НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет харчових технологій та управління якістю продукції АПК

УДК 006.91:005

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету	**В.о. завідувач кафедри**
харчових технологій та управління якістю продукції АПК	стандартизації та сертифікації сільськогосподарської продукції
_____ **Баль-Прилипко Л.В.**	_____ **Толок Г.А.**
«__» _____ 2022 р.	«__» _____ 2022 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Розроблення елементів системи управління інформаційною безпекою в умовах ФОП «Почерпайло Андрій Андрійович», м. Київ»»

Спеціальність: **152 «Метрологія та інформаційно-вимірювальна техніка»**
Освітня програма – **«Якість, стандартизація та сертифікація»**

Орієнтація освітньої програма – **Освітньо-професійна програма**

Гарант освітньої програми

к.т.н., доцент _____ **Слива Ю.В.**

Керівник магістерської роботи

к.с.-г.н., доцент _____ **Адамчук Л.О.**

доктор філософії (PhD), асистент _____ **Розбицька Т.В.**

Виконав _____ **Почерпайло А.А.**

КИЇВ – 2022
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ

І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет харчових технологій та управління якістю продукції АПК

ЗАТВЕРДЖУЮ:
В.о. завідувач кафедри
стандартизації та сертифікації
сільськогосподарської продукції,
канд. техн. наук, доц.
Прядко О.А.
«__» _____ 2022 р.

З А В Д А Н Н Я
ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ РОБОТИ СТУДЕНТУ
Почерпайлу Андрію Андрійовичу

Спеціальність: 152 «Метрологія та інформаційно-вимірювальна техніка»
Освітня програма – «Якість, стандартизація та сертифікація»
Програма підготовки – Освітньо-професійна
Тема магістерської роботи: «Розроблення елементів системи управління інформаційною безпекою в умовах ФОП «Почерпайло Андрій Андрійович», м. Київ»
затверджена наказом ректора НУБіП України № 117 «С» від 19.01.2022р. Термін подання завершеної роботи на кафедру 1 листопада 2022 р.
Вихідні дані до магістерської роботи: 1) Положення про підготовку магістрів у НУБіП України; 2) Положення про підготовку і захист магістерської роботи 3) Міжнародні та національні стандарти; 3) Словникові та довідникові джерела; 4) Навчальна та наукова література; 5) Методичні вказівки про підготовку магістерської роботи; 6) Фахові періодичні видання; 7) Матеріали державної статистики; 8) Електронні ресурси.
Перелік питань, що підлягають дослідженню:

1. Аналіз вимог стандартів та європейського і вітчизняного законодавства;
2. Розроблення елементів системи управління інформаційною безпекою в умовах підприємства.
3. Розрахунок економічної ефективності від впровадження передумов.

Дата видачі завдання «27» січня 2022 р.

Керівники магістерської роботи Адамчук Л.О.

Розбицька Т.В.

Завдання прийняв до виконання Почерпайло А.А.

РЕФЕРАТ

Магістерська робота, була розроблена з дотриманням усіх вимог та складається з 3 розділів, розміщена на 85 сторінках друкованого тексту, містить таблиці, 3 рисунки, висновки, список використаних джерел та додатки.

В *першому розділі* роботи досліджено літературу та інші джерела інформації щодо стандарту якості ISO/IEC 27001; історію сімейства стандартів ISO/IEC 27000; надано інформацію щодо виникнення та впровадження стандарту у світі та на території України; розглянуто методи та засоби забезпечення безпеки інформаційних технологій у відповідності до міжнародних стандартів.

В *другому розділі* проведена характеристика ФОП "Почерпайло Андрій Андрійович", проведено аналіз діючої системи зберігання та обміну інформацією, визначено організаційні заходи забезпечення інформаційної безпеки і захисту інформації підприємства.

В *третьому розділі* здійснено аналіз системи вдосконалення засобів захисту інформації на підприємстві, проведений аналіз процедури розробки веб застосунку, визначено особливості процесу створення веб додатку.

Ключові слова: *ІНФОРМАЦІЙНА БЕЗПЕКА, РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ISO/IEC 27001.*

ЗМІСТ

ВСТУП

Актуальність теми. Інформаційною безпекою називається стан захищеності систем обробки та зберігання даних, інформація має бути убезпечена з точки зору конфіденційності, доступності і цілісності.

Заходи щодо захисту процесу створення інформації, її введення, обробки і виведення є основними завданнями дотримання інформаційної безпеки. Основне

завдання спеціаліста з дотримання інформаційної безпеки на підприємстві полягає в тому, щоб налаштувати процеси обробки, передачі та зберігання даних таким чином щоб він відповідав стандартам які визнані у світі. Цей процес має включати убезпечення цілісності систем, захисті і гарантії точності і цілісності даних. Також важливо зберігати розуміння що цілісність навіть найкраще захищеної інформаційної системи може бути порушена. В такому випадку дуже важливо розуміти як знайти процес витоку чи знищення інформації, визначити чи інцидент ще триває або чи можливе відтворення його в майбутньому, яким чином зупинити процес якщо він ще наявний у інформаційній системі та як найменшими втратами мінімізувати наслідки інциденту.

Облік та класифікація всіх дій, що призводять до створення, модифікації та поширення інформації - один з головних стовпів на яких грунтується поняття інформаційної безпеки. Облік може бути автоматизованим або вестися вручну людиною з відповідною кваліфікацією.

Цей принцип є базисним для будь яких форм які можуть приймати дані, фізична чи електронна. Основне завдання інформаційної безпеки – збалансований захист конфіденційності, цілісності і доступності даних, з урахуванням доцільності застосування.

Сучасна та ефективна система забезпечення інформаційної безпеки (СЗІБ) це певний комплекс заходів, які відповідають за захист конфіденційної корпоративної інформації на всіх стадіях її життєвого циклу: обробки, передачі та зберігання.

Це особливо важливо для організацій які використовують дані як свій основний продукт. Наприклад ІТ підприємства, дизайн студії та організації які спеціалізуються на обробці та редагуванні медіа контенту. Наразі в Україні наявне велике різноманіття підприємств з вищеназваної специфікації. Оскільки багато з них висловили пряме засудження агресії проти України – вони як є, так і можуть стати ціллю інформаційного тероризму. Основною небезпекою для таких випадків є те, що основним продуктом цих організацій є інформація, тобто її витік чи пошкодження можуть спричинити величезні збитки на ризики. Проте

для підприємств які мають більш фізичний основний продукт ці ризики не є набагато меншими. Оскільки у сучасному світі важко уявити успішний бізнес який не має розвиненої інформаційної системи.

Система забезпечення інформаційної безпеки є дієвою, тільки в тому випадку якщо заходи які мають виконуватись є ретельно спланованими, налаштованими, а в діяльності підприємства використовуються передові технології та дотримуються міжнародні стандарти інформаційної безпеки. Цей підхід, особливо у наш час, має допомогти мінімізувати ризики, забезпечити ретельне планування для підприємств України.

Безперервне функціонування СЗІБ можливе лише завдяки поєднанню організаційних і технічних заходів, що застосовуються відповідно до верхньорівневих рішень, та розробляються в рамках системи управління інформаційною безпекою (СУІБ).

Для створення сучасних систем СЗІБ існує сімейство стандартів, які мають допомогти виконавцю створити та убезпечити процеси збереження та передачі інформації на відповідному рівні інформаційної гігієни та убезпечення всієї системи.

В цілому створення СЗІБ – це сучасний комплекс заходів для захисту конфіденційної особистої та корпоративної інформації із залученням різноманітних спеціалістів та експертів. При цьому сучасні інформаційні проекти мають спиратися на досвід та стандарти розробки передових Українських та міжнародних ІТ та підприємств які мають великі обсяги інформації у повсякденній роботі.

Аналіз останніх досліджень і публікацій. Аналіз наукової літератури свідчить, що питання системи інформаційної безпеки досліджували в своїх наукових роботах багато вчених: Гавловський В.Д., Левченко О.В., Львова А.В., Маслова М.А., Карл Я. та багато інших. Питання досить широко описане та вивчене, проте все ще залишаються величезні простори для теоретичних досліджень та практичних напрацювань, оскільки сам інформаційний простір на підприємстві невпинно розширюється.

Мета і завдання дослідження. Мета дипломної роботи полягає в тому, щоб на основі повного розгляду нормативних актів, монографічних, літературних джерел, інтернет простору інформації здійснити розроблення та покращення різних аспектів системи управління інформаційною безпекою в умовах підприємства ФОП "Почерпайло Андрій Андрійович".

Відповідно до визначеної мети було поставлено такі завдання:

- дослідити складові та особливі властивості інформаційної безпеки;
- розглянути методи та засоби забезпечення безпеки інформаційних технологій у відповідності до міжнародних стандартів.
- провести характеристику наявної інформаційної безпеки ФОП "Почерпайло Андрій Андрійович".
- розглянути історію ISO/IEC 27001.
- розглянути прийняття ISO/IEC 27001.
- визначити та провести аналіз принципів сімейства стандартів ISO/IEC 27001.
- визначити організаційні заходи забезпечення інформаційної безпеки і захисту інформації підприємства.
- провести удосконалення засобів захисту інформації на підприємстві.
- провести розробку системи інформаційної безпеки підприємства.
- визначити особливості співробітництва та інтеграції умов замовника в інформаційну систему підприємства.

Об'єктом дослідження є інформаційна безпека конкретного підприємства.

Предметом дослідження є управління інформаційною безпекою в умовах підприємства ФОП "Почерпайло Андрій Андрійович"

Методи дослідження. Методологічну основу дослідження склали наступні методи пізнання: аналіз, синтез, індукція і дедукція, методи матеріалістичної діалектики узагальнення, системний підхід, порівняльний аналіз.

Теоретична, методична та практична значущість отриманих результатів. Представлена магістерська робота є монографічним дослідженням, вона присвячена комплекеному аналізу управління та розробці елементів

системи управління інформаційною безпекою в умовах підприємства ФОП "Почерпайло Андрій Андрійович". Автором було вивчено наявну систему та минулий досвід співробітників та здійснено розробку цілого ряду теоретичних положень. Практичне значення результатів проведеного дослідження полягає у тому, що вже у розробці веб застосунку були впроваджені відповідні безпекові стандарти на практики. Результати дослідження можуть використовуватися при теоретичній та практичній роботі, яка пов'язана з дослідженням системи інформаційної безпеки.

Інформаційна база дослідження. Інформаційна база представлена нормативно-правовими актами, законами, монографіями, авторськими статтями та інформаційними сайтами мережі Інтернет.

РОЗДІЛ І. ОГЛЯД ЛІТЕРАТУРИ

1. Історія впровадження стандарту якості ISO/IEC 27001

1.1 Історія сімейства стандартів ISO/IEC 27000

Серія стандартів з менеджменту інформаційної безпеки (ІБ) ISO/IEC 27000 розробляється технічним комітетом ISO/IEC JTC 1 «Інформаційні технології» (об'єднаний технічний комітет №1 – Joint Technical Committee 1) підкомітетом SC 27 «Методи захисту в інформаційних технологіях».

Система управління інформаційною безпекою (СУІБ) містить вимоги реалізації і вдосконалення систем менеджменту захисту інформації та інформаційних технологій, що грунтуються на моделі PDCA (Plan-Do-Check-Act (планування-виконання-перевірка-дія)) та включає:

- створення (або планування) – ідентифікація активів, управління ризиками;
- впровадження (або виконання) – етапи реалізації відповідних заходів з управління безпекою;
- перевірка – моніторинг та аналіз;
- дію – підтримання в робочому стані та поліпшення.

Досить важливою частиною системи являється цикліність процесів управління безпекою інформації – вся система проходить етапи PDCA [1].

На сьогодні інформація стала на вагу золота. Через розвиток сучасних технологій та виробництв інформація може стати найважливішим ресурсом для, наприклад, фінансової компанії чи мільйонному виробникові на міжнародному ринку товарів та послуг, тому що певна інформація може збагатити компанію або ж знищити її через надходження конкретної інформації конкурентові. Також інформація може бути серйозним ресурсом в руках особи, яка вміє нею розпоряджатися, це можуть бути не тільки якісь масштабні виробники чи фінансові компанії, а звичайна людина чи група людей, тобто інформація дуже цінна і в локальному розумінні. Тому, інформація вважається найцінніщим активом для організацій різного спрямування та розмірів.

Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII дає визначення інформації в якості будь-яких відомостей та/або даних, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, а також системи захисту інформації в якості сукупності правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Підвищення значущості інформації з часом призвело до поширення потреби в розробці та реалізації структури управління безпекою інформації. Результатом такого явища стало ініціювання процесу створення відповідних

стандартів якості ISO/IEC, результатом якого виникла група стандартів ISO 27000. Це сімейство відповідає за стандартизацію певної діяльності, що пов'язана із застосування та використанням СУІБ. В таблиці 1.1 описано всі стандарти серії ISO/IEC 27000.

ISO/IEC 27000 містить ряд взаємопов'язаних стандартів та вказівок, які були опубліковані на даний момент чи ще знаходяться на етапі розробки. Також, дана група стандартів якості вміщує певні структурні компоненти, які орієнтовані на нормативні стандарти, які в свою чергу складаються з вимог до СУІБ, вимог органів із сертифікації, що надають послуги із сертифікації відповідно до ISO/IEC 27001, та додаткових вимог для секторальних впроваджень СУІБ [2]. В таблиці 1.1 описано всі стандарти із серії ISO/IEC 27000 [3].

Міжнародні стандарти, що належать до сімейства 27000, служать основою для створення і експлуатації систем управління інформаційною безпекою.

Мета даного стандарту полягає у створенні загального опису аспектів та понять системи управління інформаційною безпекою, що дозволяє ознайомитися та зрозуміти технічну термінологію загальної системи, яка використовується в процесі стандартизації.

