МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Обслуговування комп'ютерних систем та мереж»

Група: 4ФКС-56

Дипломний проект

здобувача освіти денної форми навчання
ФКС.56.01.000.ДП

АРНАУТОВ
ДМИТРО РУСЛАНОВИЧ

м. Одеса
2023 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: «**Обслуговування комп'ютерних систем та мереж»**

Група: **4ФКС-56**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи) на тему:

Модернізація ІТ-середовища сучасного підприємства на основі міжнародних стандартів з кібербезпеки.

Проектний матеріал складається з пояснювальної записки на 79 сторінках та графічного (презентаційного) матеріалу на 13 аркушах (слайдах).

Дипломник _____ (Арнаутов Д.Р.)

Керівник _____ (Стайкуца С.В.)

Консультанти:

з економічної частини _____ (Копайгородська Т.Г.)

з охорони праці _____ (Чорновол Н.І.)

з дотримання вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Голова циклової комісії _____ (Кривченко Ю.В)

Завідувач відділення _____ (Скорнякова О.В)

Захист «20» червня 2023 р. Протокол ДКК № 2

Оцінка ДКК 4 (добре)

Секретар ДКК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення **комп'ютерних систем** Комісія **КТ та ІІІ**

Спеціальність **123 «Комп'ютерна інженерія»**

Освітня програма **«Обслуговування комп'ютерних систем і мереж»**

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань І.В.

"_____" _____ 2023 р.

ЗАВДАННЯ

на дипломний проект (роботу)

Здобувачеві (здобувачці) освіти Арнаутову Дмитру Руслановичу

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи)) Модернізація ІТ-середовища сучасного підприємства на основі міжнародних стандартів з кібербезпеки

затверджена наказом по коледжу від "17" **жовтня** 2022 р. № **235-А2-ОД**

2. Термін здачі закінченого проекту (роботи) 12.06.23

3. Вихідні данні до проекту (роботи):

Об'єкт аналізу – інформаційна інфраструктура сучасного підприємства

Основні стандарти - ISO 27001, ISO 27032, PCI DSS, HIPAA, NIST 7621, GDPR, НВ 292:2006

Стратегічна мета – досягнення принципів неперервності (BCM)

Методи захисту – організаційні на основі стандартів, ТЗО, DLP, RAID, BCM

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Класифікація, склад та основні компоненти ІТ-середовища. Провести аналіз міжнародних Стандартів з кібербезпеки. Виділити організаційні, технічні та програмні заходи та засоби захисту. Напрям організаційного захисту розробити на основі NIST 7621. Застосувати технічні та програмні засоби як елементи модернізації. Навести економічну частин та охорону праці.

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Модель підприємства на основі інформаційних технологій; Основні та додаткові компоненти інфраструктури; Аналіз міжнародних стандартів та рекомендацій з напрямку кібербезпеки; Стандарт ISO 27032; Регламент захисту персональних даних GDPR; Методи та засоби модернізації інформаційної інфраструктури на основі NIST 7621; Використання систем фізичного захисту та принципів неперервності; Застосування систем протидії витокам (DLP); Порівняльний аналіз ймовірностей реалізації загроз від ненавмисних дій внутрішніх порушників; Висновки

6. Консультанти по проекту (роботі), із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Вступ, 1	Стайкуца С.В.		
2	Копайгородська Т.Г.		
3	Чорновол Н.І.		
Нормоконтроль	Петрашова В.І.		

7. Дата видачі завдання 01 травня 2023 р.

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1.	Вступ. Постановка мети та задач проектування	22.05.2023	Виконав
2.	Формування кінцевого завдання на розробку. Вступна частина дипломного проекту.	24.05.2023	Виконав
3.	Огляд літератури. Огляд існуючих рішень.	25.05.2023	Виконав
4.	Технологічний розділ. Дослідження складу та компонентів інформаційного середовища.	28.05.2023	Виконав
5.	Технологічний розділ. Робота з міжнародними стандартами з кібербезпеки.	03.06.2023	Виконав
6.	Технологічний розділ. Вибір методів та засобів для проведення модернізації IT-інфраструктури в аспекті захисту кіберсередовища.	08.06.2023	Виконав
7.	Економічний розділ.	05.06.2023	Виконав
8.	Виконання розділу «Охорона праці».	08.06.2023	Виконав
9.	Підготовка доповіді та презентації для захисту	09-11.06.2023	Виконав
10.	Підготовка до попереднього захисту, підготовка до захисту	12-15.06.2023	Виконав
11.	Отримання рецензії, відповіді на зауваження рецензента	16-17.06.2023	Виконав
12.	Захист роботи	19-30.06.2023	Виконав

Дипломник _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			ФКС 56. 01 000. 00 ДП	Дипломний проект		
А4			ФКС 56. 01 000. 00 ДП ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	ФКС 56. 01 000. 00 ДП		
Розробив		Арнаутов Д.Р.			Модернізація ІТ-середовища сучасного підприємства на основі міжнародних стандартів з кібербезпеки	Літ.	Аркуш 3 / Аркушів
Перевірив		Стайкуца С.В.				НДП	
Н. Контр.		Петрашова В.І.				ВСП "ОТФК ОНТУ" гр.4ФКС-56	
Затверд.		Кривченко Ю.В.					

ЗМІСТ

ВСТУП

Бізнес-процеси сучасних компаній і безперервність їх діяльності все більше залежать від інформаційної інфраструктури компанії. Сервери і робочі станції, активне і пасивне мережеве обладнання, програмне забезпечення та безліч сервісів - все це веде до глибокої інтеграції реального і віртуального корпоративних світів. Разом з тим, кіберсередовище несе безліч загроз і ризиків, для боротьби з якими необхідні алгоритми та методики.

За інформацією від Symantec, в 2022 році збиток інтернет-користувачів від хакерів склав 172 млрд доларів. В цілому від кібершахраїв постраждали 978 млн чоловік з 20 країн світу (Австралія, Бразилія, Великобританія, Німеччина, Гонконг, Індія, Індонезія, Іспанія, Італія, Канада, Китай, Мексика, Нідерланди, Нова Зеландія, ОАЕ, Сінгапур, США, Швеція , Франція і Японія).

Варто відзначити, що навіть при таких ризиках і загрозах не всі підприємці приділяють належну увагу питанням інформаційної безпеки. При цьому ризику піддаються всі сторони бізнес-взаємодії - компанія, співробітники, клієнти, посередники, підрядники і в цілому всі учасники робочого процесу. Зайва економія на безпеці, недбалість співробітників, незнання нормативно-правової бази, відкритість інформаційної структури підприємства уможливлює витік в кіберпростір конфіденційної корпоративної інформації та персональних даних. Все це веде до зниження ділової репутації, штрафів, падіння конкурентоздатності та потенційного банкрутства.

Технології рухають світ вперед і все більша кількість корпоративних процесів буде проводитися в кіберсередовищі. Знання нормативно-правової бази, застосування ефективних організаційних, програмно-апаратних та інших рішень, періодичне проведення аудитів безпеки - необхідність і умова збереження і розвитку сучасних компаній.

1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Класифікація, склад та основні компоненти IT-середовища

Інформаційні технології стають невід'ємною частиною бізнесу і запорукою ефективної роботи підприємства. В той же час індустрія інформаційних технологій розвивається дуже швидко. На сьогодні неможливо представити жодного підприємства без таких необхідних речей, як комп'ютер, інтернет, Wi - Fi-роутер і телефон. Особливістю малого бізнесу, як об'єкту застосування інформаційних технологій, є те, що власник бізнесу зазвичай не розбирається в програмуванні та операційних системах, але відмінно орієнтується у веденні свого бізнесу. У великих же підприємствах між власником і творцями інформаційних технологій стоїть безліч фахівців, що координують їх діяльність.

IT-інфраструктура - це комплексна структура, яка об'єднує всі інформаційні технології та ресурси, що використовуються конкретною організацією або компанією. Інформаційно-технологічна інфраструктура включає всі комп'ютери, встановлене ПЗ, системи зв'язку, інформаційні центри, мережі та бази даних. Інформаційна інфраструктура - це система організаційних структур, підсистем, що забезпечують функціонування і розвиток інформаційного простору країни і засобів інформаційної взаємодії.

IT-інфраструктура включає в себе сукупність інформаційних центрів, підсистем, банків даних і знань, систем зв'язку, центрів управління, апаратно-програмних засобів і технологій забезпечення збору, зберігання, обробки і передачі інформації, а також забезпечує доступ споживачів до інформаційних ресурсів.

Таким чином, об'єднуючи все вище сказане, можна запропонувати наступне визначення IT-інфраструктури. Інфраструктура інформаційних технологій (IT-інфраструктура) - це організаційно-технічне об'єднання

програмних, обчислювальних і телекомунікаційних засобів, зв'язків між ними і експлуатаційного персоналу, що забезпечує надання інформаційних, обчислювальних і телекомунікаційних ресурсів, можливостей і послуг працівникам (підрозділам) підприємства (організації), необхідних для здійснення професійної діяльності та вирішення відповідних бізнес-завдань. Модель підприємства, що використовує у своїй діяльності інформаційні технології, представлена на рис. 1.1.

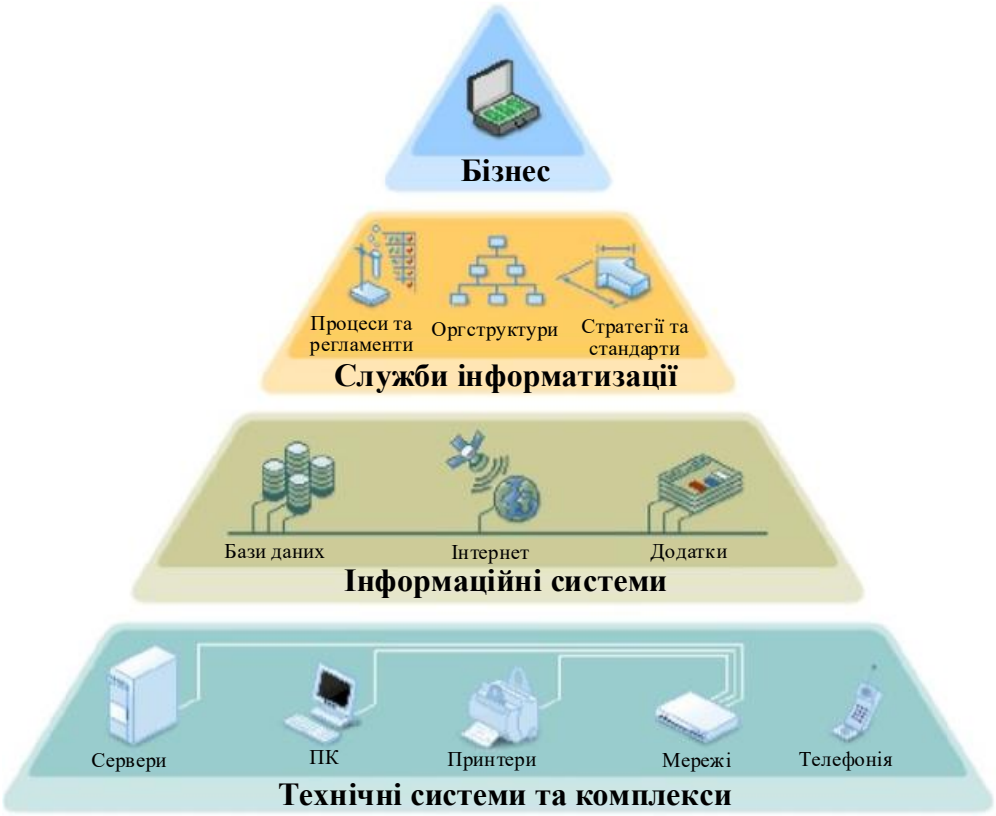


Рисунок 1.1. Модель підприємства на основі інформаційних технологій

Таким чином, якщо в організації є хоч один персональний комп'ютер або ноутбук, на ньому встановлено програмне забезпечення і є вихід в Internet, все це використовується для здійснення професійної діяльності, то присутня повноцінна IT-інфраструктура мінімального розміру.

Уміло і вірно вибудувана IT-інфраструктура підприємства може в рази підвищити прибутковість бізнесу, скоротити витрати і непродуктивні витрати, збільшити віддачу від роботи і значно полегшити діяльність компанії.

