

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

ВПРОВАДЖЕННЯ СТАНДАРТУ ISO27001 НА ПІДПРИЄМСТВІ

Виконав: студент групи ПМК-41с

Спеціальності 125 "Кібербезпеки"

(шифр і назва спеціальності)

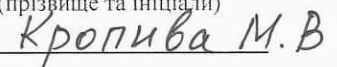
Керівник



(підпис)

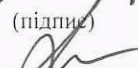
Шах А.А

(прізвище та ініціали)

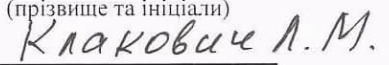


(прізвище та ініціали)

Рецензен

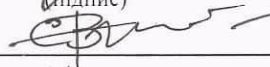


(підпис)

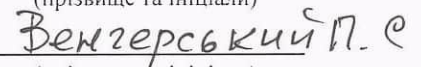


(прізвище та ініціали)

Науковий консультант



(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

ЗАВДАННЯ

НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

ШАХ АНДРІЙ АНДРІЙОВИЧ
(прізвище, ім'я, по батькові)

1. Тема роботи: ВПРОВАДЖЕННЯ СТАНДАРТУ ISO27001 НА ПІДПРИЄМСТВІ

Керівник роботи Кропива Михайло Вікторович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

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

2. Строк подання студентом роботи **13.06.2023р.**

3. Вихідні дані до роботи: Аналіз стратегії компанії та її потреб у захисті інформації,

Вимоги та кроки які потрібно виконати для сертифікування компанії стандартом

ISO 27001

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

Розгляд стандарту ISO 27001 та його значення для підприємства

Обов'язкові вимоги для отримання сертифікації

Оцінка ризиків (Risk Assessment Policy)

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Презентація та доповідь виконані в Microsoft Power Point

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 31 серпня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів дипломної роботи	Термін виконання	Примітки
1	Постановка завдання	15.09.2022	
2	Аналіз літератури та інших джерел.	12.10.2022	
3	Збір інформації	15.11.2022	
4	Ознайомлення з структурою написання	06.12.2022	
5	Написання неоретичних відомостей	25.01.2023	
6	Вивчення та аналіз структури ISO 27001	18.02.2023	
7	Структура оцінки ризиків	28.03.2023	
9	Оформлення презентації	03.04.2023	
10	Отримання рецензій	09.05.2023	
11	Подання роботи на кафедру	12.06.2023	
12	Захист в ЕК	15.06.2023	

Студент



(підпис)

Шах А.А.

(ініціали, прізвище)

Керівник роботи



(підпис)

Кропива М.В.

(ініціали, прізвище)

Науковий консультант


(підпис)

Венгерський
(ініціали, прізвище)

РЕФЕРАТ

Цей дипломний проект прямує свої зусилля на вивчення складнощів створення системи контролю за інформаційною безпекою в структурі організації. Проект охоплює широкий спектр елементів, включаючи умовні знаки та скорочення, вступ, три глави, висновки та перелік джерел, з яких було зроблено вибірку.

Область дослідження присвячена забезпеченню інформаційної безпеки підприємства. Основна ціль проекту - це створення пропозицій для поліпшення процесів розробки та впровадження системи управління ISMS, виконання аналізу досвіду впровадження таких систем та розробка відповідних рекомендацій.

У процесі роботи було здійснено аналіз основних методик створення системи контролю інформаційної безпеки; було досліджено специфіку систем контролю інформаційної безпеки на підприємствах; було проведено огляд стандартів створення систем управління інформаційною безпекою на підприємствах.

Сфера застосування: Розроблені методи можуть бути корисними при плануванні та виконанні системи контролю інформаційної безпеки на підприємстві.

Ключові терміни: інформаційна безпека, управління інформаційною безпекою, система управління інформаційною безпекою.

ЗМІСТ

ВСТУП	6
РОЗДІЛ 1. СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ	9
1.1. Розгляд стандарту ISO27001 та його значення для підприємств	9
1.1.1. Управління ризиками	11
1.2. Переваги сертифікації згідно ISO27001	14
1.2.1. Покращення репутації підприємства	15
1.2.2. Забезпечення відповідності законодавству	17
1.3. Структура стандарту ISO27001	18
1.4. Обов'язкові вимоги для отримання сертифікації	21
1.5. Risk Assessment	24
РОЗДІЛ 2. ПРАКТИЧНА ЧАСТИНА	28
2.1. Оцінка ризиків (Risk Assessment Policy)	28
2.2. Політика управління доступом (Change Management Policy)	34
2.3. Політика управління доступом (Access Management Policy)	37
2.4. Політика щодо тренінгів з інформаційної безпеки (Security Awareness Policy)	39
2.5. Політика інформаційної безпеки	41
2.6. Політика Access Management Policy	46
ВИСНОВОК	49
Рекомендації	51
Список використаних джерел	53

ВСТУП

Актуальність теми: Останнім часом стало очевидним певне упередження. Коли люди говорять про інформаційну безпеку, вони переважно мають на увазі захист від вірусів та хакерів. Однак, коли експертів з безпеки запитують, що їх найбільше турбує, вони відповідають, що їх найбільше турбує поведінка інсайдерів. Дослідження показують, що необережні та незаконні дії співробітників можуть завдати в кілька разів більше шкоди, ніж шкода, завдана, наприклад, вірусами.

"Хакерські" атаки. А кількість інцидентів, спричинених зовнішніми та внутрішніми порушниками спокою, непорівнянна.

У внутрішнього зловмисника може бути більше мотивів, особливо якщо його дії навмисні, а не помилкові: від банальної образи до матеріальної вигоди, коли його перекупує конкурент. І можливостей більше. Він або вона вже є легітимним користувачем мережі, має доступ до конфіденційних ресурсів організації і може законно використовувати додатки компанії та дані в них [13, с.130-135].

Саме тому завдання створення системи управління інформаційною безпекою для регулювання інформаційних потоків всередині організації та контролю над цілісністю, конфіденційністю і доступністю інформації має великий сенс.

Сьогодні світ знаходиться в процесі переходу до постіндустріального суспільства. З точки зору налагодження бізнес-процесів також відбувається перехід від орієнтації на постачальника до орієнтації на споживача. Це означає, що компаніям потрібно швидко змінювати напрямок, щоб адаптуватися до вимог ринку. Як наслідок, зараз вони активно розглядають бізнес-процеси, які використовують цифрові інформаційні інструменти, такі як електронний документообіг та використання комп'ютерного

програмного забезпечення. На цьому тлі компанії все частіше оперують великими обсягами даних переважно в електронному форматі. Підприємства стурбовані підтримкою безперервної роботи бізнес-процесів та захистом інформації, яка гарантує здійснення бізнес-операцій. Як наслідок, компанії витрачають гроші і час на побудову і захист своїх інформаційних інфраструктур. Метою інформаційної безпеки є захист критично важливих інформаційних активів компанії, включаючи інформацію, комп'ютерне обладнання та програмне забезпечення. Це необхідно для того, щоб уникнути можливості порушення одного або декількох атрибутів інформації (конфіденційності, цілісності, доступності)[8, с.30-35]. Оскільки жодна окрема система не є ефективною, фахівці використовують комплексний підхід для створення всеосяжної корпоративної системи управління інформаційною безпекою. Мета цієї статті - розглянути різні моделі побудови корпоративних систем інформаційної безпеки, визначити сучасні стандарти для систем інформаційної безпеки та розробити програмне забезпечення, яке допоможе компаніям пройти сертифікацію на відповідність одному з цих стандартів інформаційної безпеки. Управління.