Таблиця 1.1

Список стандартів серії ISO/IEC 27000

Стандарт	Рік публікації	Назва стандарту
ISO/IEC 27000	**2018**	Системи управління інформаційною Безпекою. Огляд та словниковий запас
ISO/IEC 27001	**2013 (переглядається)**	Системи управління інформаційною безпекою. Вимоги

ISO/IEC 27002	**2013 (переглядається)**	Кодекс практики контролю захисту інформації
ISO/IEC 27003	**2017**	Системи управління інформаційною Безпекою. Керівництво
ISO/IEC 27004	**2016**	Управління інформаційною безпекою – моніторинг, вимірювання, аналіз та оцінка
ISO/IEC 27005	**2018**	Управління ризиками інформаційної Безпеки
ISO/IEC 27006	**2015**	Вимоги до органів, що здійснюють аудит та сертифікацію систем управління інформаційною безпекою
ISO/IEC 27007	**2017 (переглядається)**	Вказівки щодо аудиту систем управління інформаційною безпекою
ISO/IEC TS 27008	**2019**	Вказівки щодо оцінки контролю інформаційної безпеки
ISO/IEC 27009	**2016 (переглядається)**	Застосування ISO / IEC 27001, що стосується сектора. Вимоги
ISO/IEC 27010	**2015**	Управління інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій
ISO/IEC 27011	**2016**	Кодекс практики контролю безпеки інформації, заснований на ISO / IEC 27002 для телекомунікаційних організацій
ISO/IEC 27013	**2015 (переглядається)**	Керівництво щодо інтегрованого впровадження ISO / IEC 27001 та ISO / IEC 20000-1

ISO/IEC 27014	**2013 (переглядається)**	Управління інформаційною безпекою
ISO/IEC TR 27016	**2014**	Управління інформаційною безпекою. Організаційна економіка
ISO/IEC 27017	**2015**	Кодекс практики контролю захисту інформації, заснований на ISO / IEC 27002 для хмарних сервісів
ISO/IEC 27018	**2019**	Кодекс практики захисту особистих даних (PII) у публічних хмарах, що виступають як процесори PII
ISO/IEC 27019	**2017**	Контроль інформаційної безпеки для енергетичної галузі
ISO/IEC 27021	**2017**	Вимоги до компетенції фахівців із систем управління інформаційною безпекою
ISO/IEC 27022	**У стадії розробки**	Керівництво процесами ISMS
ISO/IEC TR 27023	**2015**	Картографування оновлених видань ISO /IEC 27001 та ISO / IEC 27002
ISO/IEC 27030	**У стадії розробки**	Керівні принципи безпеки та конфіденційності в Інтернеті речей (IoT)
ISO/IEC 27031	**2011 (переглядається)**	Керівництво щодо готовності інформаційно-комунікаційних технологій до безперервності бізнесу
ISO/IEC 27032	**2012 (переглядається)**	Керівні принципи щодо кібербезпеки
ISO/IEC 27033-1	**2015**	Безпека мережі. Частина 1: Огляд та концепції

ISO/IEC 27033-2	**2012 (переглядається)**	Безпека мережі. Частина 2: Вказівки щодо проектування та впровадження мережевої безпеки
ISO/IEC 27033-3	**2010 (переглядається)**	Безпека мережі. Частина 3: Довідкові сценарії мережевої роботи. Загрози, методи проектування та проблеми управління
ISO/IEC 27033-4	**2014 (переглядається)**	Безпека мережі. Частина 4: Забезпечення зв'язку між мережами за допомогою шлюзів безпеки
ISO/IEC 27033-5	**2013 (переглядається)**	Безпека мережі. Частина 5: Захист зв'язку по мережах за допомогою віртуальної приватної мережі (VPN)
ISO/IEC 27033-6	**2016**	Безпека мережі. Частина 6: Забезпечення доступу до бездротової мережі IP
ISO/IEC 27034-1	**2011 (переглядається)**	Захист програм. Частина 1: Огляд та концепції
ISO/IEC 27034-2	**2015**	Захист програм. Частина 2: Нормативна база організації
ISO/IEC 27034-3	**2018**	Захист програм. Частина 3: Процес управління безпекою додатків
ISO/IEC 27034-4	**У стадії розробки**	Захист програми. Частина 4: Валідація та перевірка
ISO/IEC 27034-5	**2017**	Захист програм. Частина 5: Структура даних управління протоколами та безпекою програм
ISO/IECTS 27034-5-1	**2018**	Захист програм. Частина 5-1: Структура даних управління протоколами та безпекою програм, XML-схеми
ISO/IEC 27034-6	**2016**	Захист додатків. Частина 6: Приклади
ISO/IEC 27034-7	**2018**	Захист додатків. Частина 7: Рамка прогнозування достовірності

ISO/IEC 27035-1	**2016 (переглядається)**	Управління інцидентами інформаційної безпеки - Частина 1: Принципи управління інцидентами
ISO/IEC 27035-2	**2016 (переглядається)**	Управління інцидентами інформаційної безпеки. Частина 2: Вказівки щодо планування та підготовки до реагування на інцидент
ISO/IEC 27035-3	**У стадії розробки**	Управління інцидентами в галузі інформаційної безпеки. Частина 3: Настанови щодо операцій з реагування на інциденти ІКТ
ISO/IEC 27036-1	**2014 (переглядається)**	Інформаційна безпека відносин з постачальником. Частина 1: Огляд та поняття
ISO/IEC 27036-2	**2014 (переглядається)**	Інформаційна безпека відносин з постачальником. Частина 2: Вимоги
ISO/IEC 27036-3	**2013 (переглядається)**	Інформаційна безпека відносин з постачальником. Частина 3: Настанови щодо безпеки ланцюга поставок інформаційних та комунікаційних технологій
ISO/IEC 27036-4	**2016**	Інформаційна безпека відносин з постачальником. Частина 4: Настанови щодо безпеки хмарних послуг
ISO/IEC 27037	**2012 (переглядається)**	Настанови щодо ідентифікації, збору, придбання та збереження цифрових дока
ISO/IEC 27038	**2014 (переглядається)**	Специфікація для цифрового редагування
ISO/IEC 27039	**2015**	Вибір, розгортання та експлуатація систем виявлення та запобігання вторгнень (IDPS)
ISO/IEC 27040	**2015**	Безпека зберігання
ISO/IEC 27041	**2015**	Керівництво щодо забезпечення придатності та адекватності методу розслідування інцидентів

ISO/IEC 27042	**2015**	Вказівки щодо аналізу та інтерпретації цифрових доказів
ISO/IEC 27043	**2015**	Принципи та процеси розслідування інцидентів
ISO/IEC 27045	**У стадії розробки**	Велика безпека та конфіденційність даних - процеси
ISO/IEC 27050-1	**2016 (переглядається)**	Електронне відкриття. Частина 1: Огляд та концепції
ISO/IEC 27050-2	**2018**	Електронне відкриття. Частина 2: Керівництво для управління та управління електронним виявленням
ISO/IEC 27050-3	**2017 (переглядається)**	Електронне відкриття. Частина 3: Кодекс практики електронного виявлення
ISO/IEC 27050-4	**У стадії розробки**	Електронне відкриття. Частина 4: Технічна готовність
ISO/IEC 27070	**У стадії розробки**	Вимоги до встановлення віртуалізованих коренів довіри
ISO/IEC 27071	**У стадії розробки**	Рекомендації з безпеки щодо встановлення надійного зв'язку між пристроєм та службою
ISO/IEC 27099	**У стадії розробки**	Інфраструктура публічних ключів - Практика та рамки політики
ISO/IEC TS 27100	**У стадії розробки**	Кібербезпека - огляд та концепції
ISO/IEC TS 27101	**У стадії розробки**	Кібербезпека - керівні принципи розвитку рамок
ISO/IEC 27102	**2019**	Вказівки щодо кіберстрахування
ISO/IEC TR 27103	**2018**	Кібербезпека та стандарти ISO та IEC
ISO/IEC TR 27550	**2019**	Інжиніринг конфіденційності для процесів життєвого циклу системи

ISO/IEC 27551	**У стадії розробки**	Вимоги до аутентифікації на основі атрибутів, що не пов'язані між собою
ISO/IEC 27553	**У стадії розробки**	Вимоги безпеки для аутентифікації з використанням біометричних даних на мобільних пристроях
ISO/IEC 27554	**У стадії розробки**	Застосування ISO 31000 для оцінки ризику, пов'язаного з управлінням особистістю
ISO/IEC 27555	**У стадії розробки**	Встановлення концепції видалення ІПІ в організаціях
ISO/IEC 27556	**У стадії розробки**	Настанова, орієнтована на користувачів, для обробки персонально ідентифікованої інформації (PII) на основі переваг конфіденційності
ISO/IEC 27570	**У стадії розробки**	Правила конфіденційності для смарт-міст
ISO/IEC 27701	**2019**	Розширення до ISO / IEC 27001 та ISO / IEC 27002 щодо управління інформацією про конфіденційність - Вимоги та рекомендації
ISO 27799 *	**2016**	Інформатика в галузі охорони здоров'я - Управління інформаційною безпекою в галузі охорони здоров'я з використанням ISO / IEC 27002

** Міжнародні стандарти не мають тієї ж загальної назви, але також є частиною сімейства стандартів ISO / IEC 27000.*

1.2 Виникнення стандарту якості ISO/IEC 27001:2021

Інформація – це певний об’єм змістовних даних різної структури, форми прояву й походження. Через те, що інформація стала важливим активом в сучасному світі, то загроза безпеки інформації може створити надзвичайно серйозні, іноді й глобальні, проблеми, які потрібно вирішувати дуже швидко і ефективно, адже розповсюдження інформації схоже на вірус, що розповсюджується повітрям та не тільки, який складно стримати та локалізувати.

В практичному використанні часто застосовують комбінацію вимог до системи захисту інформації.

ISO/IEC 27001 — це стандарт безпеки, який формально визначає систему управління інформаційною безпекою (ISMS), яка призначена для забезпечення безпеки інформації під чітким управлінським контролем. Як формальна специфікація, вона передбачає вимоги, які визначають, як впроваджувати, контролювати, підтримувати та постійно вдосконалювати СУІБ. Він також визначає набір найкращих практик, який включає вимоги до документації, розподіл відповідальності, доступність, контроль доступу, безпеку, аудит, а також коригувальні та запобіжні заходи. Сертифікація за стандартом ISO/IEC 27001 допомагає організаціям виконувати численні нормативні та законодавчі вимоги, які стосуються безпеки інформації [4].

1995 рік – BSI (British Standards Institution) видає міжнародний стандарт BS 7799, який розроблявся для впровадження ISMS у відповідні компанії. Але цей стандарт не спрямовувався на виконання оцінки ризику. Через це він став лише початковим рівнем системи захисту інформації та прототипом для стандартів, які забезпечуватимуть безпечне управління інформацією.

1998–1999 рр. – був переглянутий стандарт BS 7799 та в подальшому розширений до другої частини (BS 7799–1:1998), його занесли до системи міжнародних стандартів ISO без змін. Це стало основою для створення наступного стандарту.

2000 рік – опубліковано стандарт якості ISO/IEC 17799.

2002 рік – було видано стандарт BS7799–2: 2002, що був створений на основі його попередника BS 7799-2:1999 – Специфікація інформаційної системи управління безпеки. Стандарт переглянули та видали з доповненнями для узгодження його з міжнародним стандартом якості ISO 9001:2015 (система управління якістю) й ISO 14001 (система управління навколишнім середовищем), а також для введення циклу PDCA.

2005 рік – опубліковано стандарт якості ISO/IEC 27001, який мав за основу положення й вимоги стандарту BS 7799–2: 2002. В цьому ж році було видано

стандарт BS 7799-3, який ліг в основу ISO версії ISO/IEC 27005 – Управління інформаційною безпекою системи – рекомендації щодо ризику інформаційної безпеки управління. Даний стандарт в своїй основі несе рекомендації до реалізації вимог щодо управління ризиками та відповідної діяльності, що викладені в стандарті ISO/IEC 27001: 2005. Він являється відносно загальним для того, щоб компанії різного розміру могли його використовувати [1, 2].

У зв'язку з розвитком інформаційних технологій збільшується й кількість вимог, які забезпечуватимуть захист ІТ. В результаті таких змін стандарт ISO/IEC 27001:2005 був розглянутий та удосконалений до ISO/IEC 27001:2013, а потім ISO/IEC 27001:2021.

Зміни в структурі стандарту якості можна спостерігати в таблиці 1.2. Згідно вище вказаних даних, можна зробити висновок, що кількість обов'язкових положень у новій версії стандарту зросла.

Ряд поповнень та змін в стандарті ISO/IEC 27001:2021 свідчать про важливість розвитку систем менеджменту інформаційної безпеки та необхідність приділяти більше уваги саме інформаційній безпеці [5].

Таблиця 1.2

Порівняльна таблиці стандартів ISO/IEC 27001:2005 та ISO/IEC 27001:2021

ISO/IEC 27001:2005	ISO/IEC 27001:2013
0. Вступ	0. Вступ
1. Область застосування	1. Область застосування
2. Нормативні посилання	2. Нормативні посилання
3. Терміни та визначення	3. Терміни та визначення
4. Система інформаційної безпеки (50)	4. Контекст організації (8)
5. Зобов'язання керівництва (18)	5. Лідерство (19)
6. Внутрішні аудити (4)	6. Планування (39)
	7. Підтримка (28)
	8. Операції (Експлуатація) (9)

2.2 Загальна інформація про стандарт якості ISO/IEC 27001

2.2.1 Структура стандарту

Один із перших та ключових стандартів із сімейства стандартів якості ISO/IEC 27000 став ISO/IEC 27001 – міжнародний стандарт з інформаційної безпеки, який містить вимоги для покращення систем управління безпекою будь-яких інформаційних ресурсів та ІТ.

Цей документ має таку структуру:

- Передмова
- Вступ
- Сфера додатку
- Нормативні посилання
- Терміни та визначення
- Система управління інформаційною безпекою
- Відповідальність керівництва
- Внутрішня перевірка СУІБ
- Аналіз СУІБ зі сторони керівництва
- Покращення СУІБ
- Додаток А (обов’язковий) Цілі та засоби управління

- Додаток В (інформаційний) Принципи ОЕСР (організація економічного співробітництва та розвитку) та цей міжнародний стандарт
- Додаток С (інформаційний) Відповідність між ISO 9001:2000, ISO 14001:2004 та цим міжнародним стандартом
- Бібліографія

В 2021 році Міжнародна організація із сертифікації розробила, прийняла та опублікувала оновлену версію стандарту якості ISO/IEC 27001:2021. В оновленій версії була частково змінена структура стандарту та її вимоги.