IT-інфраструктура - це не просто фундамент для існування будь-якої сучасної компанії. В даний час IT стає стратегічним активом, який є рушійною силою бізнесу. Побудова надійної IT-інфраструктури, що задовольняє бізнес процесів компанії - непросте завдання, практично не має вирішення власними силами IT-відділу компанії. Найголовніше, що IT-інфраструктура повинна задовольняти потребам бізнесу компанії. Одна з можливих інформаційних структур компанії представлена на рис.1.2

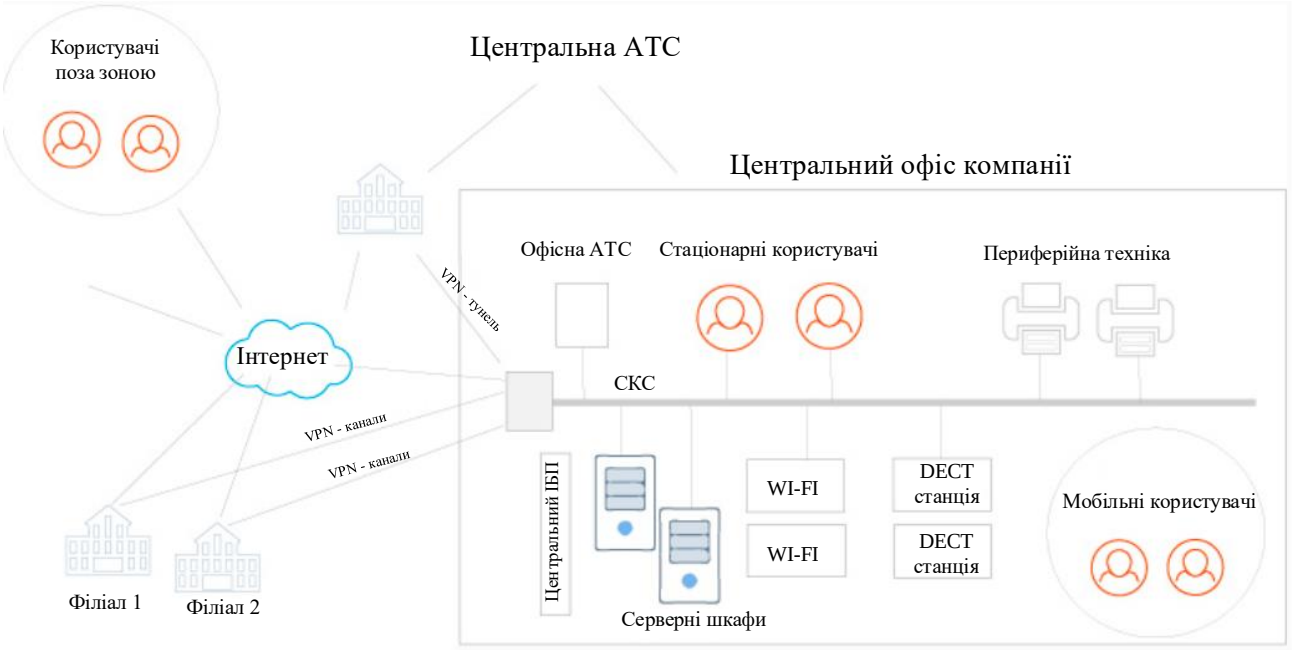


Рисунок 1.2. Приклад схеми інформаційної інфраструктури

Динаміка ринку, безліч факторів у бізнес-середовищі, загрози та ризики різного характеру вимагають від бізнесу та його інформаційної інфраструктури адекватної та своєчасної реакції на зміни середовища функціонування.

Інформаційна інфраструктура - це не просто набір окремих IT-рішень, які опинилися об'єднаними в рамках одного підприємства, а багаторівнева інтегрована система, що підтримує життєдіяльність всієї організації. Правильно вибудувану інформаційну інфраструктуру підприємства відрізняють три ключові ознаки:

− комплексне функціонування всіх частин інформаційної системи;

− промислова і функціональна сумісність;

− максимальний комфорт у використанні.

ІТ-інфраструктура сучасного підприємства повинна мати гнучкість, високу готовність, бути максимально стійкою до змін фізичних, технологічних, соціальних та інших умов функціонування. При цьому слід зазначити, що ефективно спроектована інформаційна інфраструктура здатна протистояти зовнішнім та внутрішнім загрозам, джерелами яких є техніка, природне, соціальне середовище тощо.

В основі інфраструктури інформаційної системи підприємства, в першу чергу, лежать структуровані кабельні системи (електрична мережа, телефонія, локально-обчислювальна мережа та ін.). Також передача даних може бути організована і по бездротовій мережі. На рис. 1.2 представлені основні компоненти (найважливіші складові) інформаційної інфраструктури сучасного підприємства.

Кабельна мережа, в свою чергу, має на увазі не тільки середовище передачі даних (локально-обчислювальні мережі, телефонні мережі та інше), але також і електромережу, без якої поки ще неможливо функціонування жодної системи ІТ-інфраструктури. Таким чином, найважливіші складові інформаційної інфраструктури:

− комунікаційне середовище (кабельне чи/або безпроводове);

− обладнання (активне і пасивне мережеве обладнання, серверне обладнання, робочі станції, оргтехніка (МФУ, принтери, сканери, факси), периферійні пристрої, телефонія);

− програмне забезпечення.

Для того щоб досягти необхідного результату при адекватних витратах, потрібно спроектувати оптимальну для конкретного бізнесу інфраструктуру, і робити це слід виходячи із завдань підприємства, чітко оцінивши значущість кожної з них.

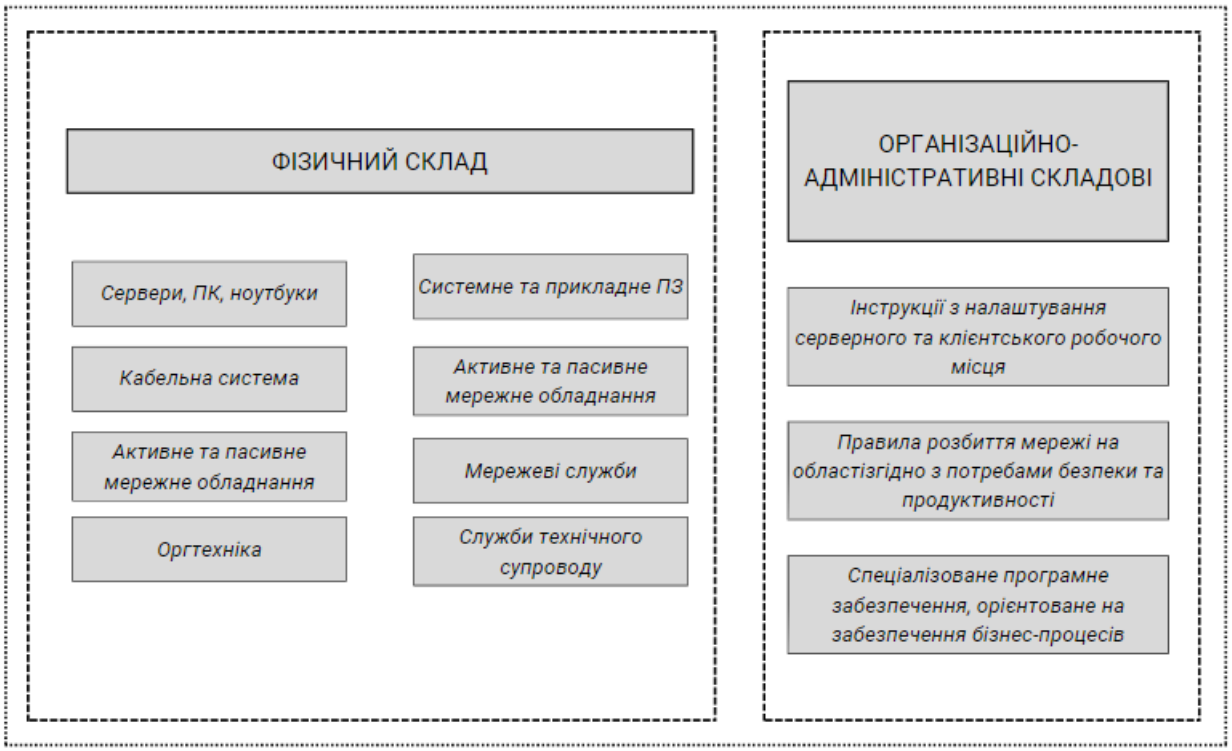


Рисунок 1.3. Склад IT-інфраструктури сучасного підприємства

Базова інфраструктура задовольняє базові потреби організації в сервісах, необхідних для роботи і є платформою для підтримки і розгортання служб і додатків, критичних для бізнесу компанії. У зв'язку з цим надійність інфраструктурного ядра повинна знаходитися на високому рівні.

Додаткова інфраструктура надає сервіси і служби, необхідні для вирішення конкретних завдань підприємства. Ці послуги не є обов'язковими і розгортаються в залежності від потреб самої організації. Функціонування цих служб безпосередньо залежить від якості роботи ядра інформаційної інфраструктури.

Базова IT-інфраструктура складається з ряду основних компонентів, які представлені на рис. 1.4.

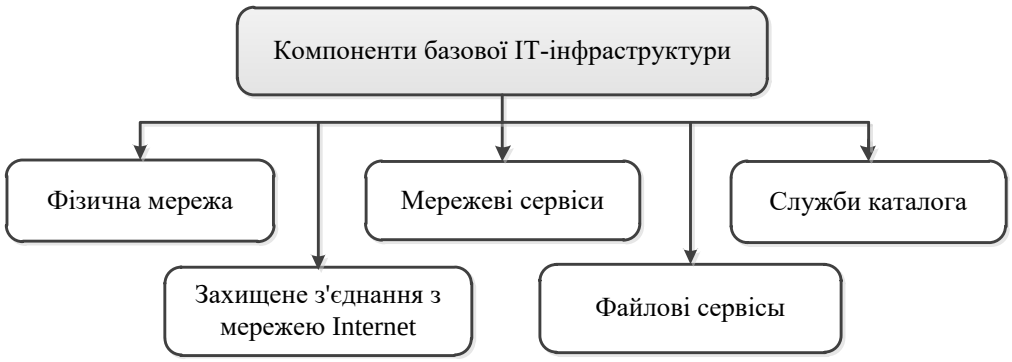


Рисунок 1.4. Компоненти базової IT-інфраструктури

Додаткова інфраструктура складається з наступних компонентів:

– управління і налаштування параметрів безпеки за допомогою групових політик;

– електронна пошта;

– спільна робота;

– сервіси друку;

– віддалений доступ;

– служби сертифікації;

– управління оновленнями;

– антивірусний захист;

– резервне копіювання і відновлення.

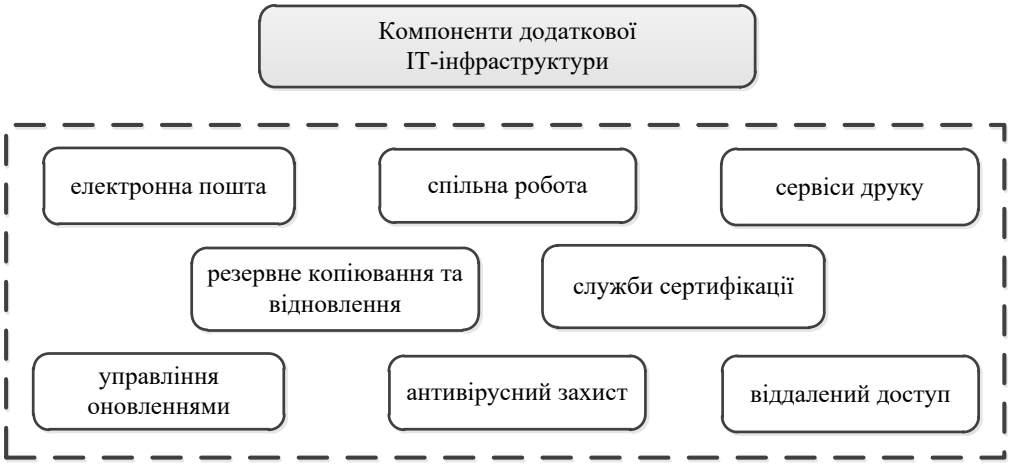


Рисунок 1.5. Компоненти додаткової IT-інфраструктури

Створення ефективної IT-інфраструктури – досить складний процес, що вимагає високого рівня компетенцій у різних напрямках IT. Потрібно проаналізувати велику кількість інформації, щоб зрештою отримати ефективну IT-інфраструктуру, що відповідає потребам бізнесу.

