнення:
Розвиток нових методів виявлення вторгнень та інтелігентних систем реагування може покращити ефективність контролю безпеки системи. Дослідники можуть вивчати методи аналізу журналів подій, використання машинного навчання та штучного інтелекту для раннього виявлення та усунення потенційних загроз.
3. Використання штучного інтелекту та машинного навчання:
Дослідження можливостей застосування штучного інтелекту та

машинного навчання для виявлення аномалій та атак в реальному часі може сприяти покращенню безпеки системи. Розробка інтелектуальних систем, здатних самостійно виявляти та аналізувати незвичайні зразки поведінки, може допомогти вчасно реагувати на потенційні загрози та запобігти вторгненням.

4. Використання блокчейн-технологій: Вивчення можливостей використання блокчейн-технологій може допомогти забезпечити недерегульоване

та незмінне зберігання інформації. Блокчейн-технологія може забезпечити надійну систему зберігання даних, де кожен блок інформації має характеристику невідомості та відстежуваності, що сприяє забезпеченню цілісності та достовірності інформації.

Ці можливості досліджень в галузі безпеки інформації відкривають шлях до подальшого розвитку і вдосконалення систем захисту даних.

Результати досліджень можуть мати значний вплив на підвищення безпеки інформації, забезпечення конфіденційності та захисту важливих даних в сучасному цифровому світі.

Список використаної літератури:

Нормативно-правова база:

- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (№ 2297-VI від 01.06.2010).
- Закон України "Про захист персональних даних" (№ 2297-VI від 01.06.2010).
- Національний стандарт України "Захист інформації. Основні терміни та визначення" (ДСТУ 3966:2019).

Вітчизняні та зарубіжні джерела та публікації:

- М. Е. Клімов, С. А. Мартинов, О. В. Єлагін. "Інформаційна безпека підприємства: організація, методи та засоби захисту." - Київ: НІСД, 2018.
- W. Stallings. "Cryptography and Network Security: Principles and Practice." - Pearson, 2017.
- B. Schneier. "Applied Cryptography: Protocols, Algorithms, and Source Code in C." - Wiley, 1995.
- National Institute of Standards and Technology (NIST) Special Publications щодо інформаційної безпеки, включаючи серію SP 800.

Зазначені джерела та публікації були використані для отримання теоретичної та практичної інформації щодо захисту інформації та визначення нормативно-правової бази в сфері інформаційної безпеки. Дані джерела є авторитетними та надійними джерелами інформації з даної області.

Додатки

Код програмного забезпечення системи захисту інформації

```
1 > import hashlib
2 import logging
3
4
5 1 usage
6 > class User:
7 >     def __init__(self, username, password):
8         self.username = username
9         self.password_hash = self._hash_password(password)
10        self.role = 'user'
11
12 2 usages
13 > def _hash_password(self, password):
14     salt = 'somerandomsalt'
15     hash_object = hashlib.sha256((password + salt).encode())
16     return hash_object.hexdigest()
17
18 1 usage (1 dynamic)
19 > def check_password(self, password):
20     return self.password_hash == self._hash_password(password)
21
22 # Реалізація розшифрування даних
23 1 usage
24 > class AuthenticationModule:
25 >     def __init__(self):
26         self.users = {}
27
28 2 usages
29 > def create_user(self, username, password):
30     # Перевірка, чи користувач з таким ім'ям вже існує
31     if username in self.users:
32         logging.warning("Користувач з таким ім'ям вже існує.")
33         return
34
35     user = User(username, password)
36     self.users[username] = user
37     logging.info("Користувача створено успішно.")
38
39     def login(self, username, password):
40         # Перевірка, чи існує користувач з вказаним ім'ям
41         if username not in self.users:
42             logging.warning("Невірне ім'я користувача.")
43             return False
44
45         user = self.users[username]
46         if user.check_password(password):
47             logging.info("Успішний вхід.")
48             return True
49         else:
50             logging.warning("Невірний пароль.")
51             return False
52
53 1 usage
54 > class AccessControlModule:
55 >     def __init__(self):
56         self.roles = {}
57         self.resources = {}
58
59 1 usage
60 > def add_role(self, role):
61     self.roles[role] = set()
62
63 1 usage
64 > def add_user_to_role(self, username, role):
65     # Перевірка, чи існує роль
66     if role not in self.roles:
```

```

61     logging.warning("Роль не існує.")
62     return
63
64     self.roles[role].add(username)
65     logging.info("Користувачу додано роль.")
66
67     1 usage
68     def grant_access(self, username, resource):
69         # Перевірка, чи існує ресурс
70         if resource not in self.resources:
71             self.resources[resource] = set()
72
73         for role, users in self.roles.items():
74             if username in users:
75                 self.resources[resource].add(username)
76                 logging.info("Доступ надано.")
77                 return
78
79         logging.warning("Користувачу не надано доступ.")
80
81     2 usages
82     def check_access(self, username, resource):
83         if resource in self.resources and username in self.resources[resource]:
84             logging.info("Користувач має доступ до ресурсу.")
85         else:
86             logging.warning("Користувач не має доступу до ресурсу.")
87
88     1 usage
89     class LoggingModule:
90         def __init__(self):
91             logging.basicConfig(filename='log.txt', level=logging.INFO)
92
93     2 usages
94     def log_event(self, event):
95         logging.info(event)
96
97     1 usage
98     class EncryptionModule:
99         def encrypt(self, data):
100             encrypted_data = data # Потрібно замінити на реальний код шифрування
101             return encrypted_data
102
103     1 usage
104     def decrypt(self, encrypted_data):
105             data = encrypted_data # Потрібно замінити на реальний код розшифрування
106             return data
107
108     auth_module = AuthenticationModule()
109     access_module = AccessControlModule()
110     logging_module = LoggingModule()
111     encryption_module = EncryptionModule()
112
113     # Створення користувачів і надання доступу
114     auth_module.create_user("user1", "password1")
115     auth_module.create_user("user2", "password2")
116
117     access_module.add_role("admin")
118     access_module.add_user_to_role("user1", "admin")
119     access_module.grant_access("user1", "important_file.txt")
120     access_module.check_access("user1", "important_file.txt")
121     access_module.check_access("user2", "important_file.txt")