Для досягнення цієї мети необхідно виконати наступні завдання

- Розробити основні вимоги до створення системи управління інформаційною безпекою підприємства, а також
- аналіз методичного матеріалу з розробки, вивчення досвіду впровадження системи управління інформаційною безпекою та
- рекомендації щодо вдосконалення процесу розробки та впровадження систем управління інформаційною безпекою.

Об'єктом дослідження: є система управління інформаційною безпекою підприємства.

Предметом дослідження: є організація управління інформаційною безпекою на підприємствах в сучасних умовах в Україні.

Методи дослідження: для вирішення вищезазначених наукових завдань у роботі використано методи системного аналізу та теорії інформаційної безпеки.

Наукова новизна одержаних результатів Розроблена методика може бути використана для планування та впровадження системи управління інформаційною безпекою підприємства.

Практичне значення отриманих результатів Розроблена методологія може бути застосована для обґрунтованого вибору шляхів і засобів захисту інформації, інфраструктури та людських ресурсів компанії відповідно до бізнес-цілей, можливостей і ресурсів компанії.

РОЗДІЛ 1. СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

1.1. Розгляд стандарту ISO27001 та його значення для підприємств

ISO 27001 - це міжнародний стандарт, що визначає вимоги до системи управління безпекою інформації (ISMS). Цей стандарт був розроблений для надання загального рамкового рішення для планування, впровадження, операційного контролю, перегляду, підтримки та поліпшення управління безпекою інформації.

Розглянемо значення ISO 27001 для підприємств:

1. **Захист інформації:** Застосування ISO 27001 допомагає організаціям встановити та підтримувати ефективні процедури та політики для захисту своєї важливої інформації. Він зосереджується на розробці «системи управління безпекою інформації», що включає не тільки IT-інфраструктуру, але й людей, процеси та бізнес-операції.
2. **Відповідність законодавству та нормативним вимогам:** ISO 27001 допомагає організаціям дотримуватися вимог щодо захисту даних та інших відповідних законодавчих та регулятивних актів. Це може знизити ризик санкцій, штрафів або інших негативних наслідків порушення цих вимог.
3. **Підвищення довіри стейкхолдерів:** Сертифікація за ISO 27001 може підвищити довіру стейкхолдерів, включаючи клієнтів, інвесторів та партнерів, оскільки це свідчить про те, що організація серйозно ставиться до безпеки інформації.
4. **Управління ризиками:** ISO 27001 передбачає розробку та впровадження процесу управління ризиками, що дозволяє

організаціям ідентифікувати, оцінювати та контролювати ризики для безпеки інформації.

5. Неперервне покращення: ISO 27001 зосереджений на неперервному покращенні. Організації зобов'язані регулярно переглядати та покращувати свою систему управління безпекою інформації, щоб вона залишалася ефективною і актуальною.

Отже, ISO 27001 - це не тільки про технічні заходи для захисту інформації. Він також передбачає оцінку ризиків, залучення керівництва, визначення цілей безпеки, навчання персоналу, управління активами, планування відновлення після аварій та багато іншого.

1.1.1. Управління ризиками

Управління ризиками є важливим аспектом будь-якого бізнесу. Воно допомагає компаніям ідентифікувати, оцінювати, і контролювати потенційні проблеми, які можуть заважати досягненню бізнес-цілей. Нижче подано детальний опис управління ризиками, з використанням прикладів та аналізом його значення.

- Підхід до управління ризиками в інформаційній безпеці: Управління ризиками є ключовим елементом впровадження ISO 27001. Воно включає два основних елементи: оцінку ризиків та управління ризиками. Оцінка ризиків полягає в ідентифікації інформаційних ризиків безпеки та визначенні їх ймовірності та впливу. Управління ризиками зосереджується на визначенні необхідних контролюючих заходів (або контролів), щоб запобігти потенційним інцидентам.

- **Загрози інформаційній безпеці:** Це частина процесу оцінки ризиків. Організація повинна перелічити всі свої активи, потім визначити загрози та вразливості, пов'язані з цими активами, оцінити вплив та ймовірність для кожної комбінації активів/загроз/вразливостей, і, нарешті, розрахувати рівень ризику.

- **Вразливості інформаційної безпеки:** Це також частина процесу оцінки ризиків, що була описана вище.

- **Контроль мітігації:** Це відноситься до процесу управління ризиками, де ви визначаєте, які контролі, або заходи безпеки, потрібні для запобігання потенційним інцидентам. Вибір контролів називається процесом управління ризиками, і в ISO 27001 вони вибираються з Додатка А, який вказує 93 контролі.

- **Стратегія управління ризиками:** Це включає вибір між чотирма основними варіантами обробки (або зменшення) кожного неприйняттого ризику.

 - **Документація і звітність:** Ми повинні задокументувати все, що ми робили до цього часу. Це важливо не тільки для аудиторів, але й для нас, якщо ми хочемо переглянути ці результати через рік або більше.

 - **Заява про застосовність (SoA):** Цей документ насправді показує профіль безпеки вашої компанії. На основі результатів управління ризиками в ISO 27001, ви повинні перелічити всі контролю, які ви запровадили, чому ви їх впровадили, і як цей документ вплине на подальше дії.

 - **План управління ризиками:** Це крок, на якому ми повинні перейти від теорії до практики. Мета Плану управління ризиками - визначити, хто саме буде впроваджувати кожен контроль, в який термін, з яким бюджетом та тощо.

 - **Ідентифікація ризиків:** Перший крок в управлінні ризиками - це виявлення потенційних проблем, які можуть заважати досягненню цілей.

 - **Моніторинг і огляд ризиків:** Останній крок полягає в моніторингу та перегляду ризиків та стратегій їх управління. Це допомагає компанії виявляти нові ризики та забезпечувати, що її стратегії управління ризиками залишаються ефективними.
- Зменшення ризиків інформаційної безпеки важливе для забезпечення захисту важливих активів компанії. Розглянемо кілька способів, якими підприємства можуть це зробити:

1. **Оцінка ризиків:** Це важливий перший крок. Оцінка ризиків дозволяє компаніям визначити, які їх активи найбільше піддатливі ризикам, які загрози можуть вплинути на ці активи, та які потенційні наслідки можуть бути.
2. **Розробка політики безпеки:** Політика безпеки визначає вимоги, процедури та правила, які повинні дотримуватися, щоб забезпечити безпеку активів компанії. Вона має бути чіткою, зрозумілою та доступною всім співробітникам.
3. **Навчання персоналу:** Багато порушень безпеки відбуваються через ненавмисні дії співробітників. Регулярне навчання може допомогти співробітникам зрозуміти важливість безпеки та вчасно розпізнавати та реагувати на загрози.
4. **Технічні заходи:** Застосування захисних технологій, таких як файрволи, антивірусне ПЗ, системи захисту від вторгнень, шифрування, і т.д., може допомогти запобігти або зменшити ризики безпеки.
5. **Регулярний аудит та перегляд:** Навіть найкраща система безпеки вимагає регулярного аудиту та перегляду. Це допомагає виявити будь-які слабкості або порушення, а також дозволяє оцінити ефективність існуючих заходів безпеки.
6. **План відновлення після аварій:** У випадку порушення безпеки важливо мати план дій, який допоможе швидко відновити операції та зменшити наслідки.