Для того, щоб проступити до планування майбутньої IT-інфраструктури потрібно:

- провести аналіз бізнес-процесів організації;

- провести аудит IT-інфраструктури (якщо планується модернізація IT-інфраструктури або міграція на нову);

- провести аналіз доступних на ринку рішень, продуктів, технологій та оцінити вартість їх володіння (витрати на придбання, експлуатацію, обслуговування);

- розрахувати бюджети та співвіднести можливості з потребами;

Результатом етапу планування IT-інфраструктури є затверджена цільова архітектура, яка відповідає потребам бізнесу як з точки зору ефективності, так і економічних показників.

Після закінчення планування IT-інфраструктури розробляється технічне завдання для виконавців із впровадження, яке описує:

– специфікацію необхідного обладнання та програмного забезпечення;

– технології та рішення, які будуть використовуватись, їх застосування;

– топологію мережі, схему мережі;

– опис глобальних налаштувань ключових компонентів IT-інфраструктури;

– опис необхідних робіт та їх обсягу;

– програму та методику випробувань (тестування);

– здачу IT-інфраструктури в експлуатацію.

У довгостроковій перспективі інформаційну інфраструктуру потрібно не лише спроектувати та впровадити, їй також необхідно керувати. Управління інфраструктурою передбачає контроль над її поточним станом, своєчасне

виявлення проблем, і навіть прийняття рішень. Управління IT-інфраструктурою необхідне для її надійного функціонування, надання надійних сервісів та вимірювання їхньої якості.

Якщо в компанії встановлено більше 1 ПК і ці комп'ютери не з'єднані між собою, виникає велика кількість проблем:

- витрачається багато часу на пошук та відновлення інформації
- файли передаються на зовнішні носії
- неможливо працювати віддалено, бо інформація стає недоступною
- вкладення у канали зв'язку, оплату провайдерів, оргтехніку стають неефективними
- якщо співробітник йде з компанії – складно відновлювати інформацію

Всі ці та багато інших проблем легко вирішуються за допомогою правильної організації інфраструктури.

У міжнародній практиці прийнята наступна класифікація IT-систем:

1. Mission Critical - системи, що працюють в «бойовому» режимі. До таких систем відносяться:

- критично важливі для бізнесу та навколишнього середовища системи і програмні додатки,
- центри управління (моніторингу, безпеки, адміністрування) мережею (ЦУМ),
- технологічні додатки, що працюють в режимі реального часу.

Вихід з ладу згаданих систем тягне за собою непоправні втрати для бізнесу, несе загрозу для життя і здоров'я співробітників компанії. Рекомендований час аварійного відновлення подібних систем - не більше 10 хвилин. Для таких систем повинні використовуватися спеціалізовані серверні платформи і інфраструктурні рівні з багаторазовим резервуванням компонентів, в тому числі з використанням резервних віддалених ЦОД (центр обробки даних).

Рисунок 1.6. Класифікація ІТ-систем за рівнем безперервності

2. Business Critical - системи, критично важливі для бізнесу, з режимом роботи 24 × 7 × 365.

Вихід з ладу цих систем тягне за собою серйозні втрати для бізнесу. Рекомендований час аварійного відновлення подібних систем - не більше 2-х годин. Для таких систем повинні використовуватися кластерні рішення і інфраструктурні рівні з частковим резервуванням використовуваних компонентів.

3. Business Operational - звичайні бізнес-додатки - системи, які не потребують роботи в реальному часі, з режимом роботи 8 × 5. Рекомендований час аварійного відновлення подібних систем - 4-6 годин. Для таких систем рекомендується використовувати резервування зберігання даних і електроживлення.

4. Office Production - додатки, не критичні для ведення бізнесу. Вихід з ладу цих систем не впливає на динаміку ключових показників ефективності (КПЕ) підприємства. Рекомендований час аварійного відновлення подібних систем - 1-2 робочих дня.

Важливо відзначити, що показники загальної безперервності бізнесу залежить від рівня безперервності і відмовостійкості «найслабшої ланки».

1.2 Проведення аналізу міжнародних стандартів та рекомендацій з напрямку кібербезпеки

Стандарти кібербезпеки (також звані стандарти кібербезпеки) - це методи, зазвичай викладені в опублікованих матеріалах, які намагаються захистити кіберсередовища користувача або організації. Це середовище включає самих користувачів, мережі, пристрої, все програмне забезпечення, процеси, інформацію, що зберігається або передається, програми, служби та системи, які можуть бути безпосередньо або опосередковано пов'язані з мережами..

Основна мета - знизити ризики, включаючи запобігання чи пом'якшення кібератак. Ці опубліковані матеріали складаються зі збірок інструментів, політик, концепцій безпеки, заходів безпеки, посібників, підходів до управління ризиками, дій, навчання, передових методів, гарантій та технологій.

Стандарт кібербезпеки може бути визначений як набір правил, які організація повинна дотримуватись, щоб отримати право на деякі конкретні речі, такі як прийом онлайн-платежів, зберігання даних про пацієнтів тощо. Стандарти складаються з деяких основних правил, яким організація повинна підкорятися для забезпечення відповідності будь-якому зі стандартів кібербезпеки. Виходячи з вимог підприємства чи організації, існує кілька різних стандартів, які можуть вибрати для надання спеціальних можливостей. У деяких місцях уряд має свій власний стандарт, згідно з яким кожен повинен підкорятися, хто готовий працювати на уряд.

Стандарти кібербезпеки також можуть бути пояснені як список політик, які мають застосовуватись у системі для забезпечення відповідності будь-якому стандарту. Наприклад, якщо будь-яка організація хоче приймати онлайн-платежі, вона має відповідати стандарту PCI DSS. Існують деякі суворі правила, які підпадають під цю відповідність, яких організація повинна дотримуватись, щоб мати право обробляти онлайн-платежі. Їхня система має бути сучасною, вільною від уразливостей, вони мають дуже часто генерувати мережеві звіти, і подібні речі включені до стандартів. Якщо організація може надати надійні звіти, вони

можуть приймати онлайн-платежі, інакше вони не зможуть вимагати оплати через свій онлайн-інтерфейс. Існує ряд стандартів кібербезпеки, які повинні захищати систему та її користувачів у різний спосіб. Залежно від того, які дані мають бути захищені, є різні стандарти. Розглянемо їх детальніше.

1.2.1 Стандарт ISO 27001

Це один із загальноприйнятих стандартів, які дотримуються організації для впровадження системи управління інформаційною безпекою. Він складається з набору процедур, у якому викладено правила та вимоги, які мають бути виконані для сертифікації організації відповідно до цього стандарту. Відповідно до цього стандарту, організація повинна підтримувати всі технології в актуальному стані, сервери повинні існувати без уразливостей, і організація повинна піддаватися аудиту після заданого інтервалу, щоб залишатися скомпільованою відповідно до цього стандарту. Це міжнародний стандарт, і кожна організація, яка обслуговує іншу організацію, яка відповідає цьому стандарту, повинна дотримуватись політики СМІБ, охопленої практикою ISO 27001.

ISO 27001 вимагає від керівництва:

- систематичного вивчення ризиків інформаційної безпеки організації з урахуванням загроз, уразливостей та впливів;

- розроблення та впровадження послідовного та всеосяжного пакету засобів контролю інформаційної безпеки та/або інших форм обробки ризиків (таких як запобігання або передача ризиків) для усунення тих ризиків, які вважаються неприйнятними;

- впровадження всеосяжного процесу управління, щоб гарантувати, що засоби управління інформаційною безпекою продовжують постійно задовольняти потреби організації в інформаційній безпеці.

Офіційна назва стандарту – «Інформаційні технології – Методи безпеки – Системи менеджменту інформаційної безпеки – Вимоги». ISO/IEC 27001: 2013 містить десять коротких розділів плюс довгий додаток, що охоплює:

1. Сфера дії стандарту

2. Як робиться посилання на документ

3. Повторне використання термінів та визначень у ISO/IEC 27000

4. Організаційний контекст та зацікавлені сторони

5. Лідерство в галузі інформаційної безпеки та підтримка політики на високому рівні

6. Планування системи управління інформаційною безпекою; оцінка ризиків; обробка ризику

7. Підтримка системи управління інформаційною безпекою

8. Введення в дію системи управління інформаційною безпекою

9. Перевірка продуктивності системи

10. Коригуюча дія

Додаток А: Список елементів керування та їх цілі

ISO 27001 - це універсальний стандарт управління інформаційними ризиками, призначений для посібника з вибору адекватних та пропорційних засобів контролю для захисту інформації. ISO 27001 був створений для використання кращої моделі, яка встановлює, впроваджує, експлуатує, контролює, аналізує, підтримує і, нарешті, покращує СМІБ.

ISO 27001 охоплює широкий спектр елементів безпеки, включаючи ключові галузі, такі як політика безпеки компанії, управління активами, фізична та екологічна безпека, контроль доступу тощо. Візуалізація основних елементів безпеки стандарту ISO 27001 представлена на рис. __

Наприклад, управління активами домену безпеки повинно мати такі елементи керування: Усі активи повинні бути чітко ідентифіковані, а опис усіх важливих активів повинен бути складений та вестись. Правила прийнятного використання інформації та активів, пов'язаних із засобами обробки інформації, мають бути визначені, задокументовані та реалізовані. Відповідний набір процедур для маркування та обробки інформації має бути розроблений та реалізований відповідно до схеми класифікації, прийнятої в організації. Для кожного з цих 14 доменів безпеки ISO 27001 складається з 114 конкретних

заходів контролю, організованих навколо 35 цілей контролю, щоб забезпечити вибір адекватних та пропорційних заходів безпеки для захисту інформаційних активів.

Рисунок 1.7. Структура стандарту ISO 27001

Рисунок 1.8. Основні елементи безпеки стандарту ISO 27001

1.2.2 Стандарт ISO 27032

Структура стандарту з кібербезпеки Міжнародний стандарт ISO 27032 виконаний в стилі ризик-орієнтованого підходу, хоча і відрізняється від національних стандартів ГОСТ 27001 і ГОСТ 27005, прив'язаних до 4-процесної моделі життєвого циклу. Стандарт визначає активи кіберпростору і зацікавлені сторони, загрози, рекомендації та заходи з обробки ризиків, причому в якості специфічної заходи виділені вказівки по координації дій та обміну інформацією.

За аналогією з класичним визначенням інформаційної безпеки в стандарті під кібербезпекою фактично розуміють властивість захищеності активів від загроз конфіденційності, цілісності, доступності, але в деяких абстрактних рамках - кіберпросторі.

Кіберпростір формулюється як комплексна віртуальне середовище (яка не має фізичного втілення), сформована в результаті дій людей, програм і сервісів в мережі Інтернет за допомогою відповідних мережевих і комунікаційних технологій. Сутностями кіберпростору можуть бути віртуальні гроші, аватари, хмари, віртуальні посольства, віртуальні злочину, віртуальні розваги тощо.

Рисунок 1.9. Базові блоки стандарту ISO 27032:2012

Що стосується власне забезпечення кібербезпеки, то в якості пріоритету

виділена координація взаємодії між організаціями, що формують кіберпростір, самостійні дії яких не забезпечують ефективний захист від кіберзагроз.

Тезаурус кібербезпеки інтегрований з поняттями інформаційної безпеки, безпеки додатків, мережевої безпеки, безпеки Інтернет, а також безпеки критичної інформаційної інфраструктури.

Безпека додатків визначається щодо програмних додатків, а також інформаційно-програмних ресурсів і процесів, що беруть участь в їх життєвому циклі. Безпека мереж пов'язана з проектуванням, впровадженням та використанням мереж всередині організації, між організаціями, між організаціями і користувачами. Безпека в мережі Інтернет стосується інтернет-послуг і відповідних систем інформаційно-комунікаційних технологій і мереж. Безпека критичної інформаційної інфраструктури характеризує захищеність від відповідних загроз, в тому числі загроз інформаційній безпеці. Ілюстрація співвідношення названих понять (як її побачили в міжнародному комітеті ISO JTC 1) представлена на рисунку 1.10.