Оновлена структура стандарту має наступний вигляд:

- Вступ
- Сфера застосування
- Нормативні посилання
- Терміни та визначення
- Контекст організації
- Лідерство
- Планування
- Підтримка
- Операція (Експлуатація)
- Оцінка ефективності
- Удосконалення (Покращення)
- Додаток А (обов'язковий) Цілі та засоби управління
- Додаток В (інформаційний) Принципи ОЕСР (організація економічного співробітництва та розвитку) та цей міжнародний стандарт
- Додаток С (інформаційний) Відповідність між ISO 9001:2015, ISO 14001:2015 та цим міжнародним стандартом
- Бібліографія

В Додатку «А» оновленої версії стандарту з'явились нові розділи:

- «А. 10 Криптографія»;
- «А. 13 Безпека комунікацій»;
- «А. 15 Взаємовідносини з постачальниками».

Також, до Додатку «А» було додано ряд нових вимог:

- А.6.1.4 Інформаційна безпека в управлінні проектами;
- А.12.6.2 Обмеження щодо встановлення програмного забезпечення;
- А.14.2.1 Політика безпечної розробки;
- А.14.2.5 Процедури розробки системи;
- А.14.2.6 Безпечне середовище розробки;
- А.14.2.8 Тестування безпеки системи;
- А.15.1.1 Політика інформаційної безпеки для відносин з постачальниками;
- А.15.1.3 Ланцюг постачання інформаційно-комунікаційних технологій;
- А.16.1.4 Оцінка та вирішення подій інформаційної безпеки;
- А.17.1.2 Впровадження безперервності інформаційної безпеки;
- А.17.2.1 Наявність засобів обробки інформації [6].

Дана версія стандарту якості інформаційної безпеки ISO/IEC 27001:2021 діє до сьогодні.

2.2.2 Впровадження стандарту в інформаційну систему

Наявність системи управління безпекою інформації на певному підприємстві дозволяє зрозуміти здатність та серйозність захисту відповідних інформаційних ресурсів. Ця система повинна використовуватися в будь-яких організаціях, що працюють з будь-якими масивами даних, особливо у випадку роботи з персональними даними клієнтів (споживачів) та робітників [7, 9].

Стандарт ISO 27001 визначає ряд наступних заходів, спрямованих на систему управління інформаційною безпекою:

- впровадження;
- функціонування;
- моніторинг;
- аналіз;
- підтримку;
- покращення.

Стандарт ISO 27001 певною мірою гармонізований та містить подібні до стандарту ISO 9001 вимоги. Відповідно підприємства, що розробляють системи менеджменту інформаційної безпеки, можуть також розробити та впровадити інтегровану систему, що відповідає вимогам стандартів ISO 27001 та ISO 9001.

Сертифікацію за стандартом ISO 27001:2021 проводять Органи сертифікації, які акредитовані національними акредитаційними організаціями. В Україні такою державною організацією з 2002 року є Національне агентство з акредитації України (НААУ). Під час акредитації НААУ керується рекомендаціями міжнародних організацій ILAC IAF та регіональної ЕА організацій з акредитації.

Процес сертифікації за ISO 27001:2021 включає наступні етапи робіт:

1. Розробка необхідного пакету документів та впровадження СУІБ на підприємстві.

2. Укладання договору з Органом сертифікації на проведення сертифікаційного аудиту на відповідність СУІБ вимог стандарту ISO.

3. Проведення діагностики групою аудиторів ключових документів системи управління інформаційної безпеки Замовника.

4. Детальний, глибокий аудит, включаючи тестування впроваджених заходів та оцінка їх ефективності.

5. Проведення сертифікаційного аудиту СУІБ на відповідність вимогам стандарту ISO.

6. Оформлення документів та видачу сертифіката з обов'язковою реєстрацією в єдиному реєстрі Органу сертифікації.

Сертифікація системи управління інформаційною безпекою на підприємстві згідно стандарту ISO 27001 надає підприємству ряд вагомих пріоритетів:

- побудова надійної структури ІБ;
- захищеність бази даних та інформації про інтелектуальну власність;
- захист від фінансових втрат та погіршення репутації, що пов'язано з дискредитацією даних;

- надійна довіра інвесторів;
- забезпечення мінімізації кібератак;
- перевага серед конкурентів на загальному ринку;
- зростання рівня довіри з боку партнерів та споживачів;
- розширює ринки надання послуг;
- надає можливість використовувати знак сертифікації у рекламних цілях;
- забезпечує пріоритети при укладанні міжнародних контрактів з іноземними компаніями [7, 8, 10].

2.2.3 Впровадження стандарту на території України

В Україні у 2014 році було ухвалено стандарт ДСТУ ISO 27001:2014 «Інформаційні технології, Методи безпеки. Системи менеджменту інформаційної безпеки. Вимоги.», який фактично є перекладеною копією стандарту ISO 27001:2021 [7]. Стандарт був прийнятий у зв'язку з домовленостями між Україною та Європейським союзом, які були ухвалені під час підписання угоди про асоціацію. До ратифікації угоди, стандарт ISO/IEC 27001 використовувався лише галузевими організаціями та компаніями.

При цьому міжнародні договори укладені Україною є частиною національного законодавства.

На Україні здійснювалась сертифікація саме за ISO/IEC 27001 в таких сферах державного регулювання:

- Енергетична;
- Промислова;
- Будівництво;
- Банківська сфера.

Однією з перших організацій України, сертифікованих за стандартом ISO/IEC 27001, був Національний Банк України, який ще з 1998 року використовував вимоги, що відповідали цьому стандарту [10].

В ході розвитку нашої держави було запроваджено значну кількість стандартів, що представляли собою перекладений на українську мову варіанти міжнародних стандартів ISO/IEC 27k. Це здійснювалось з метою створення більш прозорого середовища співпраці з багатьма іншими країнами у різних сферах.

До сьогодні держава має за мету запроваджувати як найбільше галузевих стандартів ISO/IEC 27k на основі ДСТУ. Також, поширювати впровадження стандарту ISO/IEC 27001 в приватні та державні сектори. Такі рішення зумовлені розвитком інформаційних технологій та поширенням цифрових джерел інформації, які обов'язково повинні підпорядковуватися правилам системи управління інформаційних технологій та вимогам стандарту ISO/IEC 27001, який підвищує надійність СУІБ у будь-якій сфері [7, 10].

Вдосконалення системи управління інформаційною безпекою являється актуальним у зв'язку зі швидким розвитком та поширенням інформаційних технологій на території України. Також, сертифікація різного роду діяльності держави за міжнародними стандартами свідчитиме, в першу чергу, про якість інформаційної безпеки України, що в подальшому надаватиме їй певні переваги в сертифікованих сферах діяльності серед багатьох інших країн, а також, особливо, для звичайних громадян України.

2.3. Принцип роботи стандарту якості ISO/IEC 27001 в системі інформаційних технологій.

ISO/IEC 27001 – міжнародний стандарт управління інформаційною безпекою, який передбачає порядок впровадження незалежно оцінюваної та сертифікованої системи менеджменту інформаційної безпеки. Застосування даної системи дозволяє забезпечити ефективний захист усіх фінансових та конфіденційних даних та мінімізувати ймовірність неправомірного доступу до них.

Наявність сертифікату ISO/IEC 27001 дає зрозуміти, що ефективність роботи певної компанії відповідає міжнародним стандартам якості. Це зіграє

позитивну роль на впевненості постачальників, акціонерів та інвесторів у тому, що ця компанія повною мірою забезпечує захист всього об'єму своїх даних.

Переваги, що надає цей стандарт компанії, наступні:

- можливість виявлення ризиків та запровадження заходів щодо їх оптимізації чи усунення;
- гнучкість адаптації інструментів до будь-яких областей діяльності;
- довіра з боку зацікавлених осіб та клієнтів завдяки забезпеченому захисту даних;
- відповідність стандартам гарантує статус привілейованого постачальника;
- задоволеність споживачів завдяки відповідності вимогам стандартів [11].

Управління інформаційною безпекою дає підприємствам малого і середнього бізнесу (МСБ) впевненість у забезпеченні міцної та надійної основи для зростання.

Малі підприємства, що впроваджують стандарт ISO/IEC 27001, мають можливість досягти успіху, який можна порівняти з успіхом більших компаній. Впровадження вимог до системи управління інформаційною безпекою відповідно до стандарту ISO/IEC 27001, забезпечить повний захист інформаційної незалежності компанії та мінімізацію незаконних зазіхань на неї [12].

РОЗДІЛ ІІ. ХАРАКТЕРИСТИКА ПІДПРИЄМСТВА

2.1 Характеристика підприємства

Об'єктом дослідження в дипломній роботі є ФОП "Почерпайло Андрій Андрійович".

Повне найменування юридичної особи - ФІЗИЧНА ОСОБА-ПІДПРИЄМЕЦЬ ПОЧЕРПАЙЛО АНДРІЙ АНДРІЙОВИЧ.

Код ЄДРПОУ – 2650190047 86.

Дата реєстрації - 09.01.2019 (3 роки 8 місяців).

Організаційно-правова форма - фізична особа-підприємець.

Форма власності - недержавна власність.

Адреса: місто Київ, Голосіївський район, вулиця Ломоносова, будинок 58а.

Види діяльності:

Основний:

- Комп'ютерне програмування

Інші:

- Розробку структури та контенту, необхідних для створення та створення та виконання програмного забезпечення.
- Консультації з питань інформатизації.
- Консультації стосовно виявлення ризиків у процесі розробки програмного забезпечення.
- Запровадження заходів щодо оптимізації чи усунення ризиків які виявленні в уже готовому програмному забезпеченні чи під час створення програмного забезпечення.
- Консультації з питань дотримання безпекових стандартів під час розробки програмного забезпечення.
- Запровадження заходів щодо дотримання безпекових стандартів під час розробки програмного забезпечення.

Всі співробітники ФОП працюють віддалено, за потреби можуть користуватися коворкінгом чи іншим місцем роботи, яке відповідає вимогам які затверджені підприємством та погоджені з замовником. Також часто замовники можуть надати співробітникам підприємства можливість працювати у власних виробничих приміщеннях. Це дозволено, оскільки за замовчуванням припускається що виробничі приміщення фірми відповідають стандартам інформаційної безпеки які вимагаються власне самим замовником.

Далі буде розглянуто два варіанти приміщень які використовувалися співробітниками підприємства під час роботи:

- власний офіс однієї з фірм замовника
- коворкінг який обрали співробітники для роботи

Власний офіс однієї з компаній замовника. Через особливості згоди по не розголошенню даних про співпрацю у дипломній роботі не можна розголошувати назву, інформаційну систему компанії та міри захисту які не відносяться до взаємодії співробітників ФОП «Печерпайло Андрій Андрійович» та наданих приміщень замовника.

Приміщення офісу компанії замовника було розбито між двома будівлями які між собою були з'єднані відкритим на закритим переходом. Підприємство замовника займає по 1 поверху у двох 5-ти поверхових офісних будинках. Схема розташування об'єктів на території підприємства представлена на малюнку 2.1.

Рис. 2.1 - Схема розташування об'єктів на території підприємства замовника

Підприємство займає 2 окремих офіси загальною площею приблизно 500 квадратних метрів. На першому поверсі будівлі знаходиться кафетерій з інтернет доступом, який спільний для всіх співробітників офісного центру. Чисельність комп'ютерів, ноутбуків, планшетів, тестових девайсів та серверного обладнання приблизно 350 штук.

Територія, на якій розташоване підприємство, велика, з окремою відкритою парковкою та критим паркінгом для потреб співробітників офісу. Доступ до приміщень можна здійснити через окремі вхідні двері з вулиці або з ліфту. Всі двері контролюються охоронцями, а доступ можна отримати за ключ картою. Ключ карта має бути присутня при співробітнику весь час перебування на території підприємства. На карті є фотографія, ПІО та посада співробітника для ідентифікації особи.

Коворкінг що був обраний співробітниками для зручності роботи поза домом та офісами компаній замовника. Коворкінг "BeeWorking" займає 5 поверхів будівлі у спальному районі міста Києва, загальна площа приміщень коворкінгу 5000 кв. метрів. Схема розташування об'єктів на території підприємства представлена на малюнку 2.2.

Рис. 2.2 - Схема розташування коворкінгу на території ЖК "Сонячна Брама"

Підприємство немає іншої відкритої території окрім як приміщень коворкінгу. Доступ до приміщень можна здійснити через окремі вхідні двері з вулиці. Всі двері контролюються охоронцями та працівниками рецепції коворкінгу, доступ до спільних приміщень коворкінгу є у всіх відвідувачів. Проте для орендарів окремих приміщень можливий додатковий рівень захисту. Доступ до таких приміщень здійснюється за допомогою ключ карти яку можна отримати на рецепції.

2.2 Аналіз діючої інформаційної системи

Інформаційна система підприємства ФОП "Почерпайло Андрій Андрійович" є розробленою під певні цілі низка засобів та особистих доступів

персоналу. Ця система використовується для найшвидшого, якісного та безпечного реагування на побажання замовника і надання спеціалістам відповідних умов для виконання поставлених задач у відповідності з цінностями вище.

У кожного фахівця компанії є можливість відвідувати коворкінги або працювати вдома, в залежності від потреб та умов створених для кожного спеціаліста.

Основним робочим девайсом у компанії є портативний персональний комп'ютер. Це рішення продиктоване тим, що для роботи спеціаліст може обирати місце роботи в залежності від умов в яких він знаходиться. На комп'ютери встановлений комплект програмного забезпечення. Склад типового робочого місця фахівця та перелік встановленого програмного забезпечення представлений в таблиці 2.1.

Таблиця 2.1

Надане програмне та апаратне забезпечення фахівця компанії

ФОП «Почернайло Андрій Андрійович»

Назва системи	**Назва компоненту**	**Кількість**
Персональний комп'ютер основний	Apple MacBook Pro 16" 2021	1
Персональный комп'ютер для тестування на більш старих операційних системах №1	Apple MacBook Pro 15" 2019	1
Персональный комп'ютер для тестування на більш старих операційних системах №2	Apple MacBook Pro 13" Early 2015	1

Персональный комп'ютер для тестування на більш старих операційних системах №3	Apple MacBook Air 13" Early 2014	1
Програмне забезпечення для роботи з базами даних	TablePlus version 4.8.8	1
Програмне забезпечення для роботи з перехопленням та зміни HTTP запитів	ProxyMan version 3.11.0	1
Програмне забезпечення для захищеної комунікації з замовниками та іншими співробітниками	Zoom version 5.11.6	1

Для роботи у коворкінгу передбачена можливість мати з собою лише 1 з комп'ютерів передбачених для виконання зазначених задач. Всі інші надані працівнику пристрої мають зберігатися у сейфі (якщо він живе з іншими людьми) або у закритій квартирі (якщо він живе сам).