1.2. Переваги сертифікації згідно ISO27001

ISO 27001 є міжнародним стандартом для систем управління інформаційною безпекою (Information Security Management Systems, ISMS). Отримання сертифікації ISO 27001 може приносити підприємствам ряд переваг. Ось детальний опис переваг ISO 27001, з використанням прикладів та аналізом ефекту цієї сертифікації.

- **Захист важливої інформації:** ISO 27001 допомагає організації визначити та захистити свої найцінніші інформаційні активи. Наприклад, компанія з медичною інформацією може використовувати ISO 27001, щоб захистити дані пацієнтів, забезпечуючи конфіденційність, цілісність та доступність цієї інформації.

- **Довіра клієнтів та партнерів:** Оскільки ISO 27001 є міжнародно визнаним стандартом, організації, які отримали цю сертифікацію, можуть демонструвати свою прив'язаність до безпеки інформації, збільшуючи довіру клієнтів та партнерів. Наприклад, ІТ-підприємство, що надає хмарні послуги, може використовувати свій сертифікат ISO 27001 як доказ того, що воно серйозно ставиться до безпеки даних своїх клієнтів.

- **Дотримання законодавчих та контрактних вимог:** ISO 27001 може допомогти організаціям виконувати юридичні та контрактні обов'язки, пов'язані з безпекою інформації. Це може бути особливо важливо у галузях з високим рівнем регулювання, таких як фінансові послуги або охорона здоров'я.

- **Уникнення шкідливих витрат на інциденти з безпекою:** Використання ISO 27001 допомагає організаціям виявити і зменшити ризики безпеки, що можуть призвести до дорогоцінних інцидентів з

безпекою. За допомогою систематичного підходу до управління ризиками організація може уникнути несподіваних витрат та втрати репутації.

- Конкурентні переваги: Організації з сертифікацією ISO 27001 можуть використовувати це як конкурентну перевагу, особливо в галузях, де безпека інформації є критичною. Наприклад, компанія, що надає ІТ-консалтинг, може виділятися на ринку завдяки своєму сертифікату ISO 27001.

Використання ISO 27001 може мати велику користь для організацій різних розмірів та галузей. Однак це також вимагає значних зусиль для впровадження та підтримки ISMS, тому організації повинні обмірковувати свої конкретні потреби та обставини, перш ніж вирішити, чи підходить для них ISO 27001.

1.2.1. Покращення репутації підприємства

Репутація підприємства є одним з найважливіших інтангібельних активів, що можуть значно вплинути на його успіх. Покращення репутації вимагає системного підходу та постійних зусиль. Ось декілька способів, якими організації можуть працювати над покращенням своєї репутації:

1. Високі стандарти обслуговування: Одним з найпростіших способів покращити репутацію є забезпечення високоякісного обслуговування клієнтів. Це означає не тільки виконання своїх обіцянок, але й прагнення перевершити очікування клієнтів.
2. Соціальна відповідальність: Корпоративна соціальна відповідальність може бути потужним інструментом для покращення репутації. Організації, які активно займаються благодійністю, сталий розвиток, або ініціативами щодо рівності та різноманітності, можуть покращити свій імідж у спільноті та серед стейкхолдерів.
3. Прозорість та етика: Організації, які демонструють прозорість у своїх діях та прийнятті рішень, можуть покращити свою репутацію. Прозорість може охоплювати все, від фінансової звітності до реакції на проблеми або кризи. Високі стандарти етики також сприяють покращенню репутації.
4. Менеджмент ризиків: Здатність підприємства управляти ризиками також може покращити його репутацію. Це включає розробку та впровадження ефективних стратегій для мінімізації потенційних ризиків, які можуть пошкодити імідж організації.
5. Постійне покращення: Накінець, організації, які прагнуть постійного покращення в усіх аспектах своєї діяльності, можуть покращити свою репутацію. Це може включати усе, від покращення

якості продукції або послуг до вдосконалення внутрішніх процесів та процедур.

1.2.2. Забезпечення відповідності законодавству

Забезпечення відповідності законодавству є важливою частиною успіху будь-якої організації. Це не тільки запобігає юридичним наслідкам, таким як штрафи і санкції, але також підтримує репутацію організації та довіру стейкхолдерів. Ось декілька способів, якими організації можуть працювати над забезпеченням відповідності законодавству:

- Розуміння та визначення вимог: Першим кроком до відповідності є розуміння вимог, які ставить перед вами законодавство. Це може включати вивчення законодавчих актів, регулятивних стандартів, галузевих норм та кодексів практики.
- Створення системи відповідності: Система відповідності може включати різні елементи, такі як політики та процедури, програми навчання та освіти, системи моніторингу та аудиту, а також процедури реагування на порушення.
- Навчання та освіта: Надання навчання та освіти працівникам може бути ключовим для забезпечення відповідності. Це може включати інформування працівників про вимоги законодавства, а також надання конкретних навичок та знань, необхідних для їх дотримання.
- Моніторинг та аудит: Регулярний моніторинг та аудит можуть допомогти організаціям ідентифікувати та виправити будь-які проблеми з відповідністю перед тим, як вони призведуть до серйозних наслідків. Це може включати внутрішні аудити, а також використання зовнішніх аудиторів.
- Реагування на порушення: Незважаючи на всі зусилля, порушення можуть виникнути. Важливо мати чіткі процедури для

реагування на такі ситуації, щоб мінімізувати шкоду та запобігти повторенню порушень у майбутньому.

1.3. Структура стандарту ISO27001

Стандарт ISO 27001 має визначену структуру, що забезпечує організований та систематичний підхід до управління безпекою інформації. Структура стандарту включає:

1. **Загальні вимоги** (розділ 4): Цей розділ включає загальні вимоги до створення, впровадження, утримання та постійного покращення системи управління безпекою інформації (ISMS).
2. **Керівництво** (розділ 5): Здесь описуються вимоги до керівництва з безпекою інформації, включаючи роль керівництва у встановленні політики безпеки інформації, ролі, відповідальність і повноваження в рамках ISMS.
3. **Планування** (розділ 6): Цей розділ включає вимоги до планування дій, які враховують ризики та можливості, планування змін і встановлення цілей безпеки інформації.
4. **Підтримка** (розділ 7): Цей розділ містить вимоги до ресурсів для ISMS, компетентності, свідомості, комунікації і контролю документованої інформації.
5. **Операційна діяльність** (розділ 8): Здесь описуються вимоги до управління ризиками безпеки інформації, впровадження контрольних заходів та планування відповідей на непередбачені ситуації.
6. **Оцінка результатів** (розділ 9): Цей розділ містить вимоги до моніторингу, вимірювання, аналізу та оцінки ISMS, включаючи внутрішні аудити та перегляди керівництвом.

7. **Покращення** (розділ 10): Цей розділ описує, як організація повинна відстежувати і реагувати на невідповідності і недоліки, здійснювати корекційні дії та постійно покращувати систему управління безпекою інформації.

Додаток А до стандарту **ISO 27001** містить перелік контрольних заходів (або контролів), які необхідно застосувати для управління ризиками безпеки інформації.

1) **Вступ та сфера застосування:** Вступ подає загальний огляд стандарту ISO 27001 та його цілей. Сфера застосування визначає контекст, у якому стандарт може бути використаний, та вимоги до системи управління безпекою інформації (ISMS).