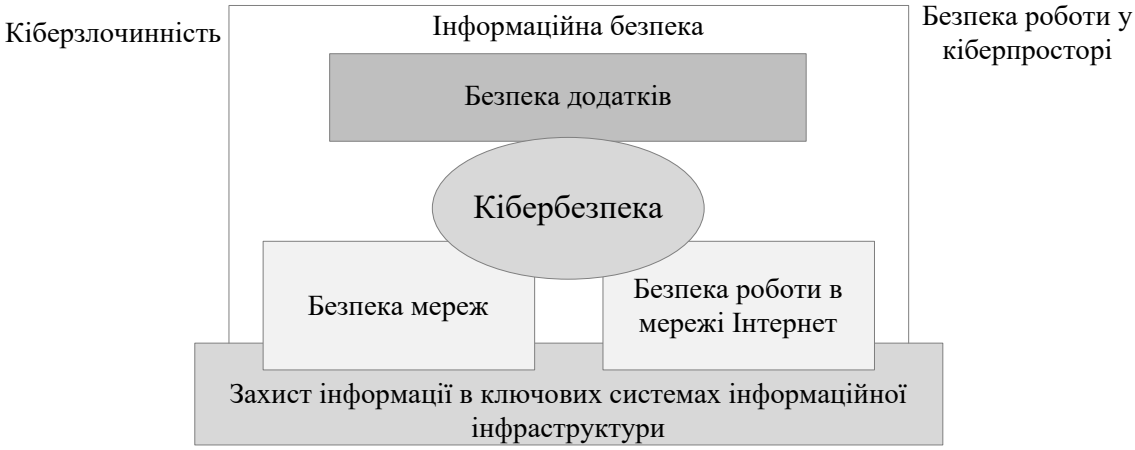


Рисунок 1.10. Положення кібербезпеки щодо інших сфер безпеки

Як відомо, до активів в області безпеки традиційно відносять все, що представляє цінність, наприклад, інформаційні та програмні ресурси. Незважаючи на «віртуальний» акцент у визначенні кібербезпеки, в стандарті активи можуть бути як віртуальними так і фізичними, наприклад: віртуальний

аватар і фізичний пристрій - USB-ідентифікатор.

Розділяють дві групи активів:

– персональні активи (наприклад, дані особистої банківської карти);

– активи організації (наприклад, URL-адресу організації).

Відповідно таксономія кіберзагроз має традиційну схему, яка включає класифікації за видами і типами активів, зовнішнім і внутрішнім ознаками, цілям, джерел і т.д.

Онтологія кібербезпеки представлена на рис.1.11, який являє собою адаптацію відповідної схеми з ISO / IEC 15408-1. Як видно з рисунку, більш пильна увага в області кібербезпеки приділяється зловмисним загрозам.

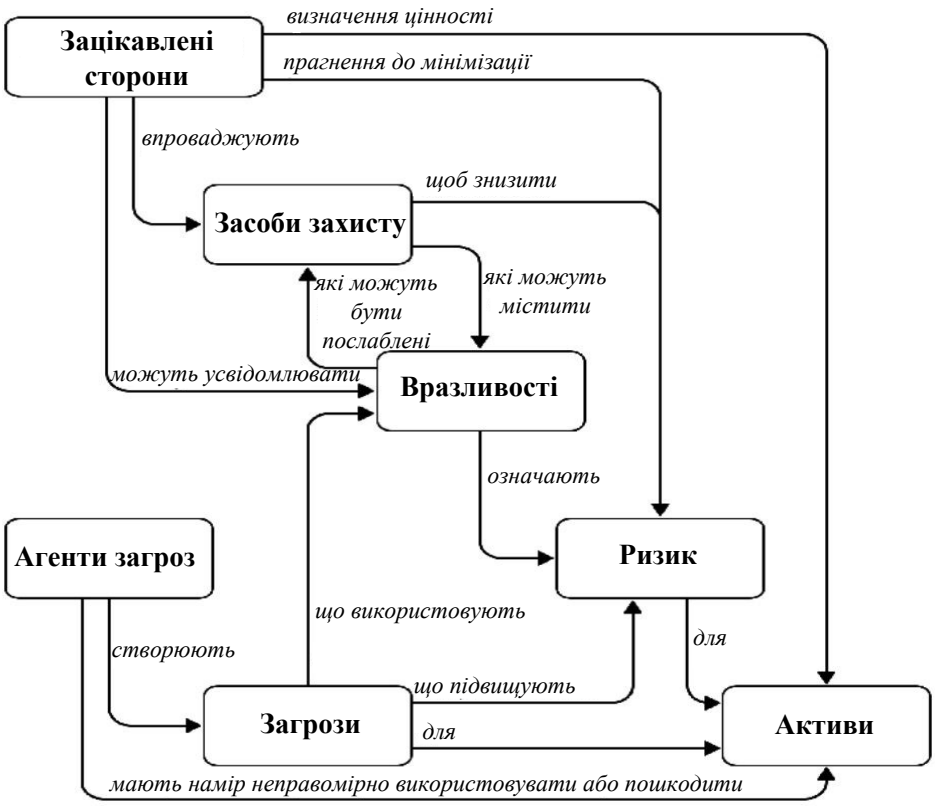


Рисунок 1.11.Основні поняття безпеки і характер зв'язків між ними

З метою планування забезпечення кібербезпеки стандарт являє три керівництва:

– рекомендації з оцінки та відпрацювання ризиків,

– рекомендації щодо дотримання вимог безпеки користувачами,

– рекомендації щодо забезпечення кібербезпеки для організацій-провайдерів.

Рекомендації з оцінки та обробці ризиків спираються на ISO 27005, акцентуючи увагу лише на особливостях кібербезпеки, наприклад, необхідність прийняття додаткової відповідальності щодо зацікавлених осіб в області кібербезпеки в плані звітності, інформованості, обліку різних законодавчих аспектів, забезпечення узгодженості дій споживачів і провайдерів на випадок інцидентів і заходів по забезпеченню безпеки.

Рекомендації для користувачів становлять сукупність норм поведінки, визначених провайдером, а саме:

– розуміння політики безпеки сайту або програми,

– розуміння ризиків безпеки,

– дотримання політики безпеки персональних даних,

– управління безпекою особистих даних,

– інформування уповноважених органів про підозрілі явища або повідомленнях,

– перевірка достовірності і розуміння політики безпеки торгових майданчиків (у разі здійснення віртуальної торгової угоди),

– контролювання цілісності використовуваного і програмного забезпечення, що,

– забезпечення безпеки онлайн-публікацій і блогів,

– дотримання корпоративної політики інформаційної безпеки в кіберпросторі,

– негайне інформування уповноважених органів про особисті порушення безпеки.

Настанови організаціям пропонують широкий комплекс заходів з управління інформаційною безпекою організацією, а саме:

– впровадження та сертифікація системи менеджменту інформаційної безпеки,

– надання безпечних продуктів, які пройшли відповідну оцінку,

– тестування, моніторинг мереж та реагування,

– техпідтримка,

– підтримання рівня своєї поінформованості щодо новітніх розробок,

– підвищення обізнаності користувачів,

– контроль дотримання політики безпеки тощо

Конкретні заходи забезпечення кібербезпеки можуть бути визначені за результатами оцінки ризиків і в рамках планування дій щодо підвищення безпеки активів. Стандарт являє ряд базових заходів, спрямованих на рішення задач:

– забезпечення безпеки додатків,

– забезпечення безпеки серверів,

– забезпечення безпеки кінцевих користувачів,

– захисту від атак методами соціальної інженерії,

– підвищення готовності.

Детального розгляду заслуговують заходи, що стосуються підвищення готовності систем, представлені в окремому додатку до стандарту:

– моніторинг darknet-мереж,

– «сінкхолінг»,

– зворотне трасування.

Нагадаємо, darknet («порожня мережу») – підмножина публічних IP-адрес, які не використовуються організацією для реальної роботи. Звернення до даної підмножини адрес, таким чином, можливо лише в результаті помилок конфігурації або нелегітимності дій, наприклад, з метою первинної розвідки шляхом сканування. У стандарті описані три варіанти darknet-моніторингу:

– метод по типу «чорної діри» (black hole),

– метод слабкої взаємодії,

– метод сильного взаємодії.

Сінкхолінг (sinkhole-метод, метод «зливної труби») являє собою спосіб перенаправлення підозрілого IP-трафіку в альтернативне «зливний» пристрій (як

правило, маршрутизатор) з метою пересилання трафіку DDoS-атак, блокування і аналізу бот-мереж і ін. Недоліком сінкхолінга є те, що атакується IP-адреса не може використовуватися для зв'язку з легітимними користувачами, поки маршрут не буде видалений.

Методи зворотного трасування (traceback) включають методи реконструювання маршрутів атак і виявлення місця розташування вузлових центрів зловмисників шляхом коректування маршрутної інформації, відстеження маркованих пакетів, аудиту журналів і т.д. Найбільш проблемною є міждоменне зворотнє трасування через необхідність вирішення питань сумісності протоколів і архітектури, технічних і організаційних питань обробки інформації конфіденційного характеру та ін.

Таблиця 1.1 - Базові заходи кібербезпеки

Категорія безпеки	Міра безпеки
Безпека додатків	Повідомлення користувачів про політику безпеки
	Захист сесій веб-додатків
	Контроль коректності даних, що вводяться (захист від SQL-інжекції)
	Забезпечення безпеки скриптів (захист від атак міжсайтового скриптинга)
	Аудит коду і незалежне тестування програмного коду
	Підтвердження справжності провайдера для споживачів
Безпека серверів	Безпечне конфігурація серверів
	Установка системи оновлень безпеки
	Захист від шкідливих програм
	Регулярне сканування контенту на наявність шкідливих програм
	Регулярне сканування вразливостей сайту і додатків
	Виявлення спроб злому
Безпека кінцевих користувачів	Використання рекомендованих версій операційних систем
	Використання рекомендованих версій програмних додатків
	Використання антивірусних засобів
	Налаштування веб-браузерів в безпечному режимі
	Блокування або безпечне виконання скриптів
	Використання фільтрів фішингу

	Використання додаткових механізмів безпеки веб-браузерів
	Використання персональних міжмережевих екранів і систем виявлення вторгнень
	Використання автоматичних оновлень довірених програм
Захист від атак методами соціальної інженерії	Розробка і впровадження політик безпеки
	Категоріювання і класифікація інформації
	Навчання і підвищення обізнаності користувачів
	тестування співробітників
	Мотивація і стимулювання співробітників
	Використання технічних механізмів контролю
Підвищення готовності	Використання пасток в «порожній» мережі
	Перенаправлення шкідливого трафіку
	Зворотнє трасування

1.2.3 Стандарт PCI DSS

Стандарт PCI DSS (Payment Card Industry Data Security Standard) – це сукупність вимог щодо забезпечення безпеки даних власників платіжних карток, які зберігаються, передаються та/або обробляються в інформаційній інфраструктурі організацій.

Основне завдання стандарту PCI DSS – це забезпечення безпеки мережевої інфраструктури і захист даних власників платіжних карток, що зберігаються, так як це найбільш вразливі місця, що безпосередньо загрожують конфіденційності та втраті коштів. Для того щоб мати гарантію безпеки збереження коштів своїх клієнтів, такі компанії, як, наприклад, VISA і MasterCard вимагають від торгових підприємств і різних постачальників послуг, які приймають платежі від покупців через дані платіжні системи, відповідати стандарту PCI DSS.

Стандарт PCI DSS регламентує правила експлуатації платіжних систем, а також процедури їх розробки і моніторингу.

Вимоги стандарту PCI DSS розповсюджуються на торгові підприємства, банки, постачальників різноманітних послуг і сервісів, роздрібні магазини, call-центри, платіжні шлюзи та на інші підприємства і організації, діяльність яких

пов’язана з обробкою, передачею і зберіганням даних власників платіжних карток.

Стандарт безпеки даних PCI DSS визначає дванадцять вимог до відповідності, організованих у шість логічно пов'язаних груп, які називаються «мети контролю», а саме:

- створення та підтримка безпечної мережі та систем
- захист даних про власників карток
- підтримка програми управління вразливістю
- реалізація суворих заходів контролю доступу
- регулярно відстежуйте та тестуйте мережі
- підтримуйте політику інформаційної безпеки

У кожній версії PCI DSS (Стандарт безпеки даних індустрії платіжних карток) ці шість вимог по-різному розділені на додаткові вимоги, але дванадцять вимог високого рівня не змінилися з моменту появи стандарту.

Дванадцять вимог для побудови та обслуговування безпечної мережі та систем можна резюмувати так:

1. Встановлення та обслуговування міжмережевого екрана конфігурація для захисту даних власників карток. Призначення брандмауера – сканувати весь мережевий трафік, блокувати доступ до системи через ненадійні мережі.

2. Зміна стандартних заводських налаштувань для системних паролів та інших параметрів безпеки. Ці паролі легко виявляються через загальнодоступну інформацію та можуть використовуватися зловмисниками для отримання несанкціонованого доступу до систем.

3. Захист даних про власників карток. Шифрування, хешування, маскування та усічення - це методи, що використовуються для захисту даних власників карток.

4. Шифрування передачі даних власників карток по відкритих загальнодоступних мережах. Надійне шифрування, включаючи використання лише довірених ключів та сертифікатів, знижує ризик злому зловмисниками.