Вся необхідна інформація для працівника знаходиться на хмарних сховищах. Доступ до цих сервісів захищений такими структурами захисту:

- двофакторна аутентифікація;
- унікальний пароль для кожного сервісу який відповідає вимогам NIST класифікації складності пароля;
- доступ до всіх сервісів можливий лише за підключенням до внутрішнього VPN сервісу компанії;
- підключення до VPN сервісу можливе лише за наявності персонального логіну та паролю співробітника.

Приблизна схема доступу зображена на малюнку 2.1.

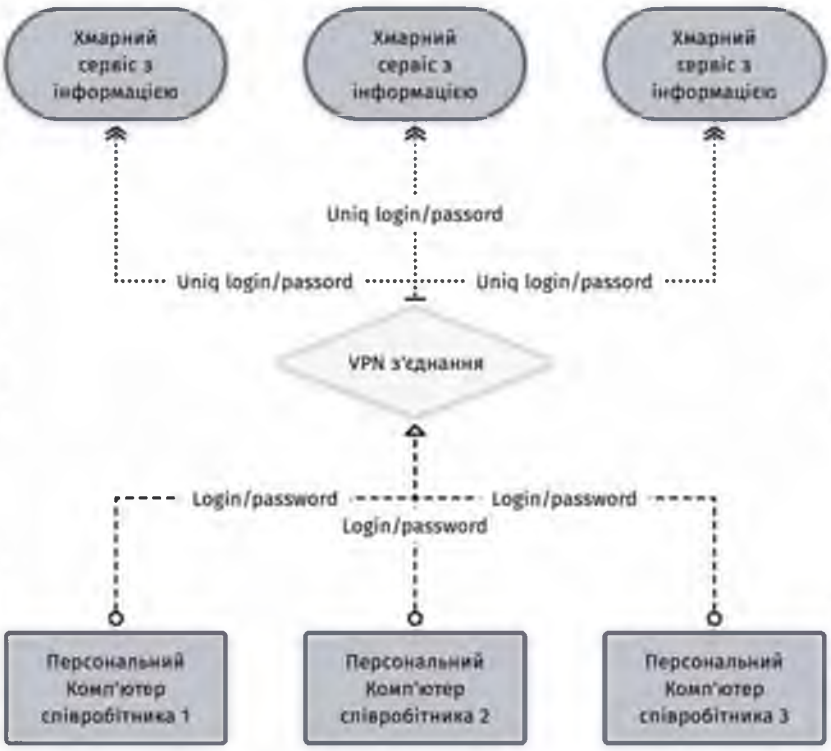

Рис. 2.1 - Приблизна схема доступу до хмарних сховищ ФОП "Почерпайло Андрій Андрійович"

Назви та специфікація основних сервісів які доступні співробітникам зазначені в таблиці 2.2. Також варто доповнити що в залежності від умов замовника або за наявності більш жорстких специфікацій сервіси можуть змінюватись на аналогічні з вищим або нижчим рівнем безпеки на шифрування даних.

Хмарні сервіси мають свої переваги і недоліки, якщо порівнювати з локальною мережею та локальними серверами. Переваги у швидкості та доступності до інформації Недоліками є менша фізична захищеність засобів зберігання інформації та потреба звертатися до третіх сторін, а саме провайдерів хмарних сервісів.

Таблиця 2.2

Сервіси з хмарного зберігання інформації для співробітників підприємства ФОП "Почерпайло Андрій Андрійович"

Назва сервісу	Призначення	Аналоги
GitHub	Сервіс для зберігання програмного коду та налаштуванню співпраці між співробітниками ФОП та замовника	GitLab, BitBucket
Postman	Сервіс для зберігання документації щодо HTTP запитів та виконання їх	Charles, Curl
Figma	Сервіс для зберігання інформації у графічному вигляді (графіки, макети дизайну, діаграми)	Sketch
Confluence	Сервіс для зберігання інформації у текстовому вигляді	Notion
Amazon S3	Сервіс для зберігання даних логування та ресурсів для побудови веб застосунків	DeNova, Microsoft Blobs Storage

Загалом співробітники підприємства можуть мати доступ до всієї необхідної бази знань яка вже розроблена іншими співробітниками раніше, так і до даних які надає замовник на сервісах які вже використовуються, або їх аналоги. Співробітники мають усі необхідні навички для роботи з аналогами вищезгаданого програмного забезпечення. Також важливими є два фактори: співробітники можуть отримати доступ до будь яких ресурсів через VPN та авторизацію. Це полегшує обмін даними між девайсами, що позитивно впливає на швидкість роботи.

Під час втрати контролю (програмного або фізичного) над девайсом є можливість деактивувати всі сесії користувача на конкретному харварному пристрої.

Програмне забезпечення ФОП "Почерпайло Андрій Андрійович" включає сукупність програм для реалізації цілей і завдань інформаційної системи, пов'язаних з основною діяльністю компанії, а також нормального функціонування комплексу технічних засобів.

Системне програмне забезпечення комп'ютерів представлено в таблиці 2.3.

Таблиця 2.3

Основне системне програмне забезпечення

ФОП “Почерпайло Андрій Андрійович”

Найменування	**Кількість**
MacOs Monterey 12.4	2
MacOs Sierra 10.12	1
MacOs Catalina 10.15	1
MacOs Big Sur 11.6	1
Архіватор The Unarchiver	5

Така кількість систем зумовлена тим, що у співробітників присутні декілька моделей девайсів, що вказано у таблиці 2.1. Також варто зазначити що на одному фізичному девайсі може знаходитися більше ніж одна операційна система для зручності співробітника. У більшості випадків для повноцінної роботи співробітнику достатньо мати до двох-трьох фізичних девайсів. Проте іноді виникають ситуації які потребують знаходження на 1 фізичному девайс 1 операційної системи і певного набору допоміжних програм.

Загалом співробітники можуть працювати напряму з кодом у відповідних редакторах. Перелік редакторів та відповідні мови програмування наведені у таблиці 2.4.

Таблиця 2.4

Перелік редакторів та відповідні їм мови програмування

Назва та стабільна версія	**Мови Програмування**

PyCharm 2022.2	Python (primary) Html, JavaScript, TypeScript
PhpStorm 2022.1.3	JavaScript (primary), PHP (primary), TypeScript (primary)
XCode 13.4.1	Swift (primary) Objectiye C

Кожен з наведених редакторів є захищеною структурою, яка дозволяє взаємодіяти з програмним кодом, редагувати на запускати його. Також є можливість налаштувати синхронізацію з деякими з хмарних сервісів, наприклад з GitHub, що суттєво полегшує роботу на прискорює швидкість виконання задач.

Для співробітників які працюють в коворкінгу є заборона на роботу більше ніж на одному пристрої. Проте за потреби людина може обирати більш зручне місце робости.

2.3. Організаційні заходи забезпечення інформаційної безпеки і захисту інформації підприємства

2.3.1 Підхід до аналізу ризиків

Підприємству для повноцінної роботи потрібна постійна наявність та доступ до інформаційних активів. В рамках роботи компанії актив це власність компанії, що має для неї певну цінність. Як результат, підприємство зацікавлене в захисті своїх активів.

Для проведення аналізу та оцінки ризиків, що пов'язані з імовірною реалізацією загроз та інформаційної безпеки підприємства, які можуть призвести до порушення конфіденційності, цілісності та доступності активів буде використана методика оцінки ризиків до інформаційної системи підприємства. Як кінцевий артефакт роботи за методологією повинна бути отримана кількісна оцінка ризиків. Оцінка отриманим ризикам виставляється у чисельних одиницях.

Після закінчення аналізу ризиків повинно бути проведене ранжирування факторів між собою, задля визначення рівня прийнятного ризику.

Аналіз ризиків інформаційної безпеки - це процес комплексної оцінки захищеності конкретного активу компанії від ймовірної реалізації загроз порушення конфіденційності, цілісності та доступності активів. Отже, одним з перших пунктів у дослідженні має бути саме визначення які активи зараз знаходяться у власності або розпорядженні компанії. Зазначимо, що для підприємства також важливо провести аналіз активів які надаються для роботи третіми сторонами (замовник, підрядник чи підприємство-партнер).

2.3.1 Визначення активів підприємства

Під час оцінки вже налагоджених процесів які використовуються під час роботи у підприємстві, разом з власниками та користувачами активів були ідентифіковані такі категорії активів:

- інформаційні активи у електронному вигляді
- інформаційні активи у не-електронному вигляді
- людські ресурси
- обладнання
- програмне забезпечення
- внутрішній бренд роботодавця, зовнішня репутація компанії
- послуги з обслуговування та сервіси, які закуповуються у третіх сторін

Класифікація не є жорсткою, оскільки активи можуть об’єднуватися у групи. Наприклад програмно-технічний комплекс, іт-сервіс чи інше. Основними компонентами у таких об’єднаннях можуть бути сукупності різних активів, як однієї категорії, так і різних. Наприклад сукупність обладнання, ПО чи інформаційних активів.

Варто описати положення методики яка використовувалась для оцінки цінності активу для компанії. Загальна цінність актива визначалась у відповідності з ступенем взаємодії на діяльність компанії, її замовників, партнерів, підрядників. Основним чинником оцінки є ймовірність реалізації

загрози для інформаційної безпеки конкретного активу чи групи активів, що призводить до порушень їх конфіденційності, цілісності та доступності.

Цінність активу визначається його власником, при потребі залучається людина яка була причетна до надання доступу чи створенню активу та експерти з питання інформаційної безпеки. Цінність визначається виходячи з кожної конкретної області застосування активу в якій він використовується чи існує. Для більш незалежної оцінки всі сторони що приймають участь у оцінці створюють незалежні звіти, потім за цими звітами приходять до середньої оцінки для більшої об'єктивності дослідження. Важливим аспектом є те, що за сильної розбіжності між оцінками ризиків одного і того самого актива рекомендовано проводити зустрічі обговорення, під час яких всі сторони пробують дійти до більш однорідної оцінки.

2.3.1 Критерії визначення цінності активу

У відповідності до стандарту ISO 27001, цінність активу встановлюється пропорційно до загрози які несе можлива для компанії, партнерів чи замовників втрата цілісності активу.

- Інформаційні активи у електронному та не-електронному вигляді

Можлива шкода визначається як безпосередньо як наслідок розкриття, модифікації чи втрати доступу до інформаційного активу. У рамках підприємства це в основному саме інформаційні активи у електронному вигляді, проте зустрічаються і активи у не-електронному вигляді.

- Обладнання, програмне забезпечення та IT-сервіси

Можлива шкода визначається по впливу на конфіденційність, цілісність та доступність інформаційних активів, які зберігаються, обробляються чи захищаються за допомогою використання цього активу, з розрахунком вартості відновлення цілісності чи доступності конкретного інформаційного активу та беручи до уваги ціну на простій спеціаліста чи техніки під час втрати можливості працювати або з інформаційними активами або з конкретним обладнанням.

Загроза активів цих типів виражається у неможливості виконувати покладені на конкретний пристрій чи програмне забезпечення функції. Це може відбуватися за рахунок помилок, пошкоджень, відмов та інших можливих перешкод. Ці ризики відбуваються за рахунок реалізації загрози інформаційної безпеки.

- Людські ресурси

Можлива шкода визначається по впливу втрати конфіденційності, цілісності та доступності інформаційних ресурсів які використовуються чи обробляються персоналом та за вартістю відновлення КЦД характеристик цього активу.

Загроза цього активу може визначатися в неможливості компетентно, якісно чи повністю виконувати персоналом посадові обов'язки, втрати відповідної компетенції у питаннях та інше.

- внутрішній бренд роботодавця, зовнішня репутація компанії

Оцінюється можлива шкода для зовнішньої репутації компанії, за рахунок втрати певної цілісності певних активів. Також варто зауважити, що треба розглядати також внутрішній бренд роботодавця, як важливий актив що дозволяє ефективно працювати існуючому персоналу та прикладати меньше зусиль для залучення спеціалістів у компанію з ринку праці.

- Зовнішні сервіси

Визначається сукупна шкода для бізнесу компанії у разі погіршення рівня, відсутності чи недоступності такого сервісу.

2.4. Визначення рівнів ризиків для існуючих активів компанії

2.4.1 Рівні оцінки ризиків для КЦД осних активів

Крім програмного коду працівники також мають справу з багатьма видами інформації, яка зберігається як у електронному вигляді так і на фізичних носіях. Крім того до основних активів підприємства також належать інфраструктура та персонал. Інвентаризації активів на рівні службової діяльності може принести більш змістовну відповідь на питання що саме потрібно захищати, яким чином і якими засобами.

Робочі активи, що мають цінність для компанії і характеризуються певною ступенем вразливості, і мають цінність для зловмисників для заволодіння, зміни або знищення є найпершою вразливістю для компанії. Завдання аналізу ризику полягає у визначенні та оцінці ризиків, яким піддається система інформаційних технологій і її активи, з метою визначення та вибору доцільних і економічно обґрунтованих засобів для створення всіх можливих засобів для забезпечення певного рівня безпеки та сучасних мір реагування для мінімізації ризику.

Для вже ідентифікованих активів типу:

- інформаційні активи у електронному вигляді
- інформаційні активи у не-електронному вигляді
- людські ресурси
- обладнання
- програмне забезпечення
- внутрішній бренд роботодавця, зовнішня репутація компанії
- послуги з обслуговування та сервіси, які закуповуються у третіх сторін

встановлюється роздільні по конфіденційності, цілісності та доступності.