2) **Нормативні посилання:** Цей розділ включає всі джерела та стандарти, на які посилається ISO 27001. Це можуть бути інші стандарти ISO або відповідні регулятивні документи.

3) **Терміни та визначення:** В цьому розділі надаються визначення ключових термінів, які використовуються у стандарті ISO 27001. Це може включати терміни, такі як "безпека інформації", "ризик" та "контроль".

4) **Контекст організації:** Цей розділ стосується розуміння організацією її контексту, визначення зацікавлених сторін, а також встановлення обсягу та меж ISMS.

5) **Лідерство:** В цьому розділі обговорюється роль керівництва в створенні, впровадженні та підтримці ISMS. Це включає встановлення політики безпеки інформації та забезпечення ресурсів.

- 6) **Планування:** Цей розділ включає вимоги до планування дій з управління ризиками і впровадження процесу управління ризиками.
- 7) **Підтримка:** Тут обговорюються ресурси, потрібні для ISMS, освіти та підвищення кваліфікації персоналу, свідомість безпеки, комунікацію та управління документацією.
- 8) **Перегляд роботи керівництвом:** Цей розділ вимагає регулярного перегляду ISMS керівництвом з метою оцінки його ефективності та визначення областей для покращення.
- 8) **Покращення:** Останній розділ зосереджується на неперервному вдосконаленні ISMS через виявлення та управління невідповідностями та інцидентами, проведення корекційних дій та перегляду вимог до поліпшення.

1.4. Обов'язкові вимоги для отримання сертифікації

Отримання сертифікації за стандартом ISO 27001 вимагає виконання певних обов'язкових вимог:

1. Оцінка ризику: Організація повинна провести оцінку ризику, включаючи ідентифікацію активів, оцінку їх вартості, визначення загроз та вразливостей, оцінку впливу на діловодство і ймовірності виникнення інцидентів безпеки.
2. Управління ризиком: Організація повинна впровадити процес управління ризиком, що допомагає обрати відповідні контролі, визначити критерії прийнятності ризику та розробити план управління ризиками.
3. Розробка ISMS: Організація повинна розробити, впровадити, виконувати, моніторити, переглядати, підтримувати та вдосконалювати ISMS.
4. Вибір контролю: На основі оцінки ризику організація повинна вибрати контролі, відповідні її вимогам. Вони повинні бути обрані з Додатка А до ISO 27001 або інших відповідних джерел.
5. Розробка Політики безпеки інформації: Організація повинна розробити політику безпеки інформації, що підтримує її бізнес-цілі та стратегію.
6. Керівництво: Керівництво організації повинно показати свою зобов'язаність до ISMS.
7. Освіта і підвищення кваліфікації: Організація повинна забезпечити необхідну освіту та тренінги для співробітників, щоб вони могли ефективно виконувати свої обов'язки.
8. Внутрішні аудити та перегляди керівництва: Організація повинна проводити регулярні внутрішні аудити свого ISMS та

перегляди керівництва для забезпечення його продовжуваної придатності, достатності та ефективності.

9. Відповідність законодавству та регулятивним вимогам: Організація повинна забезпечити відповідність всім відповідним законодавчим, статутним, регулятивним та контрактним вимогам.

10. Неперервне вдосконалення: Організація повинна постійно вдосконалювати свою ISMS на основі результатів моніторингу, вимірювання, аналізу та оцінки.

Сертифікація за стандартом ISO 27001 є важливим кроком для організацій, які прагнуть забезпечити найвищий рівень безпеки інформації. Отримання сертифіката ISO 27001 підкреслює зобов'язання організації захищати даних своїх клієнтів та партнерів, покращує репутацію організації, зменшує ризики інформаційної безпеки та допомагає відповідати вимогам законодавства.

Це стає можливим завдяки впровадженню в організації системи управління безпекою інформації (ISMS), яка включає в себе політику безпеки, процеси оцінки та управління ризиками, вибір контролів безпеки, проведення внутрішніх аудитів та постійне вдосконалення.

Однак, отримання сертифіката ISO 27001 - це не "одноразова подія", а постійний процес. Впровадження та підтримка ISMS вимагає зобов'язання керівництва, тривалого моніторингу, аналізу та вдосконалення, а також періодичних аудитів та переглядів керівництва.

В кінцевому підсумку, сертифікація за стандартом ISO 27001 є важливою інвестицією в безпеку інформації, яка може принести значні вигоди для організації, її стейкхолдерів та клієнтів.

1.5. Risk Assessment

1. Створення системи управління ризиками

Одним з ключових елементів є наявність умов для проведення оцінки ризиків. Наприклад, щорічно та щоразу, коли відбуваються значні зміни. Сюди входить те, як ви будете ідентифікувати ризики; кому ви призначаєте відповідальність за ризики; як ризики впливають на конфіденційність, цілісність і доступність інформації; а також метод розрахунку оціночної шкоди від кожного сценарію і ймовірності його реалізації.

Формальна методологія оцінки ризиків повинна вирішувати кілька питань:

- Основні вимоги безпеки вашої організації
- Шкала ризику
- Схильність до ризику
- Методологія: оцінка ризиків на основі сценаріїв або активів

2. Ідентифікація ризиків

Визначення ризиків, які можуть вплинути на конфіденційність, цілісність та доступність інформації, є найбільш трудомісткою частиною процесу оцінки ризиків.

Тут рекомендовано дотримуватися підходу, заснованого на активах. Розробка переліку інформаційних активів є гарним початком, але якщо ваша організація вже має такий перелік, то більша частина роботи вже буде зроблена.

3. Проаналізуйте ризики

Треба визначити загрози та вразливості, які стосуються кожного активу.

Наприклад, якщо загрозою є "крадіжка мобільного пристрою", то вразливістю може бути "відсутність офіційної політики щодо мобільних пристроїв".

4. Оцінити ризики

Тепер настав час оцінити, наскільки значущим є кожен ризик. Вживати заходів у відповідь на кожен ризик, з яким ви стикаєтесь, марнотратно, тому вам слід використовувати матрицю оцінки ризиків, яка допоможе вам визначити, на які ризики варто звернути увагу та визначити їх пріоритетність.

Більшість матриць оцінки ризиків виглядають так: одна вісь відображає ймовірність реалізації ризикового сценарію, а інша - збитки, які він може спричинити. Посередині виставляються бали, що базуються на їхній сукупності.

Використовуючи матрицю, ви повинні оцінити кожен ризик і порівняти загальну суму балів із заздалегідь визначеним рівнем прийнятності ризику (тобто вашим апетитом до ризику). Отримані бали визначатимуть, як ви будете реагувати на ризик, що є останнім кроком у цьому процесі.

5. Вибрати варіанти поводження з ризиком

Існує кілька способів реагування на ризик:

- Уникнути ризику шляхом його повного усунення
- Змінити ризик, застосувавши засоби контролю безпеки
- Розділити ризик з третьою стороною (через страхування або аутсорсинг)
- Зберегти ризик (якщо він підпадає під встановлені критерії прийнятності ризику)

Метод, який ми оберемо, залежатиме від наших обставин. Уникнення ризику, очевидно, є найефективнішим способом запобігання інциденту безпеки, але це, ймовірно, буде дорого коштувати, якщо не неможливо.

Наприклад, багато ризиків в організації виникають через людські помилки, і ви не завжди зможете вилучити людський фактор з рівняння.