5. Захист усіх систем від шкідливих програм та регулярне оновлення антивірусного програмного забезпечення. Шкідливе програмне забезпечення може проникати в мережу безліччю способів, включаючи використання Інтернету, електронну пошту співробітників, мобільні пристрої або пристрої зберігання.

6. Розробка та підтримка безпечних систем та додатків. Уразливості в системах та додатках дозволяють несумлінним особам отримати привілейований доступ. Необхідно негайно встановити виправлення безпеки, щоб виправити вразливість та запобігти використанню та компрометації даних власників карток.

7. Обмеження доступу до даних власників карток лише уповноваженому персоналу. Системи та процеси повинні використовуватися для обмеження доступу до даних про власників карток на основі «необхідності знати».

8. Ідентифікація та аутентифікація доступу до системних компонентів. Кожній особі, яка має доступ до компонентів системи, має бути призначений унікальний ідентифікатор (ID), який дозволяє контролювати доступ до критично важливих систем даних.

9. Обмеження фізичного доступу до даних власників карток. Фізичний доступ до даних власників карток або систем, що зберігають ці дані, повинен бути безпечним для запобігання несанкціонованому доступу або видаленню даних.

10. Відстеження та моніторинг будь-якого доступу до даних власників карток та мережевих ресурсів. Повинні бути передбачені механізми реєстрації для відстеження дій користувачів, які є критично важливими для запобігання, виявлення або мінімізації впливу компрометації даних.

11. Регулярне тестування систем та процесів безпеки. Постійно виявляються нові вразливості. Системи, процеси та програмне забезпечення необхідно часто тестувати, щоб виявити вразливості, які можуть бути використані зловмисниками.

12. Підтримка політики інформаційної безпеки для персоналу. Сильна політика безпеки включає розуміння персоналом важливості даних та їх відповідальності за їх захист

Рисунок 1.12. Вимоги щодо побудови та обслуговування безпечної мережі з позиції стандарту PCI DSS

1.2.4 Політики відповідності HIPAA

Дані про стан здоров'я належать до чутливої категорії персональних даних і володіють більшим ступенем захисту, ніж інші категорії персональних даних. Саме тому дані про стан здоров'я потребують окремого правового регулювання, яке б впорядковувало їх збір та використання. Найбільш відомим прикладом такого регулювання є прийнятий у 1996 році Закон США про мобільність та підзвітність медичного страхування (англ. "Health Insurance Portability and Accountability Act" або "HIPAA").

HIPAA – це закон, який врегульовує мобільність та підзвітність медичного страхування і встановлює стандарти захисту медичної звітності та особистих медичних даних пацієнтів. HIPAA визначає, які дані пацієнтів захищаються (англ. "protected health information" або "PHI"), а також хто повинен дотримуватись вимог HIPAA при роботі з PHI.

Дотримання вимог HIPAA - це безперервний процес, який включає впровадження надійних заходів захисту даних, навчання персоналу, оцінку ризиків, звітність та багато іншого.

HIPAA відносить до PHI такі категорії даних:

- минулі та актуальні дані про стан здоров'я особи (зокрема, анамнез особи, її діагноз, результати проведених медичних досліджень, призначене лікування);
- дані про надання медичних послуг особі; та
- минулі та актуальні дані про оплату наданих медичних послуг, які надають можливість ідентифікувати особу, або ж є достатня підстава вважати, що особу можна ідентифікувати за такими даними.

Варто зауважити, що дані про особу, за якими зазвичай її ідентифікують, як от місце проживання, ім'я та прізвище, податковий номер тощо не є PHI та не охоплюються HIPAA. Однак, якщо поруч з такими даними є інформація про стан здоров'я чи надання медичних послуг, то в сукупності такі дані становитимуть PHI і охоплюватимуться HIPAA.

Вимоги відповідності HIPAA включають п'ять основних компонентів:

Конфіденційність: регулює використання та розкриття інформації про пацієнта.

Безпека: фізичні, технічні та адміністративні заходи безпеки.

Правозастосування: містить інструкції щодо регулювання відповідальності та накладення штрафів за порушення.

Повідомлення про порушення: рекомендації про те, як і коли повідомляти про порушення Omnibus: описує, як ділові партнери повинні звертатися з PHI.

Правило безпеки HIPAA описує три типи заходів безпеки – адміністративні, фізичні та технічні – для належного захисту PHI.

Адміністративні гарантії.

Адміністративні заходи безпеки допомагають співробітникам зрозуміти, як правильно використовувати та зберігати закриту медичну інформацію.

Ці заходи безпеки призначені для:

Навчання співробітників захисту PHI

Усунення інцидентів безпеки, які можуть становити загрозу PHI

Захист PHI під час надзвичайних ситуацій

Фізичні гарантії

Фізичні заходи безпеки захищають фізичні точки доступу до PHI. Фізичні заходи безпеки визначають, як працівники повинні керувати своїми робочими станціями та мобільними пристроями, щоб забезпечити безпеку конфіденційної інформації.

Загальні фізичні заходи безпеки включають обмеження доступу до об'єкта за допомогою камер спостереження або ідентифікаційних карток, а також визначення належного та неналежного використання технологій.

Технічні гарантії

Технічні засоби захисту захищають від несанкціонованого доступу або зміни PHI, яка зберігається в електронному вигляді, наприклад, у програмі або системі. Виділимо технічні засоби захисту:

Мережеве шифрування — шифруйте будь-який ePHI відповідно до стандартів шифрування NIST щоразу, коли він передається зовнішньою мережею. (Обов'язковий)

Керування доступом — кожному користувачеві призначається централізовано кероване унікальне ім'я користувача та PIN-код для доступу до систем. Також повинні бути передбачені процедури, які визначають, коли розкривати або розкривати ePHI під час надзвичайної ситуації. (Обов'язковий)

Аутентифікація ePHI. Ви повинні ідентифікувати та аутентифікувати ePHI та захистити його від пошкодження, несанкціонованих змін та випадкового знищення. (Рекомендований)

Шифрування пристроїв. Всі кінцеві пристрої, які мають доступ до системи, повинні мати можливість шифрувати та розшифровувати дані, що особливо важливо для мобільних пристроїв та ноутбуків. (Рекомендований)

Аудит дій щодо контролю. Для відстеження всіх спроб доступу до ePHI та відстеження того, як обробляються дані ePHI, потрібне докладне ведення журналу. (Рекомендований)

Увімкнути автоматичний вихід із системи: користувачі повинні виходити з системи через певний період часу, зазвичай від 30 секунд до 3 хвилин в залежності від програми або системи (рекомендований).

Для виконання вимог HIPAA необхідно організувати:

Контролює доступ до об'єктів. Ви хочете ретельно відстежувати конкретних осіб, які мають фізичний доступ до сховища даних, — не лише інженерів, а й ремонтників і навіть сторожів. Ви також повинні вжити розумних заходів для блокування несанкціонованого доступу. (Необхідний)

Керування робочими станціями - напишіть політику, яка обмежує, які робочі станції можуть отримувати доступ до даних про стан, описуєте, як екран має бути захищений від сторін, що знаходяться на відстані, та вказуєте належне використання робочої станції. (Обов'язковий)

Захист мобільних пристроїв. Вам потрібна політика для мобільних пристроїв, яка видаляє дані перед тим, як пристрій буде передано іншому користувачеві. (Обов'язковий)

Відстеження серверів. Ви хочете, щоб уся ваша інфраструктура була в інвентарі разом із інформацією про те, де вона знаходиться. Повністю скопіюйте всі дані перед переміщенням серверів. (Рекомендовані)

Для того, щоб гарантовано впровадити принципи HIPAA, необхідно виконання низки дій, до яких належать:

1. Оцінка ризиків – ідентифікуйте, аналізуйте, створюйте та вживайте заходів для усунення наслідків, виконуючи комплексну оцінку ризиків для всіх даних про стан здоров'я. (Обов'язковий)

2. Систематичне керування ризиками. Оцінка ризиків є безперервним процесом, який необхідно переоцінювати через регулярні проміжки часу з вживання заходів для зниження ризиків до належного рівня. Політика санкцій має бути введена для співробітників, які не дотримуються правил HIPAA. (Обов'язковий)

Рисунок 1.13. Компоненти технічного захисту PHI

3. Навчання персоналу. Вам необхідно навчити співробітників усім протоколам доступу до ePHI і розпізнавати потенційні ризики кібербезпеки, такі як фішинг, злом і обман. Записи цих сесій мають зберігатися. (Рекомендовані)

4. Управління непередбачуваними обставинами. Ви повинні мати можливість забезпечити постійну безперервність бізнесу, реагуючи на аварії за допомогою процесу підготовки, що забезпечує безпеку даних. (Обов'язковий)

5. Перевіряйте свої непередбачувані обставини. Ви повинні регулярно перевіряти свій план дій у непередбачених обставинах щодо всього ключового програмного забезпечення. Повинна бути прийнята система резервного копіювання та політика відновлення. (Рекомендовані)

6. Блокування несанкціонованого доступу. Переконайтеся, що сторони, яким не надано доступ, наприклад, субпідрядники або материнські компанії, не можуть переглядати ePHI. Підписати угоди про ділове співробітництво з усіма партнерами. (Обов'язковий)

7. Документуйте всі інциденти, пов'язані з безпекою. Зверніть увагу, що цей крок не пов'язаний із правилом сповіщення про порушення, які стосуються реальних успішних зламів. Інцидент безпеки може бути зупинений усередині компанії, перш ніж дані будуть зламані. Персонал повинен розпізнавати такі випадки та повідомляти про них. (Рекомендовані)

Рисунок 1.14. Виконання дій для впровадження принципів HIPAA

На перший погляд може видатись, що HIPAA є подібним до GDPR. Однак, це не зовсім так. HIPAA поширюється на збір та обробку лише медичних персональних даних, під його дію потрапляє особливе коло осіб, яким надано доступ до цієї групи даних. Також, відповідно до HIPAA, можна здійснювати розкриття PHI в цілях лікування без попередньої згоди пацієнта, в той час як за GDPR основною підставою для розкриття даних про стан здоров'я є однозначна згода пацієнта (за умови, якщо пацієнт здатний свідомо надати таку згоду).

Окрім того, HIPAA не надає право пацієнту вимагати від закладу охорони здоров'я видалити його медичні дані, на відміну від GDPR.

1.2.5 Стандарт NIST 7621

Міжвідомчий звіт NIST(NISTIR) 7621 створений для допомоги в розумінні того, як забезпечити безпеку інформаційних систем підприємства. Він створений на основі співпраці між урядом і приватним сектором і використовує спільну мову для вирішення і управління рисками кібербезпеки.

З огляду на глибину опрацювання напрямки, документ, незважаючи на невеликий обсяг, досить змістовний, і може стати основою для формування політики безпеки інформаційної інфраструктури компанії

На рис. 1.15 представлено структуру документу NIST 7621.