Для зведення оцінок до єдиного рівня використовується найвища оцінка ризику для актива: береться максимум для окремих оцінок шкоди по КЦД для активу. Для активів що відносяться до категорії імдж та бренд роботодавця і послуг з обслуговування та сервіси, які закуповуються у третіх сторін оцінка по кожному конкретній втраті положень КЦД не виводиться, лише визначається фінальна сукупна оцінка ризику Рівні оцінки стосовно ризиків втрати конфіденційності представлені у таблиці 2.6

Таблиця 2.6

Рівні оцінок по конфіденційності

Рівень Оцінки	Опис
1	Немає розкриття конфіденційних документів/даних (що становлять комерційну таємницю чи персональні дані), відсутня шкода

2	Розкриття окремих конфіденційних документів/даних, складових КТ, шкода мінімальна відсутня шкода
3	Розкриття окремих документів/даних складових комерційної таємниці чи персональних даних або сукупності конфіденційних документів/даних, шкода середня
4	Розкриття сукупності конфіденційних документів/даних, можливий негативний вплив на репутацію компанії, можлива зупинка пов'язаних з активами процесів компанії, збитки високі
5	Розкриття сукупності конфіденційних документів/даних, зупинка пов'язаних з активами процесів компанії, негативний вплив на репутацію компанії, збитки дуже високі

За заданими критеріями була проведена оцінка ризиків для попередньо визначених активів компанії. Рівні оцінки приведені у таблиці 2.7.

Таблиця 2.7

Оцінки ризиків вразливості конфіденційності для активів компанії

Актив Компанії	Оцінка
Інформаційні активи у електронному вигляді	5
Інформаційні активи у не-електронному вигляді	5
Людські ресурси	4
Обладнання	3

Програмне забезпечення	5
Внутрішній бренд роботодавця, зовнішня репутація компанії	Н/О
Послуги з обслуговування та сервіси, які закуповуються у третіх сторін	Н/О

Рівні оцінки стосовно ризиків втрати цілісності представлені у таблиці 2.8

Таблиця 2.8

Рівні оцінок по цілісності

Рівень Оцінки	Опис
1	Немає порушення цілісності активів, шкода відсутня
2	Порушення цілісності окремих активів, шкода мінімальна
3	Порушення цілісності окремих або сукупності активів, шкода середня
4	Порушення цілісності сукупності активів, можливий негативний вплив на репутацію компанії, можлива зупинка пов'язаних з активами процесів компанії, збитки високі
5	Порушення цілісності сукупності активів, зупинка пов'язаних з активами процесів компанії, негативний вплив на репутацію компанії, збитки дуже високі

За заданими критеріями була проведена оцінка ризиків для попередньо визначених активів компанії. Рівні оцінки приведені у таблиці 2.9.

Таблиця 2.9

Оцінки ризиків вразливості цілісності для активів компанії

Актив Компанії	Оцінка
Інформаційні активи у електронному вигляді	5
Інформаційні активи у не-електронному вигляді	2
Людські ресурси	4
Обладнання	4
Програмне забезпечення	4
Внутрішній бренд роботодавця, зовнішня репутація компанії	Н/О
Послуги з обслуговування та сервіси, які закуповуються у третіх сторін	Н/О

Рівні оцінки стосовно ризиків втрати доступності представлені у таблиці 2.10

Таблиця 2.10

Рівні оцінок по доступності

Рівень Оцінки	Опис
1	Немає порушення доступності активів, шкода відсутня
2	Порушення доступності окремих активів, шкода мінімальна
3	Порушення доступності окремих або сукупності активів, шкода середня
4	Порушення доступності сукупності активів, можливий негативний вплив на репутацію компанії, можлива зупинка

	пов'язаних з активами процесів компанії, збитки високі
5	Порушення доступності сукупності активів, зупинка пов'язаних з активами процесів компанії, негативний вплив на репутацію компанії, збитки дуже високі

За заданими критеріями була проведена оцінка ризиків для попередньо визначених активів компанії. Рівні оцінки приведені у таблиці 2.11.

Таблиця 2.11

Оцінки ризиків вразливості доступності для активів компанії

Актив Компанії	Оцінка
Інформаційні активи у електронному вигляді	5
Інформаційні активи у не-електронному вигляді	2
Людські ресурси	4
Обладнання	5
Програмне забезпечення	5
Внутрішній бренд роботодавця, зовнішня репутація компанії	Н/О
Послуги з обслуговування та сервіси, які закуповуються у третіх сторін	Н/О

На основі всіх попередньо приведених оцінок була сформована сукупна оцінка ризику для кожного з попередньо визначених активів. Рівні оцінки та ранжування по ступеню ризика приведені у таблиці 2.12.

Таблиця 2.12

Оцінки сукупних ризиків для активів компанії

Актив Компанії	Оцінка
Інформаційні активи у електронному вигляді	5
Інформаційні активи у не-електронному вигляді	5
Обладнання	5
Програмне забезпечення	5
Людські ресурси	4
Послуги з обслуговування та сервіси, які закуповуються у третіх сторін	4
Внутрішній бренд роботодавця, зовнішня репутація компанії	3

В таблиці містяться ризики по найбільш цінних інформаційних активів, та загроз для них, ранжованих в порядку спадання загрози для компанії. Пояснення для високих пріоритетів для втрати доступності у фізичних девайсах є те, що через ці девайси може бути здійснений доступ до майже всієї інформаційної системи підприємства.

У процесі оцінки захищеності активів визначаються загрози, що діють на активи, а також вразливість активів, через які можуть бути реалізовані загрози для інформаційної безпеки компанії. Загрози та вразливості розглядаються лише разом один з одним.

Список вразливостей та загроз щодо активів та/або груп активів компанії формують експерти з інформаційної безпеки та/або відповідальні за процеси роботи з відповідними активами у компанії.

Для визначення вразливостей комп'ютерної мережі можуть бути використані сканери вразливостей, основними завданнями яких є тестування та

діагностика інформаційних систем загалом та окремих її елементів з метою виявлення вразливостей, видача рекомендацій щодо усунення виявлених вразливостей.

2.4.2 Рівні оцінки вірогідності загрози активів

Для повноцінного визначення повноти ризиків для інформаційної системи компанії треба визначити вірогідність реалізації загрози конкретного ризику.

Вірогідність виконання загрози оцінюється експертом з інформаційної безпеки на основі загальноприйнятих практик, власного досвіду та особливостей інформаційної системи компанії. Основними факторами при визначенні вірогідності реалізації загрози є такі параметри, як можлива частота виникнення загрози та простота реалізації загрози.

Оцінка вірогідності лежить у інтервалі від 1 до 5 балів. Критерії для оцінки надані в таблиці 2.13.

Таблиця 2.13

Критерії оцінки вірогідності реалізації загрози

Вірогідність реалізації загрози	Оцінка
Майже неможливо	1
Маловірогідно (до 1 разу в рік), складна реалізація	2
Ймовірно до 1 разу в квартал, середня реалізація	3
Ймовірно до 1 разу в тиждень, більш проста реалізація	4
Ймовірно до 1 разу на добу, дуже проста реалізація	5

Сумарне значення ризику може бути визначене за формулою:

*Ризик = Оцінка сукупних ризиків * вірогідність реалізації загрози*

На основі цієї формули та відповідних оцінок вірогідності реалізації загрози для конкретних активів компанії. Результати оцінки діючої системи безпеки інформації, відображають, наскільки повно виконуються однотипні об'єктивні функції при вирішенні завдань забезпечення захисту інформації (таблиця 2.14).

Таблиця 2.14

Оцінки ризику для активів компанії

Актив Компанії	Оцінка Сукупних Ризиків	Вірогідність реалізації загрози	Сумарний Ризик
Обладнання	5	5	25
Людські ресурси	4	5	20
Інформаційні активи у електроинсму вигляді	5	3	15
Інформаційні активи у не-електронному вигляді	5	2	10
Внутрішній бренд роботодавця, зовнішня репутація компанії	3	3	9
Послуги з обслуговування та сервіси, які закуповуються у третіх сторін	4	2	8
Програмне забезпечення	5	1	5

Після проведення оцінки ризиків проводиться ранжування значень ризиків від більшого до меншого. Ці дані відображаються у попередній таблиці. Неможливість забезпечення повного захисту від ризиків інформаційної безпеки

призводить до встановлення «Прийнятного рівня ризиків», ризики вище якого будуть оброблятися. Для компанії було зроблено висновок, що прийнятний рівень ризику для даних активів це 10 і нижче.

Надані результати оцінки можливих ризиків є підставою для вибору і формулювання завдань щодо забезпечення інформаційної безпеки підприємства, і вибору захисних заходів.

Таким чином, на основі аналізу були запропоновані такі заходи для підвищення рівню безпеки компанії та швидкого реагування на загрозу.

1. Відсутність антивірусного ПО на самих фізичних девайсах.

2. Відсутність можливості віддаленого доступу до фізичних пристроїв співробітників.

3. Відсутність можливості стерти дані з девайсу, коли фізичний доступ до нього втрачено.Результати оцінки діючої системи безпеки інформації, відображають, наскільки повно виконуються однотипні об'єктивні функції при вирішенні завдань забезпечення захисту інформації (таблиця 2.13).

3. Відсутність можливості контролювати точки доступу до мережі інтернет які використовують співробітники.

4. Відсутність єдиного сховища паролей для співробітників.

Всі ці проблеми повинні бути врахованими для подальшого налаштування у інформаційній системі ФОП “Почерпайло Андрій Андрійович”.

Нагально рекомендовано взяти до уваги завдання за загальною оцінкою ризику від більшого до меншого. Крім того, важливо забезпечити комплексний характер захисту.

РОЗДІЛ ІІІ. РОЗРОБКА ЗАХОДІВ ВДОСКОНАЛЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

3.1 Аналіз системи вдосконалення засобів захисту інформації на підприємстві

Політика безпеки має визначатися в офіційному документі, який визначає, що становить прийнятну та неприйнятну поведінку користувачів щодо безпечного поводження з інформаційними активами. Це – частина формального контролю інформаційної безпеки. Політика безпеки зазвичай є документом, який окреслює конкретні вимоги або правила, які повинні бути виконані у сфері інформаційної / мережевої політики безпеки і, як правило, охоплюють окрему сферу діяльності. Організація повинна розглядати наявність політик і процедур інформаційної безпеки так само важливим, як і наявність під рукою технічних рішень.

Одне тільки впровадження таких технічних заходів не гарантує наявність безпечного комп'ютерного середовища. У рамках своїх інструкцій із впровадження організація повинна встановити набір політик інформаційної

безпеки, які затверджуються вищим керівництвом, а потім розповсюджуються серед усіх співробітників.

Людський фактор залишається найслабшою ланкою в ланцюгу інформаційної безпеки, що спричиняє збільшення кількості загроз безпеці. Таким чином, багато кінцевих користувачів досі не усвідомлюють важливості інформаційної безпеки та відповідних організаційних вимог. Успішна реалізація політики інформаційної безпеки пов'язується з проблемами в таких сферах, як політика управління, розповсюдження, обізнаність користувачів і поведінка користувачів. Низка факторів безпосередньо впливає на поведінку користувача щодо політики інформаційної безпеки, і їх можна поділити на людські та організаційні фактори.

Незважаючи на наявність найкращих програм інформування про інформаційну безпеку, існують перешкоди, які ускладнюють успішне впровадження заходів інформування, до яких належать:

- впровадження нових технологій;
- брак організованості справ;
- невиконання подальших дій.

Залежно від застосування та моніторингу політики безпеки, впровадження інструментів моніторингу безпеки може допомогти виявити будь-які порушення політики безпеки, які можуть статися. Однак, ці інструменти моніторингу не мають широкого застосування в організації.

Невідповідність політиці інформаційної безпеки вважається перш за все людською проблемою, а не технічною. Згадуються основні три типи невідповідності: зловмисна поведінка, недбала поведінка та необізнаність.

Основною мотивацією зловмисної поведінки є зловмисний намір завдати шкоди інформаційним активам організації, тоді як недбала поведінка є наміром порушити політику безпеки організації, але не завдати шкоди цій організації [1, с. 147].

Третій тип поведінки без скарг пов`язаний з необізнаністю, через те, що кінцеві користувачі не усвідомлюють важливості інформаційної безпеки та

відповідних організаційних вимог. Користувачі, як правило, не люблять активні елементи керування, які накладаються на їхні ПК. Причина неприязні користувачів до цих елементів керування полягає в тому, що вони накладають групу заборонених команд (наприклад, жодних програм Google, Facebook, Skype тощо).

Існує прямий зв`язок між проблемами, з якими стикається організація, і недостатньою увагою, що приділяється обізнаності та навчанню з інформаційної безпеки. Поінформованість про безпеку та навчання можуть відігравати додаткову роль поряд із політикою інформаційної безпеки, щоб зменшити кількість потенційних внутрішніх загроз.

Незважаючи на те, що дотримання політики безпеки є передусім людською проблемою, організаційні фактори, які, як було виявлено, впливають на відповідність вимогам користувачів. Якість інформації політики безпеки (потік дат) зазвичай розглядається як фактор, який тісно пов'язаний із дотриманням працівниками політики безпеки інформації. Невідповідна політика може негативно вплинути на недотримання вимог. Отже, неадекватні організаційні процедури можуть призвести до браку навичок, знань і здатності справлятися з вимогами безпеки. Якість інформації має значний вплив на фактичну відповідність політиці інформаційної безпеки.

Для заохочення користувачів до дотримання політики інформаційної безпеки можна використовувати мотиватори. Гідним прикладом мотиватора є винагорода, яка визначається як матеріальний або нематеріальний подарунок, який надається працівнику, який відповідає вимогам політики безпеки. Винагороди мають значний вплив на сприйняття працівником переваг дотримання вимог.

Для отримання результату у навчання співробітників була залучена система knowbe4. Детальний опис на особливості застосування можна знайти на сайті розробників пакету програмного забезпечення https://www.knowbe4.com, а також на різноманітних веб сайтів з рекомендаціями щодо застосування або обговоренням отриманих результатів. Завдяки цій системі є можливість

принести у процес навчання геймифікацію та працю заради винагороди. Винагородою у цьому випадку виступають 2 речі: “досягнення” які можуть бачити інші співробітники компанії та зменшення власного ризикового числа, яке вимірюється у відсотках.

Санкції є одним із найважливіших факторів, що впливають на фактичне дотримання працівниками встановленої політики безпеки. Подібним чином вплив санкцій на дотримання працівниками політики інформаційної безпеки полягає у тому, що співробітники будуть дотримуватися політики безпеки, якщо їхні роботодавці будуть готові присоромити тих, хто не зважав на них.