Тому нам доведеться модифікувати більшість ризиків. Це передбачає вибір відповідних засобів контролю, які описані в Додатку А до ISO 27001.

6. Звіти з оцінки ризиків

Правильне проведення процесу оцінки ризиків, безумовно, важливо, але ви повинні пам'ятати, що це лише перший крок на шляху до ефективної безпеки. Після того, як ви завершили оцінку, ви повинні звітувати про свої висновки та впровадити план дій.

Ми повинні скласти кілька звітів на основі вашої оцінки ризиків для процесів аудиту та сертифікації. Наступні два з них є найважливішими:

1. Заява про застосовність (Statement of Applicability)
2. Заява про застосовність документує релевантність кожного з контролів ISO 27001 для вашої організації. Він повинен містити перелік контролів, які ви будете або не будете впроваджувати, разом з поясненням, чому вони були обрані або не були обрані. (Пам'ятайте, що вам потрібно застосовувати засіб контролю лише в тому випадку, якщо він зменшить ризик, який ви визначили).

Також ми повинні вказати рівень прогресу у впровадженні засобу контролю. Це може бути простий прапорець "виконано/не виконано", або ви можете надати більш детальну інформацію,

пояснивши, чи є у вас план, чи чекаєте ви на подальші вказівки, чи розпочали роботу тощо.

Нарешті, треба пояснити, чому будь-які пропущені засоби контролю були визнані несуттєвими.

7. RMP (risk management plan)

RMP містить стислий опис кожного ідентифікованого ризику, заходи, розроблені для його усунення, сторони, відповідальні за ці ризики, а також цільову дату застосування заходів з усунення ризиків.

Робота з ризиком не обов'язково означає його усунення. Залежно від обставин, можливо, буде краще модифікувати ризик, застосувавши засоби контролю безпеки, розділити ризик з третьою стороною (страховиком або іншою третьою стороною) або зберегти ризик (якщо ви вирішите, що ймовірність або серйозність ризику не виправдовує витрати на впровадження відповідних засобів контролю).

Що ще слід задокументувати?

- Додаткові документи допоможуть під час аудиту вашого SoA та RTP.
- Звіт про оцінку ризиків, що містить огляд оцінки, включаючи відповідні активи, застосовані процедури, а також оцінений вплив та ймовірність кожного ризику;
- Звіт за підсумками оцінки ризиків, що деталізує залишкові ризики, тобто ризики, які залишаються після застосування заходів з управління ризиками; і
- Звіт з коментарями, що додається до оцінки ризиків для більш детального пояснення ваших рішень.

РОЗДІЛ 2. ПРАКТИЧНА ЧАСТИНА

2.1. Оцінка ризиків (Risk Assessment Policy)

Оцінка ризиків є фундаментальним елементом управління безпекою інформації в рамках ISO27001. Вона вимагає від організації встановити, розповсюдити і підтримувати політику оцінки ризиків, яка визначає, як ризики будуть ідентифіковані, оцінені, оброблені та контрольовані.

Приклади практичного застосування могли б включати проведення регулярних аудитів безпеки, використання інструментів оцінки ризиків для ідентифікації можливих вразливостей та визначення відповідних контрольних заходів.

Політика оцінки ризиків відіграє важливу роль в стандарті ISO27001, оскільки вона забезпечує основу для ідентифікації, оцінки та управління ризиками для безпеки інформації. Це включає ризики, пов'язані з людьми, процесами та технологіями.

У випадку оцінки ризиків, ключовими елементами є:

- 1) Ідентифікація ризиків: На цьому етапі проводиться систематичний огляд організації, щоб визначити потенційні загрози, вразливості та активи. Можливі ризики можуть включати: атаки хакерів, витоки даних, технічні збої, людські помилки та інше.
- 2) Оцінка ризиків: На цьому етапі визначається вірогідність та вплив кожного ризику. Можна використовувати кілька методів оцінки ризиків, включаючи кількісні (з використанням числових значень) та якісні (на основі досвіду, експертних оцінок).
- 3) Управління ризиками: На цьому етапі визначаються заходи щодо управління ризиками. Це може включати прийняття ризику

(якщо вплив низький), уникнення ризику (не проводити діяльність, яка призводить до ризику), зменшення ризику (впровадження контрольних заходів) або передачу ризику (наприклад, через страхування).

4) Моніторинг та перегляд: Ризики повинні регулярно переглядатися для визначення ефективності заходів управління ризиками та для ідентифікації нових ризиків.

Впровадження ці етапів оцінки ризиків:

- Ідентифікація ризиків: Інструменти для ідентифікації ризиків можуть включати чек-листи, інтерв'ю, робочі групи і технічні аудити. Важливо враховувати всі потенційні джерела ризику, включаючи інформаційні технології, фізичні активи, людські ресурси та постачальників.

- Оцінка ризиків: При оцінці ризиків слід враховувати імовірність та потенційний вплив кожного ризику. Це може вимагати збору даних, аналізу інцидентів безпеки в минулому і консультацій з експертами.

- Управління ризиками: При виборі стратегії управління ризиками важливо взяти до уваги фактори, такі як бізнес-цілі, вартість впровадження контрольних заходів та вимоги стейкхолдерів. Це може потребувати виважених рішень та стратегічного планування.

- Моніторинг та перегляд: Постійний моніторинг і перегляд ризиків є ключовим для підтримки ефективної системи управління безпекою. Це може включати регулярні аудити, аналіз інцидентів безпеки, відгуки від працівників та моніторинг зовнішнього середовища на наявність нових загроз.

Таблиця 2.1. Risk Assessment (приклад 1)

	Початкова ймовірність	Початковий вплив	Початковий ризик	Контроль ризику	Кінцева ймовірність	Кінцевий вплив	Ризик залишку
Розкриття пароля	5 - Певний	5 - Дуже високий	25 - Високий	<ol style="list-style-type: none"> 1. Обізнаність та навчання 2. Використання менеджера паролів 3. Використовую двофакторну авторизацію 	2 - Малоймовірно	5 - Дуже високий	10 - середній
Несанкціонований доступ до мережі	4 - Дуже ймовірний	4 - Високий	16 - Високий	<ol style="list-style-type: none"> 1. Впровадити IDS/IPS, SEM 2. Встановити 3. Фреймворки 4. Регулярне сканування та закриття уразливостей 	2 - Малоймовірно	4 - Високий	8 - середній
Відключення електроенергії	5 - Певний	4 - Високий	20 - Високий	<ol style="list-style-type: none"> 1. Встановлення електрогенераторів та резервних акумуляторів 2. Розділити електромережу для різних відділів 	1 - Неможливо	2 - Незначний	2 - низький

Обладнання для роботи з поштою	4 - Дуже ймовірний	2 - Незначний	8 - Ймовірний	1. Регулярні перевірки 2. Реактивне обслуговування 3. Профілактичне обслуговування	2 - Мало ймовірно	2 - Незначний	4 - низький
--------------------------------	--------------------	---------------	---------------	--	-------------------	---------------	-------------

Таблиця 2.2. Risk Assessment (приклад 2)

	Початкова ймовірність	Початковий вплив	Початковий ризик	Контроль ризику	Кінцева ймовірність	Кінцевий вплив	Ризик залишку
Недостатній рівень знань про ISO 27001	4 - Дуже ймовірний	5 - Дуже високий	20 - Високий	1. Навчання персоналу 2. Залучення консультантів з ISO 27001 3. Навчальні курси для керівників	2 - Мало ймовірний	3 - Помірний	6 - Низький