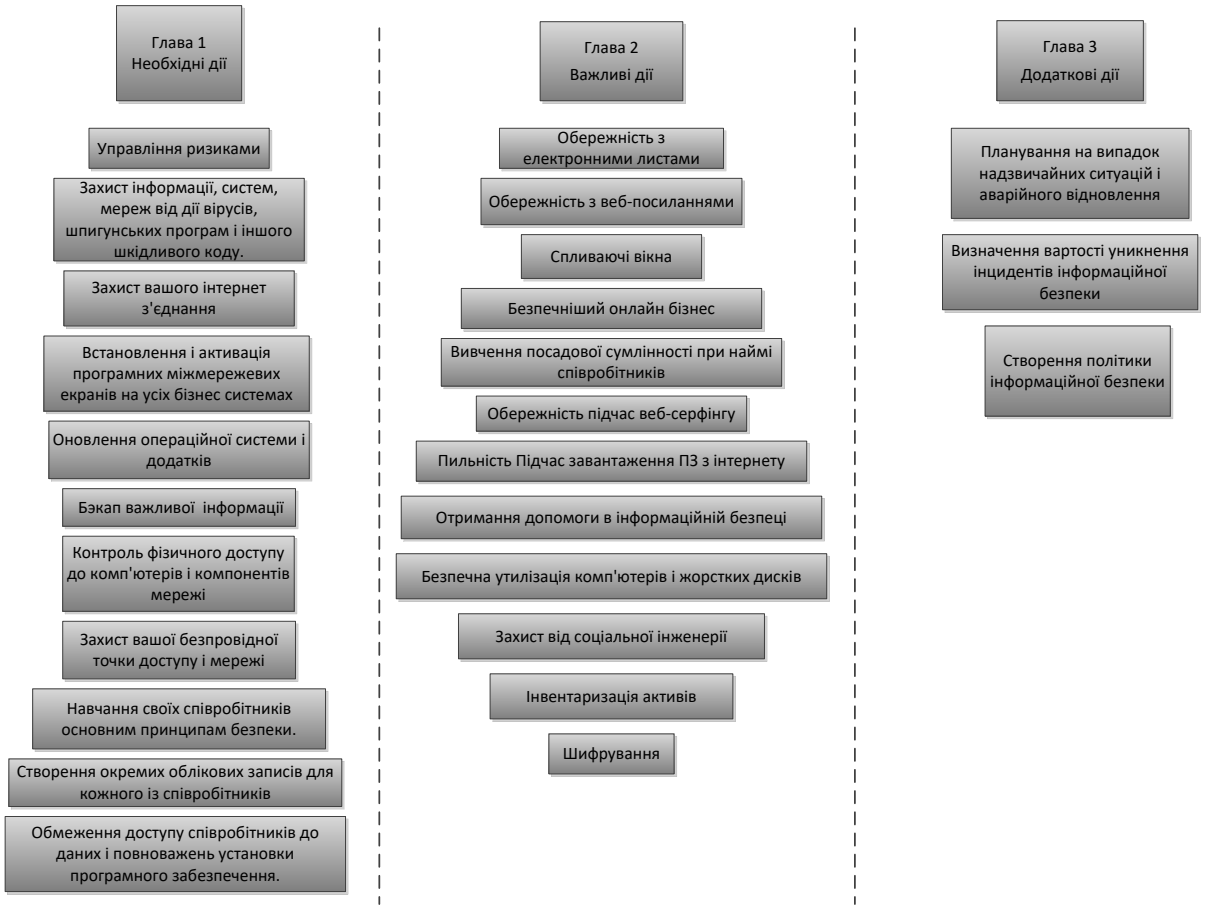


Рисунок 1.15. Структура документу NIST 7621

Заходи захисту по NIST 7621 можуть виконувати наступні функції: ідентифікація, захист, виявлення, реагування, відновлення. Усі заходи і їх функції приведені в таблиці 2.1.

Таблиця 1.2 – Консолідована таблиця NIST 7621

Дії		Функції кібербезпеки
Необхідні дії		
1	Управління ризиками	Ідентифікація, захист
2	Захист інформації, систем, мереж від дії вірусів, шпигунських програм і іншого шкідливого коду.	Захист
3	Захист вашого інтернет з'єднання	Захист
4	Встановлення і активація програмних міжмережевих екранів на усіх бізнес системах	Захист, виявлення
5	Оновлення операційної системи і додатків	Захист
6	Бекап важливої інформації	Реагування, відновлення
7	Контроль фізичного доступу до комп'ютерів і компонент мережі	Захист, виявлення
8	Захист вашої безпровідної точки доступу і мережі	Захист
9	Навчання своїх співробітників основним принципам безпеки.	Захист
10	Створення окремих облікових записів для кожного із співробітників	Захист
11	Обмеження доступу співробітників до даних і повноважень установки програмного забезпечення.	Захист
Важливі дії		
1	Обережність з листами	Захист, виявлення
2	Обережність з веб-посиланнями	Захист, виявлення
3	Спливаючі вікна	Захист, виявлення
4	Безпечніший онлайн бізнес	Захист
5	Вивчення посадової сумлінності при наймі співробітників	Захист
6	Обережність при веб-серфінгу	Захист
7	Пильність при скачуванні ПЗ з інтернету	Захист
8	Отримання допомоги в інформаційній безпеці	Ідентифікація, захист, виявлення, реагування, відновлення
9	Безпечна утилізація комп'ютерів і жорстких дисків	Ідентифікація, захист
10	Захист від соціальної інженерії	Захист, виявлення
11	Інвентаризація активів	Ідентифікація
12	Шифрування	Захист
Додаткові дії		
1	Планування на випадок надзвичайних ситуацій і аварійного відновлення	Ідентифікація, захист, виявлення, реагування, відновлення
2	Визначення вартості уникнення інцидентів інформаційної безпеки	Захист
3	Створення політики інформаційної безпеки	Ідентифікація, захист, виявлення, реагування, відновлення

Рисунок 1.16 – Формування профілю безпеки в залежності від дій та функцій кібербезпеки

1.2.6 Регламент захисту персональних даних (GDPR)

У 2018 році як для B2C, так і для B2B компаній виникла необхідність систематизації роботи з персональними даними для відповідності GDPR (the General Data Protection Regulation). GDPR (загальний регламент щодо захисту даних), затверджений Європейською Комісією в 2016 році, покликаний замінити існуючу директиву 95/46 / ЕС [13], яка була правовою фундаментом захисту інформації в ЄС з 1995 року. Абсолютно точно можна сказати, що поліпшення з позиції GDPR несуть як якісний, так і кількісний характер. Так, регламент описує і доопрацювання існуючих вимог, і впровадження рішень актуальних проблем (наприклад, збір і обробка даних для подальшого використання з метою

профілювання маркетингових кампаній, що викликало великий резонанс в ЗМІ в 2018 році).

Варто зазначити, що дія GDPR поширюється не тільки на підприємства, які працюють в рамках Європейського Союзу, але також і на всі компанії, які володіють або обробляють дані його громадян, надають їм товари, сервіс або відстежують активність і інтереси користувачів.

На рис. 1.17 представлені ключові статті загального регламенту щодо захисту даних.

Керівництво також описує ряд питань, наприклад:

− способи збору, обробки, зберігання і знищення персональних даних (ПД) організаціями та окремими підприємцями

− ступінь відповідності бізнес-процесів компанії чинним правовим нормам і спрямованість на мінімізацію інформаційних потоків з ПД (в цілях безпеки)

− загальний внесок в безпеку підприємств та інформаційне співтовариство в цілому шляхом детального опису аспектів ІБ в рамках GDPR.

Нівелювання вимог GDPR може викликати суттєві фінансові штрафи. Санкції за невідповідність регламенту можуть досягати 20 мільйонів євро або 4% річного обороту (вибирається те, що більше). Суворі покарання впроваджені, щоб показати справжню вартість ПД і прав людини на конфіденційність. Також це дієвий стимул для прискорення процесу впровадження норм і правил регламенту. На практиці найкращим показником необхідності таких поліпшень є зниження довіри людей до інтернет-ресурсів. Все більш масовий характер набирають обурення громадськості про неможливість залишатися поза проведеної аналітики для формування цільової аудиторії і ведений маркетингових кампаній на основі існуючих даних про кожного користувача у вигляді його інтернет активності, а також поширення баз контактних даних, що тягне за собою подальші "холодні" розсилки , дзвінки тощо., що явно можна віднести до однієї з актуальних проблем, з якою також бореться GDPR, а саме - спам.

Рисунок 1.17. Ключові статті GDPR

Велика розмаїтість слабких місць інтернет-ресурсів призводить лише до зниження лояльності користувачів до мережі, а це включає в себе проблеми більшого характеру - зниження онлайн продажів, активності в соціальних мережах і т.д. Саме такі об'єктивні характеристики і є безумовною опорою для підтвердження необхідності роботи над інформаційною безпекою і відповідністю GDPR.

Найбільше уваги в Регламенті приділяється таким поняттям як BigData, моніторинг активності і профілювання по інтересам громадян, згода на обробку, зберігання, передачу ПД, використання cookies і питання безпеки вже на стадії розробки (наприклад, шифрування даних, псевдонімізація), право на забуття, доступ і зміна інформації про себе, а також отримання інформації як в зрозумілому для людини вигляді, так і в машинно-читається.

Для контролерів і обробників інформації це тягне за собою перегляд і зміна робочих процесів усередині компанії, як показано на рис. 4.3, які знизять рівень ризику для ПД:

− організаційного та правового характеру всередині компанії (наприклад,

інструктажі для персоналу, правова база, угоди про нерозголошення);

− взаємодії з третіми особами (наприклад, закупівлі або аутсорсинг);

− правила ведення звітності;

− активне спілкування з користувачами (повідомлення про зміни, збір погоджень);

− розробка програмних і технічних рішень для задоволення прав користувачів;

− розробка плану дій в разі витоків або зломів.

Рисунок 1.18. Етапи успішного впровадження вимог GDPR

Регламент є великим склепінням інструкцій і правил, як і попередні, але детальність і зрозумілість подальшого впровадження лише допомагають відповідати на можливі запитання ще до їх виникнення. Всі існуючі регламенти, директиви, закони та стандарти в результаті націлені на одне: надавати кращий сервіс клієнтам і людям, які довіряють інтернет-ресурсу для них інформацію. Впровадження змін для відповідності GDPR потребують багато зусиль і викличе стрес у вас і ваших співробітників, так як побудова прозорої системи для всього циклу життя інформації це завдання, яка зажадає детального і всебічного аналізу

існуючого робочого процесу, існуючих договорів, інтерфейсів програм, сайтів, пристроїв, а також прояв проактивної взаємодії з базою клієнтів але, якщо це робить користувачів більш впевненими в інтернет-мережі, показує стурбованість проблемами цифрового суспільства, це в в результаті призведе до зростання підприємств, які працюють в інтернет-ніші, як результат роботи Регламенту. У структурі сучасного підприємства Регламент торкнеться кожну сферу, в яку потрапляють персональні дані громадян ЄС. Співробітник має доступ до файлів, які містять ПД, тільки в разі, якщо вони йому дійсно необхідні для роботи, а мета їх використання чітко вказана в політиці безпеки та умов конфіденційності, з якими погодився користувач.

1.2.7 Стандарт HB 292:2006

У стандарті HB 292:2006 процес управління безперервністю бізнесу розглядається як складова більш загального процесу управління ризиками. При цьому беруться до уваги ризики, як внутрішні, так і зовнішні, які знаходяться за межами безпосереднього контролю організацією. Наприклад, це можуть бути внутрішні ризики стратегічного рівня, що впливають на діяльність організації в цілому, або ризики операційного рівня, локально впливають на бізнес-процеси організації. Також береться до уваги, що наслідки ризиків можуть бути різними і призводити до фінансових втрат, юридичних переслідувань, втрати іміджу та репутації, переслідувань з боку регулюючих органів, переривань бізнесу та ін.

Вважається, що управління ризиками визначає організаційні і технічні контрзаходи, які спрямовані в першу чергу на запобігання подій, що переривають бізнес. Управління безперервністю бізнесу розглядається як складова управління ризиками, що дозволяє визначити економічно виправдані контрзаходи, прийняті в разі переривань бізнесу. По суті BCM стосується фактичних подій – реалізації загроз безперервності бізнесу – і дій, які необхідно зробити у відповідь на ці події. У цьому сенсі BCM і доповнює процес управління ризиками, який по хворій частині стосується ймовірності реалізації

загроз переривань бізнесу і вибору превентивних заходів захисту від таких подій.