Підвищення обізнаності та навчальні програми впливають на дотримання користувачами політики інформаційної безпеки. Недостатня обізнаність і знання політики могли б дозволити персоналу порушувати принципи визначеної стратегії. Інструменти моніторингу та аудиту безпеки можна використовувати для зміни небажаної поведінки з метою забезпечення виконання політики інформаційної безпеки. Коли користувачі повністю ознайомляться з цими інструментами, їм буде запропоновано змінити свою поведінку та бути більш відповідальними. На відповідність інформаційної безпеки особи впливають інструменти комп'ютерного моніторингу та аудиту. Таким чином, інструменти моніторингу допомагають пом'якшити невідповідність навичок працівників існуючим вимогам.

Переконливі обчислювальні технології можуть вплинути на ставлення людей і призвести до конструктивних змін у багатьох сферах, наприклад, маркетингу, безпеці та навколишньому середовищі. Використання переконливих технологій для розповсюдження політики та процедур може призвести до впровадження ефективних програм інформаційної безпеки.

Досягнення відповідності політиці інформаційної безпеки було б складним завданням без взаємодії користувачів, і тому контроль поведінки користувачів щодо цих політик є ключем до успіху. Сприйняття вважається ключовим компонентом людської поведінки та основною частиною інтелекту. Іншими словами, інтерпретація або розпізнавання сенсорної інформації людиною має

значний вплив на поведінку користувача. Саме тому сприйняття IT-користувачів має великий вплив на їх поведінку та прийняті рішення.

Якість сприйняття визначається кількома факторами, такими як обізнаність, знання, контрольованість, серйозність і можливість. Якщо існує розрив між реальним рівнем інформаційної політики та сприйняттям безпеки кінцевими користувачами, їхня поведінка та рішення зазнають відповідного впливу. По суті, наявність повного образу та повної обізнаності про те, що відбувається в політиці інформаційної безпеки, позитивно впливають на здатність користувачів розпізнавати потенційні загрози.

Ситуаційну обізнаність можна розглядати як знання про певну сферу. Загалом адекватне усвідомлення ситуації веде до ефективного прийняття рішень і допомагає зменшити потенційний рівень помилок користувачів. Іншими словами, ненавмисні внутрішні загрози, такі як помилки, можуть бути пов`язані з поганим розумінням ситуаційної обізнаності, а не з неправильним прийняттям рішень. Таким чином, співробітники повинні бути в курсі останніх моделей загроз і відповідних вимог безпеки.

Прикладом цього є те, що користувач не знає про фішингову кампанію, що може призвести до збою безпеки мережі. Більш відкриті, сумлінні та приємні учасники з більшою ймовірністю будуть дотримуватися політики інформаційної безпеки. І навпаки, учасники, які будуть більш екстравертами та невротичними, частіше порушуватимуть політику інформаційної безпеки. Співробітники, швидше за все, не можуть встановити межу між робочим і домашнім середовищем, а тому вони можуть потрапити в пастку «довіри до невинності» і почати опубліковувати особисту та ділову інформацію в соціальних мережах. Все вищезазначене необхідно враховувати при розробці інформаційної політики підприємства [2, с. 98].

При аналізі внутрішніх загроз необхідно враховувати організаційну культуру та регіональну / національну культуру, оскільки вони мають прямий вплив на ефективність рівнів захисту інформації та поведінку. Корпоративна культура може існувати, навіть якщо члени організації свідомо не усвідомлюють

її існування. Отже, головним завданням є додавання культури безпеки до організаційної культури, коли перша не є фундаментальною частиною останньої. Задоволеність співробітників визначається як загальне відчуття благополуччя працівника під час роботи. Працівник, який задоволений своїм роботодавцем, швидше за все, дотримуватиметься політики інформаційної безпеки організації. Таким чином, очікується, що користувачі, які позитивно ставляться до своєї організації, добре розуміють свої обов`язки, особливо щодо дотримання політики інформаційної безпеки. Задоволеність роботою позитивно впливає на дотримання заходів політики інформаційної безпеки. Таким чином, існує зв`язок між задоволеністю роботою та поступливою поведінкою, а саме вищий рівень задоволеності роботою мотивує користувачів виконувати вимоги.

Звичка – автоматична або ненавмисна поведінка. Таким чином, автоматизм є ключовим елементом стримувати прояв звички. Зазвичай звички можна оцінити шляхом вимірювання попередньої поведінки або частоти поведінки. Працівники виконують багато дій, не приймаючи свідомих рішень, а потім звикають до виконання цих дій. Існує аргумент, що звички пояснюють використання інформаційних технологій. Стверджується, що на реальну поведінку користувачів сильно впливають їхні звички використання технологій. Звична поведінка пояснює недотримання політики інформаційної безпеки. Звички користувачів суттєво впливають на намір дотримуватися політики інформаційної безпеки. Для організації дуже важливо привчити своїх працівників до правильних звичок, які допомагають їм дотримуватися політики інформаційної безпеки. Змінити поведінку користувачів або позбутися старих звичок роботи з інформаційними активами непросто. Однак, організація може знайти рішення та відстежити ефективність цих рішень.

Формування системи інформаційної безпеки відбувається з урахуванням вимог стандарту ISO / IEC 27001. Він створений для надання моделі розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення системи управління інформаційною безпекою. Визначений стандарт дозволяє залучити процесний підхід до розроблення, впровадження,

функціонування, моніторингу, перегляду, підтримування та вдосконалення системи інформаційної безпеки організації.

Для ефективної діяльності організації необхідно ідентифікувати та управляти багатьма видами діяльності. Будь-яку діяльність, що використовує ресурси та підлягає управлінню з метою забезпечення перетворення вхідних даних у вихідні, можна розглядати як процес. Часто вихідні дані одного процесу є безпосередньо вхідними даними для наступного.

Застосування системи процесів у межах організації разом з ідентифікацією цих процесів та їх взаємодіями, а також управління ними можна розглядати як «процесний підхід». «Процесний підхід» до управління інформаційною безпекою заохочує користувачів робити наголос на важливості:

- розуміння вимог інформаційної безпеки організації і необхідності розроблення політики та цілей інформаційної безпеки;
- впровадження контролів та їх функціонуванні для управління ризиками інформаційної безпеки організації в контексті загальних бізнес-ризиків організації;
- моніторингу та перегляді продуктивності та ефективності системи безпеки;
- постійному удосконаленні, основанному на об'єктивному вимірюванні.

Визначений стандарт узгоджується із стандартами ISO 9001:2015 та ISO 14001:2015 з метою підтримки послідовного та комплексного впровадження і функціонування разом з іншими пов`язаними стандартами управління. Таким чином, одна відповідним чином запроектована система управління може задовольняти вимоги всіх цих стандартів.

3.2 Аналіз процедури розробки сайту

Розробка сайту передбачає виконання великого обсягу робіт, незалежно від розміру майбутнього проєкту. Саме тому для реалізації успішного продукту

необхідно ретельно продумати всі етапи створення веб-сторінки та дотримуватись створеного плану. Виокремлюють такі етапи розробки сайту:

- визначення тематики та основної мети проєкту;
- розробка технічного завдання;
- прототипування, макетування та дизайн;
- верстка та програмування;
- наповнення контентом;
- тестування;
- здача готового проєкту.

Проєктування сайту – важливий процес, який має велике значення для розвитку бізнесу. Веб-розробники добре усвідомлюють, що створення односторінкового лендінгу або такого глобального проєкту як інтернет-магазин, однаково потребує великої кількості уваги, часу, фінансів, а також залучення до роботи команди фахівців.

Робота в команді завжди приводить до непорозумінь, а відсутність плану може призвести до не передбачуваного результату. Чіткий алгоритм дій з детально опрацьованими нюансами допоможе переконатися у тому, що проєкт просувається у потрібному напрямку. Процес створення сайту починається з усвідомлення проблеми. Сайт – дуже ефективний інструмент для ведення успішного бізнесу.

Важливо, щоб клієнт це розумів. Відповідно, спонукальними мотивами для його розробки може стати відсутність сайту, недієздатність наявного ресурсу або його неспроможність виконувати конкретні дії, що пов`язані з певними технічними недоліками. Чітке розуміння основної задачі майбутнього проєкту – дуже важлива складова, від якої залежить успіх бізнесу.

Спочатку потрібно визначити для чого сайт потрібен. Від цього залежатиме тип ресурсу, портрет цільової аудиторії та основні вимоги. Чітке розуміння мети та остаточного результату допоможе вибудувати ланцюг структури проєкту та сформувати етапи створення сайту, які необхідні для досягнення мети. Усі ці особливості необхідно обговорювати на початковому

етапі. Для цього потрібно працювати у тісному взаємозв'язку з замовником. Клієнтам дуже часто не вдається висловити загальну ідею. Активна участь у переговорах допоможе розробити концепцію, сформулювати основні цілі та вибрати інструменти для їх досягнення. Тільки після досягнення порозуміння та визначення основних пріоритетів, можна переходити до наступного етапу.

Технічне завдання – офіційний документ та фундамент для подальшої роботи. В ньому прописуються всі деталі: структура або мапа сайту (кількість сторінок, розділів, категорій, блоків), вимоги стосовно дизайну, функціонального, візуального та текстового наповнення, а також технічні можливості.

Технічне завдання – інструкція, яка буде постійно використовуватися під час розробки сайту. Перейти до основних видів робіт можна буде лише після узгодження всіх питань. На наступному етапі створюється макет, який перевтілить ідеї у реальний об'єкт. Мова не про розробку повноцінного веб-інструменту, готового до роботи, але можна його роздивитися та оцінити переваги. Для цього команда дизайнерів працює над декількома ескізними варіантами, беручи за основу технічне завдання.

Після підготовки прототипів та макетів їх узгоджують з замовником. При необхідності вносяться необхідні зміни, поки проєкт не буде ухвалено остаточно. Наступний крок – формування технічної складової. Спеціалісти для цього використовують знання з основ HTML, підключають CSS стилі, а потім з`єднують їх з CMS. Слід зазначити, що не всі сайти створюються на основі CMS. Наприклад, прості односторінкові ресурси здатні функціонувати без системи управління контентом.

Надалі послідовність створення веб сайту передбачає надання послуг з програмування. Фахівець повинен «оживити» сайт та наповнити його необхідним функціоналом. У більшості випадків програмування здійснюється на основі CMS, наприклад, на WordPress або сервісі Тільда, але в інших – потребується написання коду з нуля, наприклад, для того, щоб розробити унікальний функціональний блок тощо [3, с. 175].

Після завершення створення верстки отримується, по суті, робочий інструмент, але з порожніми розділами та сторінками. Їх необхідно заповнити текстовими та графічними матеріалами. Важливо, щоб контент відповідав стандартам оптимізації для подальшого просування ресурсу в пошукових системах.

Тестування – завершальний етап, який включає проведення різних видів перевірок на предмет помилок, некоректного функціонування та загальної працездатності ресурсу. Виявлені помилки усуваються фахівцями до тих пір, поки не будуть повністю вирішені. Ще один важливий пункт – розміщення сайту в інтернеті. В момент, коли отримується зверстаний проєкт, який готовий до роботи, не варто думати, що він почне приносити прибуток у цю ж секунду. Для цього сайт має бути доступним для користувачів, тому його переносять на постійне місце розміщення – хостинг. Окрім того, йому потрібно обрати доменне ім`я.

Після розміщення сайту в інтернеті проводяться фінальні тестування, щоб перевірити його працездатність. Після передачі замовнику готового проєкту, фахівці проводять навчання з роботи з сайтом. Це допоможе клієнту самостійно оновлювати інформацію на ресурсі, збирати аналітику, вносити певні зміни та діяти на свій розсуд. За бажанням клієнт може продовжити роботу з розробником, адже будь-який ресурс потребує подальшого розвитку, підтримки та просування.

Сайт та особистий кабінет клієнта замовники часто відносять до завдань веб студії і розробки сайту, хоча це не зовсім правильно. Для компаній з B2B діяльністю особистий кабінет клієнта часто представляє інтерес в якості взаємодії з поточною компанією – бачити всі замовлення, надати і терміни оплати замовленнь, бачити переліки придбаних товарів або перелік фактичного устаткування, що знаходиться в сервісному центрі.

Створити сайт з особистим кабінетом для клієнтів можна різними способами:

- Замовити сайт з особистим кабінетом на обраної платформі у веброзробника або компанії, яка розробляє сайт. Недолік моделі в необхідності продублювати бізнес логіку на сайті, хоча вона вже є в обліковій системі. Даний варіант підходить при простій об`єктній моделі даних.

- Варто спрямувати клієнта всередину облікової системи, де буде зібрана для нього інформація. Один з варіантів вирішення завдання, коли клієнти через браузер можуть потрапити всередину сторінки облікової системи та виконати там необхідні дії або подивитися необхідну інформацію. Переваги даного варіанту полягають в простоті рішення з обмовкою на технологічну платформу облікової системи, адже вона повинна надавати такий варіант доступу до даних і можливістю розмежувати права до інформації. Недоліком такого варіанту може стати велика кількість клієнтів, яким потрібно забезпечувати доступ. Даний варіант підходить для невеликої кількості користувачів одночасно, які мають працювати з базою.

- Створення сайту з особистим кабінетом клієнта на базі API доступу. Переваги даного варіанту в тому, що на стороні сайту немає необхідності робити структуру даних, зменшувати час реалізації проєкту, присутньою є можливість багаторазового використання даних з API іншими системами без збільшення навантаження на сам сайт, можливість заміни платформи сайту без втрати даних. Недоліком такого варіанту є існування додаткової проміжної бази даних для зберігання і надання даних по API в IT-інфраструктурі підприємства. Даний варіант підходить для великої кількості користувачів, для складних моделей надання даних і аналітики для користувачів та клієнтів. Одним з варіантів вирішення даного завдання є використання інтеграційної платформи iPaaS для надання корпоративних даних з інших інформаційних джерел у вигляді API для зовнішнього використання.

Розробка та проєктування сайту відбувається відповідного до вимог стандарту ДСТУ ISO / IEC / IEEE 23026:2016. Він встановлює вимоги до всього життєвого циклу web-сайтів, охоплюючи стратегію, дизайн, розробления,

випробування та валідацію, а також керування та підтримання для інтранет- і екстранет-середовищ.