Відмова персоналу від змін	5 - Певний	4 - Високий	20 - Високий	1. Комунікація з персоналом 2. Організація тренінгів та семінарів 3. Використання системи стимулювання	3 - Можливий	2 - Низький	6 - Низький
Відсутність фінансових ресурсів	3 - Можливий	4 - Високий	12 - Середній	1. Розробка детального бюджету 2. Заплановане резервування коштів 3. Залучення зовнішніх інвестицій	2 - Малоімовірний	2 - Низький	4 - Низький
Недостатня підтримка керівництва	3 - Можливий	5 - Дуже високий	15 - Високий	1. Презентація переваг ISO 27001 керівництву 2. Включення керівництва в процес впровадження 3. Регулярна звітність	2 - Малоімові# I need to quote the table to refer to it later.	2 - Низький	3 - Низький

Таблиця 2.3. Risk Assessment (приклад 3)

Етап	Ризик	Контроль ризику
Підготовка до впровадження	Недостатній рівень знань про ISO 27001	Організація навчання та семінарів для співробітників
Розробка політики безпеки	Неадекватне розуміння потреб організації	Залучення досвідчених консультантів з безпеки інформації
Розробка процедур та інструкцій	Відмова персоналу від змін	Проведення регулярних зустрічей із зворотним зв'язком
Впровадження необхідних технічних заходів	Високі витрати	Планування бюджету та пошук зовнішніх інвесторів
Проведення аудиту безпеки інформації	Недостатня підтримка керівництва	Постійна комунікація з керівництвом та демонстрація прогресу
Постійне покращення	Недостатня мотивація персоналу	Розробка програми винагород та заохочень

Важливо розуміти, що оцінка ризиків - це постійний процес, а не одноразове завдання. Підприємства повинні регулярно переглядати і оновлювати свою політику оцінки ризиків, щоб враховувати зміни в бізнес-процесах, технологіях, регуляторному середовищі та загрозах безпеки. Через встановлення та підтримку ефективної політики оцінки ризиків, організації можуть ідентифікувати, оцінити та обробляти потенційні загрози для інформації, що вона обробляє.

2.2. Політика управління доступом (Change Management Policy)

Управління змінами - це критичний процес, який допомагає контролювати впровадження нових систем, оновлень або змін до існуючих конфігурацій, щоб забезпечити, що вони не викликають небезпеки для безпеки інформації.

Приклади могли б включати формалізацію процесу впровадження змін, який передбачає попередню оцінку ризиків, тестування змін перед їхнім впровадженням і пост-впровадження огляду для забезпечення безпеки.

Політика управління змінами (Change Management Policy):

Політика управління змінами - це необхідний компонент системи управління безпекою інформації, який допомагає підтримувати стабільність, безпеку та надійність систем і сервісів під час впровадження нових змін.

Цей процес включає ряд етапів:

- 1) Планування: Перед тим, як впровадити зміну, вона повинна бути належно спланована. Це означає, що потрібно визначити, які зміни потрібні, чому вони потрібні, як вони будуть впроваджені, і який вплив вони можуть мати на інформаційну безпеку.
- 2) Оцінка та затвердження: Оцінка ризиків повинна бути проведена, щоб визначити можливі наслідки зміни. На цьому етапі зміна має бути затверджена відповідним керівництвом перед її впровадженням.
- 3) Впровадження: Зміна повинна бути впроваджена в контрольованому середовищі. Це може включати тестування зміни, щоб переконатися, що вона працює належним чином і не призводить до несподіваних проблем з безпекою.

- 4) Огляд: Після впровадження зміни, вона повинна бути переглянута для забезпечення її ефективності і для ідентифікації можливих проблем, які можуть виникнути.
 - 5) Процес затвердження змін: Процес затвердження змін вимагає від організацій створення формальної структури, в якій кожна зміна повинна бути розглянута і затверджена перед її впровадженням. Важливо, щоб цей процес був документований, прозорий і включав відповідних стейкхолдерів.
 - 6) Роль тестування: Тестування важливе для забезпечення того, що внесені зміни не призведуть до непередбачених наслідків або проблем з безпекою. Це може включати тестування в ізольованому середовищі перед повним впровадженням зміни.
 - 7) Обов'язок документування: Документування є важливим елементом управління змінами. Кожна зміна, її оцінка ризику, процес затвердження, результати тестування та вплив на систему повинні бути документовані для майбутнього посилення та аудиту.
 - 8) Навчання та комунікація: Працівники, які зачіпаються змінами, повинні бути повідомлені і, при необхідності, проінструктовані щодо нових процедур або систем. Важливо забезпечити, щоб вони розуміли причини змін, їх вплив та їх роль у впровадженні змін.
 - 9) Перегляд і вдосконалення: Після впровадження зміни, вона повинна бути переглянута для забезпечення її ефективності. Це може включати аналіз впливу зміни, визначення проблем, які можуть бути вирішені, та вдосконалення процесу управління змінами на основі навчання.
- Політика управління змінами є невід'ємною частиною політики безпеки інформації в рамках ISO 27001 і вимагає тщеславного підходу до планування, впровадження, оцінки та перегляду змін.

Управління змінами є важливим для забезпечення безпеки інформації під час впровадження нових систем або оновлення існуючих. Впровадження ретельної політики управління змінами може допомогти підприємствам зменшити ризики, пов'язані з такими змінами.

2.3. Політика управління доступом (Access Management Policy)

Управління доступом вимагає від організації визначити і впровадити політику, яка регулює, хто може мати доступ до яких ресурсів, і за яких умов.

Приклади можуть включати використання принципу найменшого привілею, двофакторної аутентифікації, та контролю доступу на основі ролей.

- 1) Принцип найменшого привілею (PoLP) є важливою частиною політики управління доступом. Він вимагає від організацій надавати користувачам, системам та процесам лише ті права та дозволи, які є необхідними для виконання їхньої роботи. Застосування цього принципу може допомогти зменшити ризик навмисного або ненавмисного зловживання системами. Прикладом впровадження принципу найменшого привілею може бути використання системи контролю доступу, яка вимагає від адміністраторів системи працювати під звичайними користувацькими обліковими записами, поки їм не потрібно виконувати завдання, що вимагають більших привілеїв.
- 2) Двофакторна аутентифікація - це метод перевірки ідентичності користувача, який вимагає два або більше факторів: щось, що користувач знає (наприклад, пароль), щось, що він має (наприклад, фізичний токен або смартфон), або щось, що є характерною особливістю самого користувача (наприклад, біометрія). Двофакторна аутентифікація може значно підвищити безпеку, оскільки шанси, що зловмисник зможе забезпечити обидва фактори, зменшуються.

3) Контроль доступу на основі ролей: Контроль доступу на основі ролей (RBAC) - це метод обмеження системного доступу до користувачів на основі ролей, які вони виконують у межах організації. Ролі визначаються відповідно до відповідності до авторитету і відповідальності в межах організації, а права доступу пов'язані з кожною роллю, а не з кожним окремим користувачем.

Управління змінами є важливим для забезпечення безпеки інформації під час впровадження нових систем або оновлення існуючих. Впровадження ретельної політики управління змінами може допомогти підприємствам зменшити ризики, пов'язані з такими змінами.