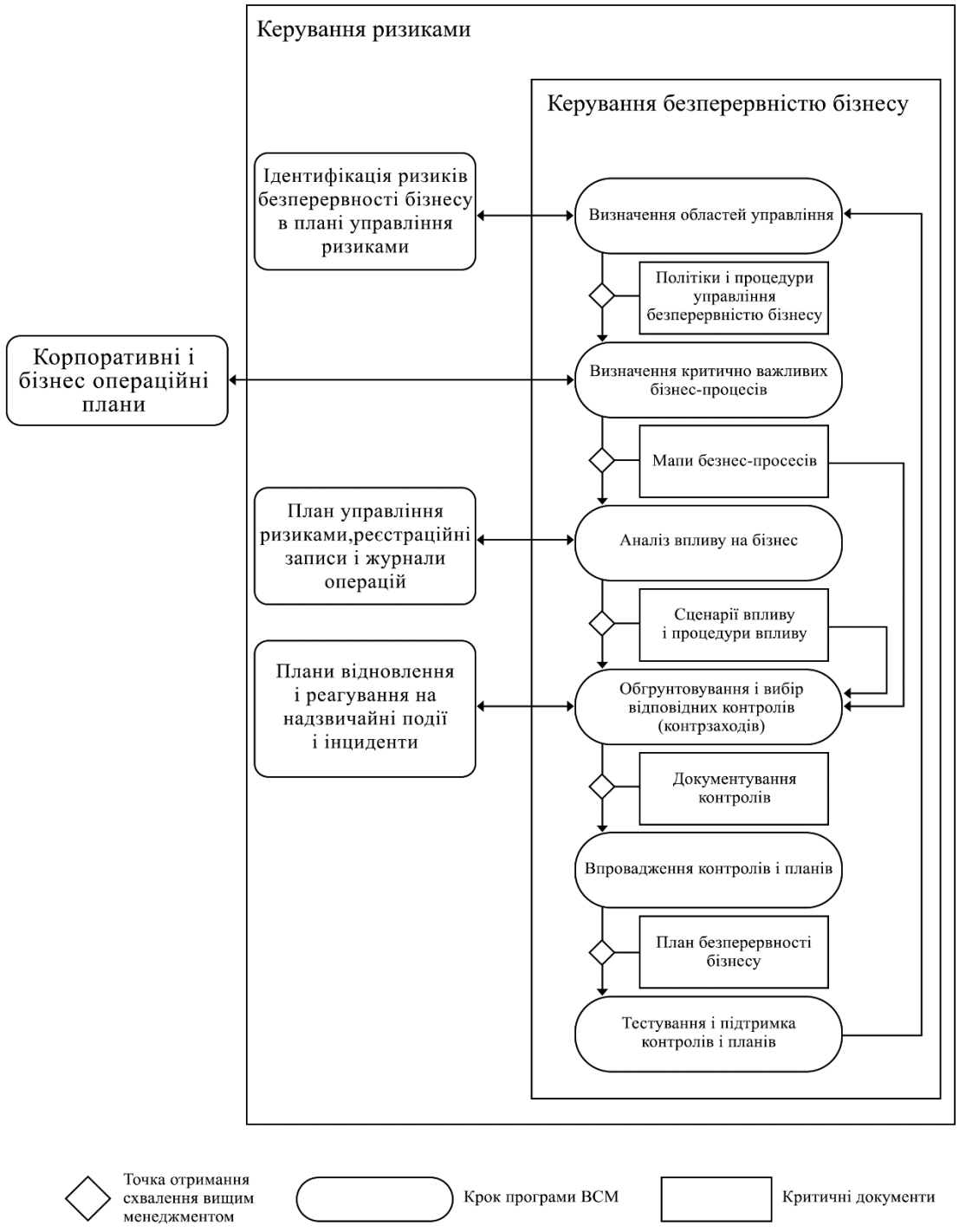


Рисунок 1.19. Рекомендації ANAO з управління ризиками і безперервністю бізнесу

На рис. 1.20 представлений алгоритм управління ризиками переривань бізнесу, який складається з наступних чотирьох кроків:

1) визначення характеристики бізнесу;

2) оцінка залишкових ризиків;

3) впровадження необхідних контрзаходів;

4) оцінка ефективності прийнятих контрзаходів

Рисунок 1.20. Опис процесу управління ризиками

У стандарті НВ 292:2006 підкреслюється, що основною метою ВСМ є підтримання в актуальному стані достатньої кількості ресурсів, необхідних для стабільного функціонування організації в надзвичайних ситуаціях.

1.3 Методи та засоби підвищення рівня захисту ІТ-інфраструктури на основі стандартів з кібербезпеки

1.3.1 Етап і алгоритми захисту на основі стандарту NIST 7621

Розглянемо більш детально основні етапи захисту кіберсередовища згідно NIST 7621.

1. Управління ризиками.

Ризик менеджмент - це процес ідентифікації ризиків, до яких схильний ваш бізнес, і управління цими рисками за рахунок реалізації захисних заходів для мінімізації виявлених ризиків.

Оцінка ризиків - дія з виявлення ризиків, до яких схильний ваш бізнес. Оцінка ризиків включає виявлення загроз вашому бізнесу і вразливостей вашого бізнесу перед кожною з цих загроз.

Оскільки велика частина власників/менеджерів малого бізнесу не є професіоналами у сфері інформаційної безпеки, увесь це набір дій слід надати фірмі підрядникові (яка, бажано, спеціалізується на оцінці ризиків малого бізнесу). Підрядники повинні провести тестування систем і мереж підприємства, а саме, провести процес пошуку вразливостей програмного і апаратного забезпечення. Можливо, це може бути організовано засобами професіоналів внутрішнього відділу кібербезпеки при наявності організаційно-штатної структури.

Слід влаштовувати щорічний незалежний аудит IT-безпеки для підтвердження ефективності програми IT-безпеки. Щорічні перевірки повинна проводити компанія, відмінна від тієї, що забезпечувала інформаційну безпеку. Це допоможе забезпечити "належну сумлінність" при захисті корпоративної інформації, у тому випадку, якщо інциденти кібербезпеки мають місце бути.

2. Встановіть, використайте та регулярно оновлюйте антивірус і антишпигун на кожному комп'ютері, який використовуєте.

Налаштуйте антивірус для перевірки оновлень вночі(наприклад, опівночі), після чого виставите час сканування (наприклад, 12:30). Графік оновлення і перевірки анти-шпигунського програмного забезпечення можна виставити так само як і анти-вірусного, але із затримкою в декілька годин (2:30 і 3:00). Плануйте їх так, що б одночасно відбувався тільки один вид діяльності.

Хорошою ідеєю буде придбати копії вашого антивірусного програмного забезпечення для будинку вам і вашим співробітникам, оскільки багато хто любить працювати вдома

3. Забезпечте безпечне підключення до Інтернету.

Більшість компаній мають широкосмуговий доступ до мережі Інтернет. Важливо мати на увазі, що при такому типу доступу до мережі Інтернету комп'ютер піддається загрозам 24 години в добу 7 днів в тиждень .

При використанні широкосмугового доступу до мережі Інтернет важливо встановити і підтримувати працюючим апаратний міжмережевий екран між вашою внутрішньою мережею і мережею Інтернет. Цю функцію може виконувати безпроводова точка доступу/маршрутизатор або це може бути функцією маршрутизатора, який надається постачальником послуг Інтернету. Якщо співробітники працюватимуть вдома, переконаєтеся, що домашні мережі усіх працівників захищені апаратним брандмауером.

Регулярно міняйте паролі брандмауера. Змініть ім'я адміністратора, оскільки значення за умовчанням легко вгадуються.

Необхідно мати програмні брандмауери на кожному комп'ютері, навіть якщо у вас є апаратний брандмауер, що захищає вашу мережу. Якщо ваш апаратний брандмауер буде скомпрометований хакерами або яким-небудь шкідливим кодом, зловмисник або шкідлива програма отримає повний доступ до комп'ютера та інформації на ньому.

4. Встановіть та активуйте програмне забезпечення брандмауерів на усіх бізнес-системах.

Встановіть, використайте і постійно оновлюйте програмний брандмауер на кожному комп'ютері системи. Переконайтеся в тому, що брандмауер включений. Існують комерційні програмні міжмережеві екрани, які можна придбати за розумною ціною або використовувати безкоштовно. Переконайтеся, що у співробітників включені міжмережеві екрани. Необхідно мати програмні брандмауери на кожному комп'ютері, навіть якщо у вас є апаратний брандмауер.

На випадок, якщо апаратний брандмауер зламаний хакером або шкідливим кодом

5. Оновлюйте вашу операційну систему і додатки.

Усі виробники операційної системи надають патчі і оновлення для своїх продуктів для виправлення проблем безпеки і поліпшення їх функціональності. Так, Microsoft надає щомісячні патчі в другий вівторок кожного місяця.

6. Зробіть резервні копії важливих даних.

Використовуйте резервне копіювання даних на кожному комп'ютері. Необхідно створити резервну копію даних, оскільки жорсткі диски ломаються, співробітники роблять помилки і шкідливі програми можуть знищити дані на комп'ютерах. Без резервного копіювання даних, можна легко потрапити в ситуацію, коли ви повинні оновити свої дані з паперових копій і інших ручних файлів. Робіть це автоматично, якщо це можливо. Автоматичне резервне копіювання треба робити не рідше, ніж один раз в тиждень і зберігати на окремому жорсткому диску на вашому комп'ютері, або в автономному режимі з використанням знімного носія або інтернет-сховища. Процедура повинна бути виконана на кожному з корпоративних комп'ютерів. Важливо періодично перевіряти резервні копії даних, щоб переконатися в тому, що інформаційний носій читається. Важливо робити повну резервну копію один раз в місяць і зберігати її чимдалі від вашого офісу у безпечному місці. Якщо щось станеться з офісом (пожежа, повінь, крадіжки тощо), дані будуть у повній цілості в іншому

7. Контролюйте фізичний доступ до комп'ютерів і мережевих компонентів.

Не допускайте сторонніх осіб до ваших комп'ютерів. Це включає блокування ноутбуків, коли вони не використовуються. Розмістіть дисплеї комп'ютерів так, щоб ті, щоб люди, які проходять повз, не могли бачити інформацію на екрані. Управління доступом до систем і мереж також включає в себе формування повної впевненості в тих, хто має доступ до систем або мереж. Це включає ”обслуговуючий персонал”, який приходить в службові приміщення в нічний час прибирання. Злочинці часто намагаються отримати таку роботу з

метою злому комп'ютерів для отримання важливої інформації, яку вони розраховують знайти там. Також необхідно бути обережним з ремонтним персоналом, для якого також легко вкрасти особисту або конфіденційну інформацію і вийти з нею так, що ніхто не помітить.

8. Безпека безпроводової точку доступу.

Якщо ви використовуєте безпроводову мережу, краще зробіть так, щоб вона не транслювала SSID, тобто зробіть її прихованою та змініть пароль адміністратора. Важливо використовувати шифрування, щоб ваші дані при передачі між АРМ та безпроводовою точкою доступу не могли бути прочитаними за допомогою прослуховування. Рекомендується шифрування Wi - Fi Protected Access 2(WPA - 2) за допомогою Advanced Encryption Standard(AES) для безпечного шифрування.

9. Навчайте ваших співробітників сновним принципам безпеки.

Співробітників, що використовують будь-які програми, які містять конфіденційну інформацію, слід навчити правильно її використовувати та захищати. В перший же день роботи ваших нових співробітників вони повинні вивчити вашу політику інформаційної безпеки і те, що вони повинні робити, для захисту вашої конфіденційної ділової інформації. Крім того, пояснити їм ваші вимоги із приводу обмеження особистого користування телефонами, принтерами, і будь-якою іншою власністю вашого бізнесу або наданими ресурсами. Після цього тренінгу, вони повинні підписати твердження про те, що вони розуміють вашу бізнес-політику, наслідуватимуть її, і розуміють штрафні санкції за її недотримання. Встановіть правила, які описують, як обробляти і захищати дані про клієнтів і інші бізнес-дані. Вони можуть забороняти брати корпоративну інформацію (бізнес-дані) додому або включати правила роботи в домашніх умовах. Ефективною інвестицією буде навчання співробітників основам інформаційної, системної і мережевої безпеки

10. Окремі облікові записи для кожного із співробітників на комп'ютерах і в додатках.

Створіть для кожного співробітника окремий обліковий запис з надійним паролем для кожного з працівників. Пароль повинен складатися з випадкової послідовності букв, цифр і спеціальних символів. Його довжина повинна складати не менш, ніж 8 символів, краще більше. Для кращого захисту інформаційних систем переконайтеся, що усі співробітники використовують облікові записи, які не мають права адміністратора. Це зупинить будь-яку спробу встановлення несанкціонованого програмного забезпечення. Без окремих облікових записів для кожного користувача важко притягнути кого-небудь до відповідальності за втрату або несанкціоноване маніпулювання. Паролі можуть стати загальновідомими, якщо їх не міняти, тому мають бути змінені принаймні, кожні 3 місяці.

11. Обмежте доступ співробітників до даних, а також обмежте повноваження встановлення програмного забезпечення.

Не надавайте доступ до усіх даних у будь-якому працівникові. Для усіх співробітників забезпечуйте доступ тільки до тих систем та інформації, яка їм потрібна для виконання службовим обов'язків. Не дозволяйте одній людині одночасно ініціювати та схвалювати угоду. Гірка правда полягає в тому, що інсайдери - ті, хто працює у вас в компанії, - є джерелом великої небезпеки. Причина полягає в тому, що вони вже знаходяться усередині вашої організації, їм довіряють, та вони мають доступ до важливої ділової інформації.

На рис. 2.2 представлено консолідовану структуру, що відображує основні етапи формування захисту згідно NIST 7621.

Розглянемо додаткові алгоритми захисту згідно NIST 7621, які детально представлені на рис. 2.3

1. Будьте обережні з електронною поштою та її вкладеннями, особливо, якщо в листі знаходиться конфіденційна інформація.

Не відкривайте вкладення електронної пошти, якщо ви не чекаєте листа з додатком, або ви не довіряєте відправнику. Одним з найбільш поширених засобів поширення шпигунського або шкідливого коду є вкладення електронної пошти. Зазвичай, ці загрози прикріплені до електронних листів, які змінюють

адресу відправника. Варто подзвонити людині, яка відправила повідомлення і якщо вона його дійсно відправила, запитати про вкладення. Іноді комп'ютер людини заражений шкідливим кодом, який використовує комп'ютер для розсилки електронних листів від імені власника кожному, хто знаходиться в адресній книзі. Ці електронні листи, як правило, мають копії шкідливого коду у вигляді вкладень і намагаються встановити шкідливий код на комп'ютері будь-кого, хто отримує електронну пошту і відкриває вкладення. Остерігайтеся електронних листів, які просять конфіденційну інформацію, незалежно від того, хто є відправником. Ніхто не проситиме конфіденційну інформацію.