Цей стандарт стосується тих, хто застосовує web-технології для подання інформації щодо інформаційно-комунікаційних технологій, наприклад, для подання документації користувача систем і програмних засобів, документації життєвого циклу проєктів інженерії систем та програмних засобів, документації політики, планів і процедур керування службою інформаційних технологій [4, с. 225].

У ньому встановлено вимоги до власників та постачальників web-сайтів, менеджерів, відповідальних за встановлення рекомендацій щодо розроблення та експлуатування web-сайту, до розробників програмних засобів, експлуатаційного й обслуговувального персоналу, які можуть бути як працівниками організації-власника web-сайту, так і сторонніми особами.

Метою цього стандарту є поліпшення зручності застосування інформаційних web-сайтів і спрощення супроводу експлуатації керованого Web з огляду на:

- знаходження актуальної та своєчасної інформації;
- застосування керування інформаційною безпекою;
- спрощення процедури використання сайту;
- забезпечення узгодженості й ефективності розроблення та супроводу сайту.

3.3 Аналіз особливостей розробки процедури створення сайту

В умовах існування спеціальних конструкторів та платформ створення сайту не існує потреби в особливих навичках програмування, веб-розробки та веб-дизайну. Для стандартного сайту достатньо замовити хостинг, налаштувати відповідну тему, додати необхідні плагіни та наповнити його контентом. Щоб зробити сайт самостійно, слід обрати CMS (систему керування контентом) чи

конструктор. Наразі пропонується досить багато як безкоштовних, так і платних варіантів із широким функціоналом.

Існують два підходи до вибору домену: купити новий домен або з історією. Старий домен простіше просувати, якщо на ньому раніше був якісний та трастовий ресурс, а його тематика збігалася з тією, яку буде мати новий проєкт. Перевагою буде і наявність посилань. Однак, перед придбанням важливо переконатися, що на домен не накладено фільтри пошукових систем.

Домен складається з кількох частин, які розділені точками, їх називають рівнями. Найчастіше використовують домени другого-четвертого рівнів. При виборі доменного імені найчастіше зупиняються на назві бренду. Такий варіант буде зручним для запам`ятовування, а також є актуальним для ранжування навігаційних запитів.

Краще підбирати просту назву, яка матиме однозначну транслітерацію, наприклад, globus, dom, iskra, ritm. Використання складних словосполучень викликає труднощі у користувачів при наборі адреси сайту у пошуковому рядку браузера. У країнах СНД досить поширені кириличні назви, зокрема домени першого рівня, наприклад, .РУС, .РФ, .УКР та інші. Використовувати кирилицю в домені слід обережно, оскільки вона кодується в ASCII-символи, і це викликає складності при використанні посилань.

Відповідний варіант доменної зони залежить від типу сайту:

- Доменна зона може свідчити про його територіальну приналежність – національну чи регіональну: .ua, .ru, .kz, by.
- Характеризувати тематику чи сферу діяльності: com.ua – комерційні сайти України, .info – блоги, .tv – канали чи ресурси телебачення.
- Відповідати офіційним організаціям, наприклад, освітнім установам та уряду – .gov, .edu. Такі доменні зони доступні лише при наданні ліцензій та підтверджуючих документів.
- Бути міжнародною – для сайтів із цільовою аудиторією у різних країнах, наприклад, .org, .com.

Якщо сайт орієнтований на просування лише в одному регіоні країни, наприклад, у Києві, то можна використовувати субдомен у такому форматі: kiev.назва-бренда.com.ua. В даному випадку в майбутньому буде простіше розширюватися, не змінюючи основного домену (назва-бренда.com.ua). Просто додаватимуться субдомени з іншими містами. Якби слово «Київ» використовувалося здебільшого в домені, то при розширенні в майбутньому довелося б змінювати весь домен [5].

Перевірити вік обраного домену, дізнатися тематику сайту, який був розташований на ньому, та іншу важливу інформацію можна за допомогою онлайн-сервісів, наприклад: Webarchive, Whoishistory. При виборі хостингу важливо звернути увагу на такі аспекти:

- Ціна. На січень 2022 року в Україні мінімальна щомісячна абонплата у хостинг-провайдерів знаходиться в приблизному діапазоні від 45 до 100 гривень на місяць і залежить від обсягу послуг і терміну, за який оплачено хостинг.
- Об'єм дискового простору. Важливо правильно розрахувати орієнтовний обсяг сайту та контенту, який буде завантажено. Велика кількість мультимедійних файлів вимагатиме суттєвого дискового простору на хостингу.
- Аптайм – час безперервної роботи сервера. Цей показник має становити не менше 98%.
- Тип диска. SSD-диски працюють у 5 разів швидше, ніж HDD.
- Ліцензія. Компанія з надання хостингу має бути офіційно зареєстрована та мати ліцензію на відповідний вид діяльності.
- SSL-сертифікат. Багато хостинг-провайдерів надають SSL-сертифікат безкоштовно. Сертифікат безпеки важливий для всіх сайтів, особливо для інтернет-магазинів та інших ресурсів, які мають доступ до персональної інформації.
- Наявність технічної підтримки. Важливо, щоб хостинг-провайдер надавав цілодобову технічну підтримку, до якої можна звернутися у разі виникнення проблем у роботі сайту.

- Версія PHP. Для коректної, швидкої та безпечної роботи сайту на серверах не повинні використовуватися застарілі версії PHP (раніше, ніж 7.1).
- Можливість встановлення CMS. Зручно, якщо дистрибутиви для інсталяції потрібної CMS будуть на серверах хостинг-провайдера. У цьому випадку їх можна буде використовувати для встановлення двигуна відразу після покупки домену та замовлення хостингу.
- Домен. Деякі провайдери надають домен у подарунок при замовленні хостингу на тривалий час, наприклад, на рік.

Щоб розмістити проєкт на сервері, варто створити новий сайт у панелі керування, а потім встановити на ньому потрібну CMS. У різних хостинг-провайдерів ця процедура може трохи відрізнятися.

Після завантаження всіх файлів CMS у кореневий каталог сайту може знадобитися налаштування прав доступу до них (755 або 644). Такі права дозволяють редагувати файли лише власнику сайту, іншим користувачам доступне лише їхнє читання. Якщо виставити права 777, редагування файлів стане доступним будь-яким користувачам, а це – суттєва загроза безпеці. Відновити права доступу можна у розділі налаштування або файл-менеджері. Надалі впродовж найближчого часу сайт стане доступним за обраною URL-адресою для забезпечення успішного його використання [6].

3.4 Рекомендації щодо покращення системи інформаційної безпеки підприємства

Підсумовуючи, ефективну систему інформаційної безпеки підприємства варто будувати на аналізі вже існуючих проблем у безпеці та на аналізі і проговоренню виконання повсякденних задач. Аналіз існуючих проблем та опис структури повсякденних задач вже були зроблені раніше. Основні загрози які вже були виявлені раніше:

- Відсутність антивірусного ПО на самих фізичних девайсах.

- Відсутність можливості віддаленого доступу до фізичних пристроїв співробітників.
- Відсутність можливості стерти дані з девайсу, коли фізичний доступ до нього втрачено.
- Відсутність можливості контролювати точки доступу до мережі інтернет які використовують співробітники.
- Відсутність єдиного сховища паролей для співробітників.

Після аналізу того як зазвичай проходить робота на підприємстві на прикладі аналізу розробки веб сайту можливо запропонувати деякі покращення.

Оскільки поставлена ціль поставити антивірус на всі девайси дуже амбітна, то було прийнято рішення виставити ряд вимог яким має відповідати оптимальне програмне забезпечення:

- Програмне забезпечення має працювати на старих версія операційної системи Mac Os
- Не конфліктувати з власними структурними елементами захисту (Filevault, Карантин, Activity Monitor) Mac Os
- Бути сертифікованим через AV сертифікацію

Проаналізувавши всі варіанти які присутні на маркеті, було виявлено що всім зазначеним вище вимогам відповідає декілька варіантів антивірусного програмного забезпечення. Це антивіруси Aviro та Intego. Оскільки обидва варіанти відповідали вимогам, то було прийнято рішення спробувати обидва і порівняти зручність. У антивірусного програмного забезпечення Aviro була можливість безкоштовного використання з обмеженим функціоналом, що і стало причиною його затвердження. Також ціна на це програмне забезпечення та перелік додаткових функцій виявився достатнім для подальшого його використання, зокрема це:

- Підтримка версій MacOs з 10.11, що на 1 версію перекриває потребу і дає простір для використання ще 1 системи
- Захист у режимі реального часу, що зменшує ризики потрапляння шкідливих програм на фізичний девайс під час роботи

- Конфігуратор, що дозволяє обрати оптимальний для роботи компанії перелік функцій, що дає можливість меньше негативно впливати на продуктивність робочого процесу

Враховуючи перелічені фактори можливо вважати що антивірус Aviro є найкращим варіантом для захисту інформації в компанії, до того ж ціна на продукт цієї компанії є закономірною до наданого переліку послуг.

Для віддаленої можливості працювати з пристроями співробітників було вирішено встановити програмне забезпечення AnyDesk, що відповідає основним вимогам щодо зручності інтерфейсу та можливості редагувати, зберігати та видаляти файли з фізичного девайсу.

Для більш свідомого користування мережею інтернет та відношення до даних співробітників та замовників, були прийнято рішення видати наказ по підприємству, в якому:

- Провести інформаційну презентацію стосовно безпеки роботи віддалено.
- Приділити більшу увагу до моніторингу безпеки, а саме на дотримання вже існуючих положень у власному домі та при роботі у публічних місцях
- Визначити заходи адміністративного покарання за порушення правил роботи з документами і відомостями, що містять комерційну таємницю
- Довести до співробітників щодо неможливості застосування робочого програмного та апаратного забезпечення у особистих цілях
- Прийняти заборону на зберігання особистої інформації на комп'ютері
- Від працівників, які за посадою володіють відомостями комерційної таємниці ввести додаткові умови у договорі та перезаключити вже існуючі договори. А саме брати письмові зобов'язання про нерозголошення комерційної таємниці та даних замовника.

- У разі звільнення працівника, вимагати від нього передачі всіх носіїв інформації, що становлять комерційну таємницю, які перебували в його розпорядженні
- Розробити журнал обліку фізичних девайсів на балансі співробітника
- Розробити правила роботи з електронною поштою

Запропоновано ввести єдине для всієї компанії сховище для паролів. Також дослідження роботи показали що для співробітників було би зручно мати доступ як до спільних даних по паролям компанії, так і мати власний простір де можливо зберігати лише особисті паролі до робочих сховищ та кластерів.

Таким вимогам повністю відповідало програмне забезпечення 1Password. А крім того, після впровадження обов'язкового користування були помічені такий функціонал застосунку, що позитивно вплинув на роботу співробітників:

- Можливість генерувати захищені паролі, на злам яких буде витрачено дуже значний період часу. Наприклад для взлому паролю 73c*RG47Cm!k2WKNWj@KJ8edXMaDDgGcfc за даними з сайту https://random-ize.com/how-long-to-hack-pass буде витрачено 1.3816001894523395*e^50 років
- Спільне на всю компанію сховище не лише паролей, а майже будь-яких текстових даних
- Наявність застосунків для IOs девайсів та розширення для браузеру

Загалом за наявними даними, для покращення інформаційної захищеності та мінімізації пробдем з наявними загрозами такої кількості змін буде достатньо. Оскільки ітеративний підхід до запровадження змін є одним із найбільш ефективних, то таких змін на теперішній час буде достатньо. Проте, після аналізу саме тих результатів що будуть через певний час після застосування вищезгаданих рекомендацій можливо буде провести ретроспективу та аналіз принятих рішень. На основі якої вже визначити які підходи та заходи показали свою ефективність, а які варто змінити чи взагалі передивитися їх застосування.

ВИСНОВКИ

Інформаційна безпека - це сукупність практик які мають бути застосованими для запобігання несанкціонованому доступу, використання, розкриття, спотворення, заволодіння, зміни або знищення інформації.

В основі підтримання належного рівня інформаційної безпеки лежить діяльність по захисту інформаційних даних - забезпечення їх конфіденційність, доступність та цілісність. Прийняти всі дії для недопущення будь-якої компрометації в критичній ситуації, та знаходження варіантів для зменшення наслідків таких ситуацій.

Це поняття можна застосувати для всіх типів даних (як фізичних, електронних або даних у хмарних сховищах). Основне завдання інформаційної безпеки – збалансований захист конфіденційності, цілісності і доступності даних, з урахуванням доцільності застосування і з найменшими втратами для продуктивності працівників.

Основним здобутком під час реалізації інформаційної безпеки на підприємстві є проектування та налаштування роботи на підприємстві так щоб забезпечувалась інформаційна безпека конкретних об’єктів (СЗІБ). Основними завданнями під час побудови, а саме під час дослідження існуючої інформаційної безпеки підприємства є:

- виявити вже існуючу інформаційну систему

- аналіз існуючої інформаційної системи
- виявлення найбільш вразливих компонентів системи
- виявлення вимог щодо подальшого захисту інформації
- використовуючи отриману інформацію та враховуючи вимоги національного та міжнародного захисту інформації почати розробку положень нової СЗІБ для конкретних елементів інформаційної системи
- визначення стратегії для впровадження створених положень нової СЗІБ у роботи підприємства

Сама реалізація основних вимог політики інформаційної безпеки має бути впроваджена на рівні відповідних департаментів. Мають бути впроваджені відповідні програмно-апаратні, інженерно-технічні та інші способи і засоби захисту інформації. Фінальним процесом має бути впровадження системи подальшого моніторингу системи інформаційної безпеки та ітеративних покращень у вже існуючих складових, за потреби.

ISO / IEC 27001 це один з міжнародних стандартів щодо дотримання інформаційної безпеки, розроблений спільно Міжнародною організацією зі стандартизації та Міжнародної електротехнічної комісією. Стандарт був створений та підготовлений до випуску підкомітетом SC27 Об'єднаного технічного комітету JTC 1. У стандарті містяться вимоги які чітко визначають області інформаційної безпеки які мають бути створені та положення щодо розвитку і підтримки Системи менеджменту інформаційної безпеки (СМІБ).