2.4. Політика щодо тренінгів з інформаційної безпеки (Security Awareness Policy)

Навчання з інформаційної безпеки має на меті забезпечити, що всі працівники зрозуміють свої обов'язки щодо безпеки інформації та знають, як реагувати на потенційні інциденти.

Приклади могли б включати регулярне навчання працівників, проведення тестових атак фішингу для перевірки свідомості працівників, та надання ресурсів для самоосвіти.

Наведемо приклади:

- Регулярне навчання з інформаційної безпеки важливе для підтримання та посилення знань працівників про правила та процедури, пов'язані з безпекою. Це може включати онлайн-курси, семінари, вебінари та інтерактивні навчальні модулі, які охоплюють ключові теми, такі як управління паролями, фішинг, соціальна інженерія та захист від малвару.
- Тестові атаки фішингу: Проведення тестових атак фішингу - це ефективний спосіб оцінити, наскільки добре працівники зрозуміли та засвоїли навчання з інформаційної безпеки. Це включає в себе відправлення підроблених електронних листів, що містять безпечні посилання або вкладення, із метою перевірки реакції співробітників. Результати можуть допомогти виявити слабкі місця в освіті та підготовці персоналу.
- Ресурси для самоосвіти: Надання ресурсів для самоосвіти, таких як статті, брошури, відео та інтерактивні модулі, може сприяти

постійному розвитку знань працівників про безпеку. Ці ресурси можуть бути доступними через внутрішню корпоративну мережу або на спеціалізованому порталі з інформаційної безпеки. Регулярне надання актуальної інформації також може допомогти підтримувати високий рівень свідомості з питань безпеки серед співробітників.

Навчання і освіта з питань інформаційної безпеки є критичними для забезпечення того, що всі працівники зрозуміють свої обов'язки.

Постійне навчання та самоосвіта можуть допомогти підтримувати високий рівень свідомості щодо безпеки в усій організації.

2.5. Політика інформаційної безпеки

1. Document Owner and Approval:

- Політика управління змінами належить директору з інформаційної безпеки, який відповідає за те, щоб вона залишалася актуальною та відображала поточну практику та потреби ІТ-служб в організації.
- У нашій організації остаточну відповідальність за затвердження цієї політики несе директор з інформаційної безпеки (CISO). Політика переглядається щороку або частіше, якщо відбуваються значні зміни в операційному середовищі. Директор з інформаційної безпеки проводить цей перегляд, консультуючись, за необхідності, з іншими зацікавленими сторонами.
- Після завершення перегляду оновлена політика подається на затвердження директору з інформаційної безпеки. Політика набуває офіційного статусу та набуває чинності лише після того, як її схвалює директор з інформаційної безпеки.
- Усі оновлення та зміни до політики своєчасно доводяться директором з інформаційної безпеки до відома відповідних зацікавлених сторін. Ці зацікавлені сторони несуть відповідальність за розуміння та дотримання оновленої політики.

2. Scope:

- Дана політика впроваджується до всіх модифікацій в інструментах, архітектурі та ІТ-службах, що надаються інформаційними службами компанії. Зміни, які здійснені в неоперативних системах (наприклад, тестових оточеннях, які не мають впливу на виробничі ІТ-служби), не входять в рамки цієї політики.

3.Responsibilities:

- Керівник змін встановлює важливість запитів на зміни, оцінює їх вплив, а потім приймає або відхиляє запропоновані зміни. Він відповідає за підтримання системи управління змінами та забезпечення виконавців змін необхідними інструментами. Більше того, керівник змін займається документацією процесів управління змінами та планів змін.
- Ініціатор зміни відповідає за розробку та подачу запитів на зміни. Він забезпечує належне оформлення форми запиту на зміну та її подачу в потрібний термін, щоб зміни були затверджені. Ініціатор також має визначити тестувальника та виконавця зміни і отримати затвердження від відповідних осіб.
- Виконавець зміни відповідає за впровадження затверджених змін.
- Тестувальник змін відповідає за тестування розроблених змін.
- Власники сервісів, процесів та конфігурації зобов'язані здійснювати реєстрацію змін.

4. Policy:

- Зміни мають бути впроваджені лише після затвердження керівником змін.
- Необхідно створити план впровадження змін.
- Зміни реалізуються виключно поза робочим часом.
- Всі власники сервісів, процесів та елементів конфігурації зобов'язані реєструвати всі зміни в системі реєстрації змін.
- Всі внесені зміни мають бути задокументовані.
- Має бути розроблений план відновлення у випадку збою.
- Зміни не повинні погіршувати якість продукції.
- Повинен бути створений план тестування.
- Зміни мають бути протестовані.
- Всі тести мають бути задокументовані.

5. Enforcement:

- Порухення цієї політики будь-якою зацікавленою стороною буде розглядатися серйозно і може призвести до дисциплінарних заходів аж до звільнення або розірвання договірних відносин у випадку з постачальниками та партнерами.
- Випадки недотримання вимог розглядатимуться менеджером змін і, за необхідності, поводитимуться до відома вищого керівництва. Усі випадки невідповідності повинні бути задокументовані та доведені до відома відповідного органу в організації.
- Будь-яка зміна, впроваджена без належного затвердження або без дотримання керівних принципів політики, буде вважатися порушенням цієї політики. Зміни можуть бути скасовані, а відповідальна особа або група може бути притягнута до відповідальності.
- Для забезпечення дотримання цієї політики будуть проводитися регулярні аудити. Результати аудиту розглядатимуться менеджером змін та поводитимуться до відома вищого керівництва. Будь-які виявлені прогалини або невідповідності призведуть до негайних коригувальних дій.
- Співробітникам, підрядникам та іншим зацікавленим сторонам рекомендується повідомляти про будь-які підозри у порушенні цієї політики своєму безпосередньому керівнику або менеджеру змін.

- Регулярно проводитимуться тренінги та інформаційні сесії, щоб усі зацікавлені сторони розуміли свої обов'язки згідно з цією політикою та важливість її дотримання.
- Здійснюватиметься постійний моніторинг та звітування для забезпечення ефективності політики та управління змінами відповідно до неї. Якщо політика виявилася неефективною, вона буде переглянута і, за необхідності, змінена.

2.6. Політика Access Management Policy

1. Document Owner and Approval:

Цей документ "Політика управління доступом" є власністю директора з інформаційної безпеки (CISO) організації. Політика розглядається та затверджується Радою директорів щороку або частіше, якщо це необхідно.

2. Scope:

Ця політика поширюється на всіх співробітників, підрядників, партнерів і будь-яких інших осіб, які мають доступ або отримують доступ до будь-яких інформаційних ресурсів компанії. Це включає всі форми доступу, як фізичні (наприклад, доступ до приміщень та обладнання), так і електронні (наприклад, доступ до систем, баз даних та мереж).

3.Responsibilities:

- IT-директор відповідає за нагляд за розробкою, впровадженням та дотриманням цієї політики.
- Керівники відділів несуть відповідальність за забезпечення дотримання цієї політики їхніми співробітниками.
- IT-відділ відповідає за впровадження контролю доступу, управління доступом користувачів, навчання та підтримку.
- Усі користувачі несуть відповідальність за відповідальне використання своїх привілеїв доступу та повідомляють про будь-які підозри у порушенні цієї політики.