```

```

120 # Журналювання подій
121 logging_module.log_event("Успішний вхід користувача user1")
122 logging_module.log_event("Невдала спроба доступу до important_file.txt")
123
124 # Шифрування та розшифрування даних
125 encrypted_data = encryption_module.encrypt("Конфіденційна інформація")
126 decrypted_data = encryption_module.decrypt(encrypted_data)
127
128 print(decrypted_data)

```

Цей код використовується для реалізації системи захисту інформації на підприємстві XYZ. Він містить класи для аутентифікації користувачів, контролю доступу, журналювання подій та шифрування даних. Код демонструє функціональність системи та взаємодію цих модулів для забезпечення безпеки і конфіденційності інформації.

Його можна розглянути детальніше:

- Клас `User` відповідає за представлення користувача системи. У конструкторі створюється об'єкт користувача з вказаним ім'ям користувача та захешованим паролем. Метод `_hash_password` використовує алгоритм хешування SHA-256 для створення хешу пароля.
- Клас `AuthenticationModule` відповідає за реєстрацію користувачів та перевірку їх ідентифікації. У методі `create_user` створюється новий користувач з вказаним ім'ям та паролем. Хеш пароля зберігається в словнику `users`. Метод `login` перевіряє, чи існує користувач з вказаним ім'ям, та перевіряє правильність пароля шляхом порівняння хешів.
- Клас `AccessControlModule` відповідає за управління доступом користувачів до ресурсів. Він містить словники `roles` та `resources`, де зберігаються ролі та ресурси відповідно. Методи `add_role` та `add_user_to_role` додають ролі та призначають їх користувачам. Метод `grant_access` надає користувачеві доступ до вказаного ресурсу, якщо він має відповідну роль. Метод `check_access` перевіряє, чи має користувач доступ до вказаного ресурсу.

- Клас `LoggingModule` відповідає за журналювання подій. В конструкторі він ініціалізує об'єкт журналування з вказаним рівнем логування та файлом журналу. Метод `log_event` записує подію в журнал з рівнем INFO.

- Клас `EncryptionModule` відповідає за шифрування та розшифрування даних. Методи `encrypt` та

- `decrypt` наразі просто повертають вхідні дані без змін, але їх можна замінити реальним кодом шифрування та розшифрування.

- Далі в коді створюються об'єкти модулів (`auth_module`, `access_module`, `logging_module`, `encryption_module`) та виконуються деякі дії:

- Створюються користувачі "user1" та "user2" з відповідними паролями за допомогою `auth_module.create_user`.

- Додається роль "admin" за допомогою `access_module.add_role`.

- Користувачу "user1" надається роль "admin" за допомогою `access_module.add_user_to_role`.

- Користувачу "user1" надається доступ до ресурсу "important_file.txt" за допомогою `access_module.grant_access`.

- Перевіряється доступ користувача "user1" до ресурсів "important_file.txt" та "important_file.txt" для користувача "user2" за допомогою `access_module.check_access`.

- Записуються події в журнал за допомогою `logging_module.log_event`.

- Виконується шифрування та розшифрування даних за допомогою `encryption_module.encrypt` та `encryption_module.decrypt`.

На виводі виводиться розшифровані дані, які наразі є тими ж самими, що й вхідні дані.

Весь код реалізує базові функціональні можливості для аутентифікації, контролю доступу, журналювання та шифрування, але для використання в реальних системах потрібно ретельно перевірити та оптимізувати його, а також додати необхідні заходи безпеки та захисту даних.