Структура стандарту ISO / IEC 27001 (ISO 27001) включає у себе затверджені світові рекомендації та практики управління інформаційною безпекою. ISO 27001 впроваджує до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси. Підвищення значущості інформації з часом призвело до поширення потреби в розробці та реалізації структури управління безпекою інформації. Результатом такого явища стало ініціювання процесу створення відповідних стандартів якості ISO/IEC, результатом якого виникла група стандартів ISO

27000. Це сімейство відповідає за стандартизацію певної діяльності, що пов'язана із застосування та використанням СУІБ.

ISO/IEC 27000 містить сукупність взаємопов'язаних стандартів та вказівок, які були опубліковані на даний момент чи ще знаходяться на етапі розробки. Варто зазначити, що ця група стандартів якості вміщує певні структурні компоненти, які орієнтовані на нормативні стандарти, які в свою чергу складаються з вимог до СУІБ, вимог органів із сертифікації, що надають послуги із сертифікації відповідно до ISO/IEC 27001, та додаткових вимог для секторальних впроваджень СУІБ

Впровадження положень стандарту ISO 27001 може бути виконане для майже кожної організації, не дивлячись на специфікацію. Є приклади успішного впровадження практик у комерційний та некомерційних, приватних та державних, великих та малих підприємств . У написанні стандарту брали участь провідні світові експертами в області інформаційної безпеки.

Важливим моментом є те, що після запровадження стандарту на підприємстві є можливість отримати сертифікацію від відповідних незалежних органів. Ця сертифікація буде визнаною не тільки в кордонах України, а і по всьому світі, оскільки стандарт є міжнародним. Ця сертифікація означає що організація працює з впровадженими положеннями щодо інформаційної безпеки відповідно до даного стандарту і всі замовники можуть бути впевненими у збереженні та відповідальному поводженню з власними та їхніми даними.

Основними принципами стандарту ISO 27001 є: конфіденційність інформації, цілісність інформації, доступність інформації.

Міжнародна стандартизація складових системи управління інформаційною безпекою формує три напрямки розвитку в сфер СМІБ: сімейство стандартів „Методи забезпечення безпеки" – ISO/IEC 27000-ISO/IEC 27037; сімейство стандартів „Методи та засоби забезпечення безпеки" – ISO/IEC 15408 („Загальні критерії", 3 частини), ISO/IEC 13335 (5 частин), ISO/IEC 18045; сімейство стандартів „Управління та аудиту інформаційних технологій" (CobIT, ITSM, ITIL та ін.). У зв'язку з розвитком інформаційних технологій збільшується

й кількість вимог, які забезпечуватимуть захист ІТ. В результаті таких змін стандарт ISO/IEC 27001:2005 був розглянутий та удосконалений до ISO/IEC 27001:2013, а потім ISO/IEC 27001:2021.

Ряд поповнень та змін в стандарті ISO/IEC 27001:2021 свідчать про важливість розвитку систем менеджменту інформаційної безпеки та необхідність приділяти більше уваги саме інформаційній безпеці.

Особливо у підприємствах діяльність яких пов'язана з Інформаційними Технологіями дуже гостро стоїть питання ефективної реалізації будь-якого стандарту поводження з інформаційною безпекою.

Стандарт ISO/IEC 27002: 2005 (ISO 17799) в плані захисту на зберігання інформації володіє однією з найоптимальніших сукупностей можливостей. Виходячи з зазначеного, доцільно доповнити діючі та перспективні стандарти такими продуктами як довідник з питань інформаційної безпеки, гіпертекстовий довідник з питань захисту інформації, керівництво для співробітників служби безпеки, тренінги що адаптовані під різні рівні взаємодії та доступу до інформаційної системи, різноманітні демонстраційні версії і презентації, зручною навігацією до прийнятих положень по інформаційній безпеці компанії.

На мою думку одним з найважливіших процесів у розробці заходів щодо інформаційної безпеки є оцінка ризику що вже можуть бути наявні у виробництві. Існує багато приватних підприємств які спеціалізуються на наданні саме послуг щодо цього кроку у розробці інформаційної безпеки. Особливо важливо розуміти ризики які можуть виникнути та які наслідки може мати через це компанія. В ході оцінки ризику також можна оцінити частоту виникнення небажаних подій і ймовірність цього. Це має створити підґрунтя для розробки та пріоритизації подальших кроків у інформаційній системі.

Через відсутність стандартизованих підходів та методик для оцінки ризиків і в кожному конкретному випадку необхідно ретельно прораховувати і продумувати всі фактори ризику, проводити аналіз і розрахунок, що є дуже трудомістким завданням.

З усіх методів оцінки ризиків необхідно застосовувати сукупність методів аналізу, обробки інформації та тільки після цього оцінювати ризики ІБ, і здійснювати управління ІБ. Удосконалення системи оцінки ризиків та уніфікація підходів що застосовуються являється дуже актуальним завданням актуальним у зв'язку зі швидким розвитком та поширенням інформаційних технологій на території України. Також, сертифікація різного роду діяльності держави за міжнародними стандартами свідчитиме, в першу чергу, про якість інформаційної безпеки України, що в подальшому надавати їй певні переваги в сертифікованих сферах діяльності серед багатьох інших країн, а також, особливо, для звичайних громадян України.

Об'єктом дослідження в магістерській роботі є ФОП "Почерпайло Андрій Андрійович". Основна форма діяльності – комп'ютерне програмування.

Підприємство не має конкретного офісу та займає різні офіси в залежності від домовленості з замовником, проте основне місце праці працівників це їх власний дім. Таке рішення в умовах сьогодення надає як переваги так і недоліки у рамках дотримання стандартів інформаційної безпеки підприємства. Чисельність комп'ютерів, ноутбуків, планшетів в власності підприємства близько 6 штук, проте за необхідності ця цифра швидко зростає в залежності від умов та кількості співробітників.

Інформаційна система підприємства ФОП "Почерпайло Андрій Андрійович" є розробленою під певні цілі низка засобів та особистих доступів персоналу. Ця система використовується для найшвидшого, якісного та безпечного реагування на побажання замовника і надання спеціалістам відповідних умов для виконання поставлених задач у відповідності з цінностями вище.

У кожного фахівця компанії є можливість відвідувати коворкінги або працювати вдома, в залежності від потреб та умов створених для кожного спеціаліста.

Широко застосовуються різне програмне забезпечення. Оскільки підприємство в основному займає ланку виробництва та тестування програмного

забезпечення для системи Mac Os, то саме ця система широко представлена у співробітників компанії. Присутні системи від версії 10.12, що була в релізі на 2016 рік до 12.4 що є найновішою стабільною системою на ринку. В процесі роботи, співробітники стикаються з необхідністю тестування та написання власного програмного коду. Через це у компанії є широкий набір інструментів для зберігання, редагування та створення таких програм. Наприклад GitHub, TablePlus, Postman та редактори коду такі як PyCharm та PhpStorm. Всі програми є купленою власністю підприємства. Це означає що весь софт на робочих системах є безпечним, стандартизованим та ліцензованим.

На основі аналізу були знайдені такі загрози для підприємства

- Відсутність антивірусного ПО на самих фізичних девайсах.
- Відсутність можливості віддаленого доступу до фізичних пристроїв співробітників.
- Відсутність можливості стерти дані з девайсу, коли фізичний доступ до нього втрачено.
- Відсутність можливості контролювати точки доступу до мережі інтернет які використовують співробітники.
- Відсутність єдиного сховища паролей для співробітників.

Насамперед була проаналізована найбільш звична задача для підприємства, а саме проектування та розробка веб сайту. Незважаючи на наявність найкращих програм інформування про інформаційну безпеку, існують перешкоди, які ускладнюють успішне впровадження заходів інформування, до яких належать:

- впровадження нових технологій;
- брак організованості справ;
- невиконання подальших дій.

Для підприємства був запропонований такий спектр вдосконалень:

- Встановлення антивірусного програмного забезпечення Aviro
- Проведення ряду воркшопів та інформаційних зустрічей

- Встановлення програмного забезпечення AnyDesk для віддаленого доступу до девайсів співробітників
- Встановлення єдиного менеджеру паролей 1Password

За результатами запропонованих змін було прийнято запровадити зустріч та ретроспективу на якій буде проведений аналіз ефективності та ефекту впроваджених змін на роботу підприємства.

Після того, як зазначені зміни будуть прийняті можливо буде також дослідити витрати на впровадження змін, та побудувати розрахунки коефіцієнту економічної ефективності, які будуть гарним додатковим підґрунтям до прийняття рішень щодо запроваджених змін.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вадим Гребеніков «Управление информационной безопасностью. Стандарты суиб». URL: https://mybook.ru/author/vadim-grebennikov-2/upravlenie-informacionnoj- bezopasnostyu-standarty/read/ (дата звернення 14.07.2022).
2. Information Security Management System. URL: https://otrs.com/otrs-solutions/isms/ (дата звернення 14.07.2022).
3. A History Of Information Security. URL: https://www.ifsecglobal.com/cyber-security/a-history-of-information- security/ (дата звернення14.07.2022).
4. ISO/IEC 27001:2013 Information Security Management Standards. URL: https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001 (дата звернення 14.07.2022).
5. Стандарт ISO/IEC 27001:2013. URL: https//intercert.com.ua/articles/posts/292-standart-iso-iec-27001-2013 (дата зверненя 14.07.2022).
6. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=5345 34 (дата звернення 15.07.2022).

7. СЕРТИФИКАЦИЯ ISO/IEC 27001. URL: https://iitc.com.ua/ru/sertifikatsiya/sertifikatsiya-iso-27001/ (дата звернення 19.07.2022).

8. Національне агентство з акредитації України. URL: http://naau.org.ua (дата звернення 19.07.2022).

9. Разработка системы ISO 27001. URL: https://atestor.ua/services/vnedrenie-standarta-iso-27001/ (дата звернення 19.07.2022).

10. ДСТУ ISO/IEC 27001:2015 відповідає ISO/IEC 27001:2013; Cor 1:2014, IDT – Information technology – Security techniques – Information security management systems – Requirements (Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги). Київ: ДП «УкрНДНЦ», 2016. 22 с.

11. Основы стандарта менеджмента информационной безопасности ISO/IEC 27001. URL: https://www.bsigroup.com/ru-RU/ISO-IEC-27001/ISO-IEC-27001-Introduction/ (дата звернення 19.07.2022).

12. ISO/IEC 27001 для предприятий малого и среднего бизнеса (МСБ). URL: https://www.bsigroup.com/ru-RU/ISO-IEC-27001/ISO-IEC-27001-SMEs/ (дата звернення 19.07.2022).

13. Біленчук П. Д., Борисова Л. В., Неклонський І. М., Собина В. О. Правові засади інформаційної безпеки України: монографія. Харків: АМ-Фенікс, 2018. 289 с.

14. Бурячок В. Л., Толюпа С. В., Семко В. В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник. Київ: ДУТ-КНУ, 2016. 178 с.

15. Логінова Н. І., Джобожур Р. Р. Правовий захист інформації навчальний посібник. Одеса: Фенікс, 2015. 264 с.

16. Пількевич І. А., Лобанчикова Н. М., Молодецька К. В. Захист інформації в автоматизованих системах управління: навчальний посібник. Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

17. Fisher T. Free and Public DNS Servers. Lifewire. URL: https://www.lifewire.com/free-and-public-dnsservers-2626062 (Дата доступу: 25.09.2022).

18. Global Cybersecurity Index (GCI) 2018. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf (Дата доступу: 25.09.2022).

19. NIST Special Publication 800-63B. URL: https://pages.nist.gov/800-63-3/sp800-63b.html

ДОДАТКИ

НУБіП України

НУБіП України

НУБіП України

НУБіП України

Додаток А.

НУБіП України

НУБіП України

НУБіП України

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет харчових технологій
та управління якістю продукції АПК

XI МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ ВЧЕНИХ, АСПІРАНТІВ І СТУДЕНТІВ

«Наукові здобутки у вирішенні актуальних проблем виробництва та переробки сировини, стандартизації і безпеки продовольства»

ЗБІРНИК ПРАЦЬ

за підсумками
XI Міжнародної науково-практичної
конференції вчених, аспірантів і студентів

КИЇВ – 2022

ЗМІСТ

УДК 004.056.53

А.А. Почерняйло, здобувач ОС «Магістр»
Т.В. Ровінська, доктор філософії (PhD), асистент
Л.О. Адамчук, к. с.-г. н., доцент
Національний університет біоресурсів і природокористування України, м. Київ

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА БАЗІ МІЖНАРОДНИХ СТАНДАРТІВ СЕРІЇ ISO

Міжнародні стандарти серії ISO 27000 є основоположними в сфері управління інформаційною безпекою. Вони являють собою модель системи менеджменту, яка визначає загальну організацію процесів, класифікацію даних, системи доступу, напрямки планування та удосконалення системи безпеки, відповідальність співробітників і оцінку ризику.

Основна ідея стандартів серії ISO – забезпечення надійного захисту інформаційних ресурсів та організація ефективного доступу до даних й процесу їх обробки згідно з визначеними послугами.

Переваги застосування системи управління інформаційною безпекою на базі міжнародних стандартів серії ISO:

1. Забезпечення неперервності.
2. Мінімізація ризиків.
3. Зниження витрат на інформаційну безпеку.
4. Забезпечення цілісності, конфіденційності та доступності критичних інформаційних ресурсів.
5. Забезпечення комплексного та централізованого контролю рівня захисту інформації.

Згідно з міжнародним стандартом ISO 27001, система управління інформаційною безпекою – це частина загальної системи управління організації, яка заснована на оцінці ризиків, створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення загальної інформаційної безпеки.

Висновок

На основі проведеного аналізу сучасних заходів управління інформаційною безпекою на базі міжнародних стандартів ISO виявлено, що управління безпекою є важливим аспектом забезпечення безпеки властивостей інформаційних ресурсів та послуг в мережах передачі даних. Для досягнення й підтримки безпеки в інформаційно-комунікаційних системах та мережах потрібен певний діапазон засобів та заходів управління.

ЛІТЕРАТУРА

1. BS EN ISO/IEC 27001:2017 Information technology. Security techniques. Information security management systems. Requirements.

НУБіП України

НУБіП України

НУБіП України

НУБіП України