4. Policy:

- Доступ до інформаційних ресурсів повинен ґрунтуватися на принципі найменших привілеїв, що означає, що особам слід надавати мінімальний рівень доступу, необхідний для виконання їхніх посадових обов'язків.
- Права доступу користувачів повинні переглядатися та оновлюватися на регулярній основі, а також негайно після зміни ролі користувача.
- Весь доступ користувачів повинен бути санкціонований та задокументований.
- Доступ до конфіденційної інформації повинен суворо контролюватися та реєструватися.
- Користувачі повинні захищати свою автентифікаційну інформацію та не передавати її іншим.
- Тимчасовий доступ повинен бути обмежений у часі та негайно відкликаний, як тільки він більше не потрібен.

5. Enforcement:

- Будь-які порушення цієї політики можуть призвести до дисциплінарних стягнень, аж до розірвання трудових або контрактних відносин.
- Про будь-які випадки несанкціонованого доступу або зловживання правами доступу слід повідомляти, і вони будуть розслідуватися.
- Для контролю за дотриманням цієї політики проводитимуться регулярні аудити.
- Для забезпечення розуміння та дотримання цієї політики будуть проводитися тренінги та інформаційні сесії.

- Якщо політика виявилася неефективною, вона буде переглянута та оновлена за необхідності.

ВИСНОВОК

В рамках даної дипломної роботи було проведено заглиблене дослідження політик безпеки інформації згідно зі стандартом ISO 27001. Кожна з аналізованих політик відіграє важливу роль в загальній системі управління безпекою інформації в організації.

Оцінка ризиків, управління змінами, управління доступом та просвітництво в галузі безпеки – це важливі складові, які допомагають забезпечити інформаційну безпеку в організації. Вони не лише зменшують можливість втрати даних або хакерських атак, але і покращують загальну свідомість співробітників про значення безпеки інформації.

Додаток А до ISO 27001, який включає список контрольних заходів безпеки, є іншим важливим елементом, що варто враховувати при розробці політик безпеки інформації.

Однак, важливо зазначити, що безпека інформації - це неодноразовий процес, а постійний процес, що вимагає неперервного моніторингу, оновлення та навчання. Кожна організація має бути готова до змін, адаптуватися до нових загроз та активно працювати над покращенням своїх політик та процедур.

В подальшому, рекомендується продовжити дослідження в цій області, оскільки технології та загрози безпеки постійно розвиваються. Безпека інформації важлива не лише для організації, а й для всіх її співробітників, клієнтів та партнерів.

Вдосконалення безпеки інформації - це невід'ємна частина роботи будь-якої сучасної організації. У процесі розробки та впровадження політик з оцінки ризиків, управління змінами, управління доступом та освіти з безпеки інформації, організації

можуть стати більш стійкими до потенційних загроз та підвищити ефективність своїх операцій.

Крім того, організації повинні розуміти важливість неперервної адаптації та навчання. Технології та засоби забезпечення безпеки швидко розвиваються, і організації повинні бути готові швидко реагувати на ці зміни. Неперервне навчання і розвиток в області безпеки інформації не лише допоможе організації захистити свої ресурси, але й допоможе її співробітникам бути більш обізнаними і впевненими у своїй роботі.

У кінцевому підсумку, впровадження ефективних політик безпеки інформації, зокрема, тих, що описані в стандарті ISO 27001, є важливим кроком для забезпечення довгострокової стабільності та успіху організації. Впровадження таких політик вимагає зусиль, але потенційні вигоди, які вони можуть принести, безсумнівно, переважають можливі витрати.

Дана дипломна робота демонструє значущість безпеки інформації та необхідність ретельного розуміння та впровадження відповідних політик. Надіємось, що це дослідження буде корисним для організацій, які прагнуть підвищити свій рівень безпеки інформації.

Рекомендації

- 1. Неперервне оновлення політик безпеки:** Технології швидко розвиваються, і з цим приходять нові загрози безпеки. Організаціям необхідно регулярно оновлювати свої політики безпеки, щоб вони відповідали сучасним стандартам і вимогам.
- 2. Навчання співробітників:** Безпека інформації - це не лише технологічне питання. Співробітники організації є одним з найбільших ризиків для безпеки інформації. Регулярні тренінги і освіта з безпеки інформації мають велике значення.
- 3. Розширення охоплення політик:** Політики безпеки мають охоплювати всі аспекти організації, включаючи фізичну безпеку, безпеку мережі, безпеку даних, і т.д.
- 4. Впровадження інструментів автоматизації:** Використання автоматизованих інструментів для моніторингу безпеки інформації може значно знизити ризик втрати даних і злому.
- 5. Співпраця з експертами:** Розробка і впровадження політик безпеки інформації - складний процес, який може вимагати експертних знань. Варто розглянути можливість співпраці з експертами в області безпеки інформації.
- 6. Підтримка керівництва:** Без активної підтримки керівництва, політики безпеки можуть не бути ефективно впроваджені. Важливо забезпечити, що управління розуміє значення безпеки інформації та активно підтримує її політики.

7. Сертифікація ISO 27001: Розгляньте можливість сертифікації ISO 27001. Це міжнародно визнаний стандарт, що підтверджує зобов'язання організації до безпеки інформації.

Список використаних джерел

1. ISO. (2021). "ISO/IEC 27001 Управління інформаційною безпекою". <https://www.iso.org/isoiec-27001-information-security.html>
2. Міжнародна організація зі стандартизації. (2013). "ISO/IEC 27001:2013". Женева, Швейцарія: ISO.
3. BSI Group. (2018). "Впровадження СУІБ, шлях ISO 27001:2013".
4. IT Governance. (2021). "ISO 27001 - Стандарт інформаційної безпеки". <https://www.itgovernance.co.uk/iso27001>
5. ISACA. (2018). "ISO 27001: Посібник із впровадження та сертифікації".
6. Студія управління ризиками. (2021). "Як впровадити ISO 27001". <https://www.riskmanagementstudio.com/>
7. ISO/IEC. (2018). "Сімейство ISO/IEC 27000 - Системи управління інформаційною безпекою".
8. BSI. (2021). "ISO/IEC 27001 Управління інформаційною безпекою". <https://www.bsigroup.com/>
9. Посібник з сертифікації ISO. (2021). "Процес сертифікації ISO 27001".
10. Міжнародна електротехнічна комісія. (2018). "Інформаційні технології - методи безпеки".

11. ISMS.online. (2021). "ISO 27001:2013 Системи управління інформаційною безпекою".
12. PECB. (2021). "Навчальні курси ISO/IEC 27001".
<https://pecb.com/>
13. Стаття «Інформаційна безпека і її складові». – Електронний ресурс – Режим доступу: <https://egrivna.com/informacijna-bezpeka-i-ii-skladovi-2/>
14. NQA Certification Ltd. (2021). "ISO 27001:2013 Системи управління інформаційною безпекою". <https://www.nqa.com/>
15. Sans Institute. (2019). "Офіційний стандарт ISO/IEC 27001 щодо СУІБ".
16. TechTarget. (2021). "Що таке ISO 27001?".
<https://www.techtarget.com/>
17. Дістерер, Г. (2013). "ISO/IEC 27000, 27001 та 27002 для управління інформаційною безпекою". Журнал інформаційної безпеки, 4(2), 92-100.
18. Про захист інформації в автоматизованих системах: Закон України // Відомості Верховної Ради. 1994.-№31.-286
19. Методика оцінювання захищеності інформаційних систем за допомогою СУІБ «Матриця». [Електронний ресурс] Режим доступу: http://www.epos.ua/view.php/about_pubs_archive
20. Про національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28