Рисунок 1.21. Основні та додаткові етапи формування захисту згідно NIST 7621

2. Будьте обережні з веб-посиланнями в електронній пошті, миттєвими повідомленнями, соціальними засобами масової інформації.

Не натискайте на посилання в електронних повідомленнях. Після того, як одержувач натискає на посилання, шкідливе програмне забезпечення встановлюється на комп'ютер користувача. Не відкривайте посилання, якщо ви не знаєте, до якого сайту воно веде або не довіряєте людині, яка послала вам електронну пошту. Краще подзвонити відправнику та запитати, з якою метою відправлено посилання. Перевірте, чи співпадає фактичне посилання з тим, що представлено в листі. Наведіть курсор миші на посилання та звірте адресу посилання з тим, яке з'явиться в нижній частині вікна браузеру.

3. Стежте за шкідливими спливаючими вікнами і іншими хитрощами хакерів.

При використанням мережі Інтернет, не реагуйте на спливаючі вікна із запитом про натиснути кнопку "ОК" для чого-небудь. Якщо з'являється спливаюче вікно на екрані, що повідомляє, що у вас є вірус або шпигунське ПЗ і що пропонує завантажити антивірусне або анти-шпигунських програмне забезпечення для його усунення, закрийте спливаюче вікно, натиснувши X у верхньому правому кутку спливаючого вікна. Не реагуйте на спливаючі вікна, що повідомляють про потребу мати новий кодек, драйвера або спеціальну програму для чогось на веб-сторінці. Закрийте спливаюче вікно, натиснувши X у верхньому правому кутку спливаючого вікна. Навчіть своїх співробітників не використати свої USB - накопичувачі в офісі або брати робочі USB-накопичувачі додому і підключити до їх домашніх комп'ютерів. Не зайвим буде і відключити "Autorun" для портів USB на робочих комп'ютерах.

4. Обережніше ведіть онлайн-бізнес або банкінг

Інтернет-бізнес повинен вестися тільки з використанням захищеного з'єднання. Після будь-кого комерційної або банківської онлайн-діяльності, треба видалити кеш, тимчасові файли інтернету, cookies та історію браузеру на випадок злому хакером або шпигунської програми.

5. Вивчайте посадову сумлінність при наймі співробітників.

При наймі співробітників, проведіть комплексну перевірку даних про них. Розгляньте можливість перевірки усіх потенційних співробітників на судимості. Подзвоніть їх колишнім працедавцям. Якщо є освітні вимоги для посади, на яку ви наймаєте співробітників, подзвоните в школу або вищий учбовий заклад, який вони закінчили та перевірте їх дату випуску і середній бал. Також варто зробити перевірку своїх даних. Багато людей дізнаються, що вони є жертвами крадіжки особистих даних тільки після того, як вони роблять перевірку своїх даних і знаходять записи про арешти і адреси, де вони ніколи не жили.

6. Будьте обережні при веб-серфінгу.

Ніхто не повинен переглядати веб-сторінки, використовуючи обліковий запис користувача з правами адміністратора. Якщо ви переглядали веб-сторінки, використовуючи обліковою запис адміністратора, будь-який шкідливий код, на який ви випадково наштовхнетеся в Інтернеті, може самостійно встановитися на ваш комп'ютер. Краще створити гостьовий обліковий запис.

7. Будьте пильні, викачувавши програмне забезпечення з мережі Інтернет.

Не завантажуйте програмне забезпечення з невідомої веб-сторінки. Безпечними можна рахувати тільки ті веб-сторінки, які належать підприємствам, з якими у вас довірчі ділові стосунки. Усі інші веб-сторінки слід розглядати з недовірою. Будьте обережні, використовуючи безкоштовне програмне забезпечення або використовуючи умовно-безкоштовні джерела в інтернеті. Більшості з них не мають технічної підтримки або з урізаною функціональністю.

8. Звертайтеся за допомогою в інформаційній безпеці, коли вам це треба.

Не існує експертів в кожній сфері. Тому, коли вам потрібні спеціалізовані знання в області інформаційної, комп'ютерної або мережної безпеки, звернетеся по допомогу до професіоналів. Досліджуйте діяльності кожної фірми, вимагайте список минулих клієнтів і зв'яжіться з кожним з них для того, щоб дізнатися думку клієнтів про роботу цієї фірми і чи будуть вони надалі користуватися її послугами. Дізнайтеся, про працівників та фахівців, які працюватимуть з вами, запитаєте про професійну кваліфікацію. Дізнайтеся, як довго фірма у бізнесі.

9. Проведіть безпечну утилізацію старих ПК та носіїв.

При утилізації старих комп'ютерів витягніть жорсткі диски і знищіть їх. Це можна зробити розібравши жорсткий диск і ударивши по ньому кілька разів молотком. Не забудьте зруйнувати електроніку в жорсткому диску. Також можна віддати ваші жорсткі диски компаніям, що спеціалізуються на знищенні облаштувань зберігання даних. При утилізації старих носіїв, таких, як компакт-диски, не забудьте видалити усю особисту або ділову інформацію. Утилізація даних, що зберігаються на папері, також вимагає особливої уваги. При утилізації паперу, що містить конфіденційну інформацію, треба знищити її за допомогою машини під назвою shredder. Спалюйте папір, що містить особливо важливу інформацію. Підприємства малого бізнесу, зазвичай, викидають старі комп'ютери не знищуючи жорсткі диски. Важлива ділова інформація часто попадається на комп'ютерах, придбаних на eBay і йому подібних. Це може привести до крадіжки даних.

10. Захистіться від соціальної інженерії.

Соціальна інженерія є спробою особисто або в електронному вигляді отримати неавторизований доступ до інформації, систем або об'єктів шляхом маніпулювання людьми. Соціальний інженер досліджує організацію для того, щоб упізнати імена, посади, обов'язки, а також загальнодоступну інформацію про особу. Потім соціальний інженер говорить, що він секретар, або служба підтримки з правдоподібною але вигаданою історією для того, щоб переконати людину, що він є членом деякої організації і потребує доступу до даних. Працівники повинні знати, як розмовляти з такими людьми. Працівник повинен спочатку ідентифікувати зухвалого абонента, просячи інформацію, яку знатиме тільки справжній службовець організації, яка може запросити такі дані. Якщо людина не в змозі надати таку інформацію, то працівник повинен ввічливо, але твердо, відмовити в наданні інформації. Співробітник повинен повідомити керівництво та СБ про спробу отримати інформацію або доступ до ресурсів системи.

11. Проводьте інвентаризацію активів

Проведіть інвентаризацію усіх ваших апаратних і програмних засобів. Вона повинна включати ідентифікацію усіх ваших важливих даних, які ви використовуєте. Інвентаризація має бути періодичною з регламентом, принаймні 1 раз на рік.

12. Виконуйте шифрування для захисту вашій бізнес інформації.

Шифрування є процесом захисту вашої конфіденційної ділової інформації за допомогою ПЗ шифрування для того, щоб зробити інформацію неможливою до викриття усіх, хто не має ключа шифрування. Варто повністю зашифрувати усі дані, що зберігаються на жорсткому диску. При цьому не забудьте ключ шифрування, запишіть його і сховайте в надійне місце. При шифруванні важливо не забути і про інші обчислювальні і комунікаційні пристрої. Часто для зручності ведення бізнесу використовують смартфони. Якщо на смартфоні є важлива ділова інформація - його необхідно зашифрувати для захисту інформації від крадіжки несанкціонованої заміни або видалення. Більшість виробників смартфонів надають можливість шифрування. Це стосується і планшетів.

1.3.2 Формування фізичної безпеки та безпеки інфраструктури

Розглянемо один із основних методів захисту ПД – формування фізичної безпеки та безпеки інфраструктури. При реалізації такого виду захисту вирішується 2 питання – формування безпечних зон та безпека обладнання. Враховуючи той факт, що інформація все більше стає електронною, гарним прикладом може стати організація захисту приміщення серверної кімнати на підприємстві. Схему організації захисту елементами СККД та план приміщення приведено на рис. 1.22.

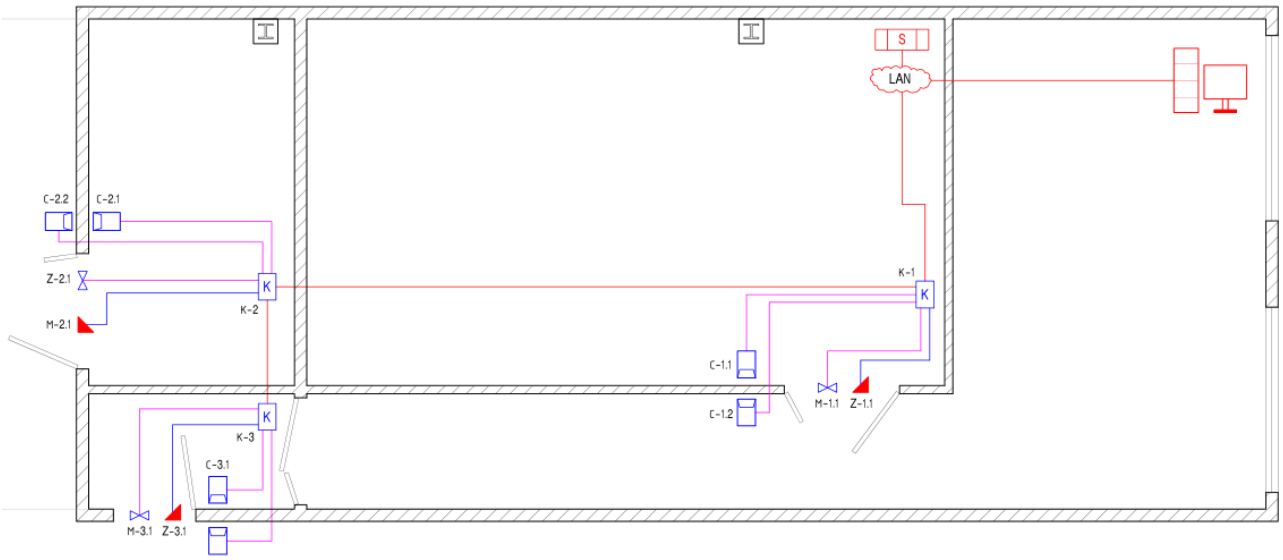


Рисунок 1.22. Формування фізичної безпеки та безпеки інфраструктури елементами СККД

Фізична безпека і безпека інфраструктури включає:

1. Формування безпечних зон
   - Периметр фізичної безпеки
   - Регламентація захисних заходів фізичного доступу
   - Забезпечення захисту офісів, приміщень з комп'ютерним і комунікаційним обладнанням
2. Безпека обладнання
   - З точки зору розташування та захисту обладнання
   - Безпека при передачі даних по кабелю
   - Регулярність технічного обслуговування обладнання

Розробка і впровадження заходів, спрямованих на підвищення фізичної безпеки і безпеки інфраструктури також допомагає вирішувати проблематику.

1.3.3 Використання систем протидії витокам

Data Leak Prevention (DLP) – технології запобігання витоків конфіденційної інформації з інформаційної системи зовні, а також технічні пристрої (програмні або програмно-апаратні) для такого запобігання витоків.

Системи будуються на аналізі потоків даних, що перетинають периметр захищеної інформаційної системи. При детектуванні в цьому потоці конфіденційної інформації спрацьовує активний компонент системи, і передача повідомлення (пакета, потоку, сесії) блокується.

Основними завданнями технічної системи захисту від витоків є:

– отримати опис даних, що захищаються (налагодження системи);

– вміти розпізнавати захищені дані в потоці, вихідному з внутрішнього інформаційного поля компанії зовні (розпізнавання дій, спрямованих на переміщення конфіденційних даних);

– реагувати на виявлені спроби (формування доказової бази для розслідування інцидентів).

Проведемо аналітичне порівняння деяких DLP-систем за обраними критеріями

1. Наявність механізму контентної фільтрації. Наявність механізму контентної фільтрації є обов'язковим для DLP-системи, так як в разі її відсутності, користувач, який має доступ до секретної інформації, зможе передати її за межі мережі компанії, просто «републікуючи її» і відправивши по електронній пошті або іншим способом. У разі наявності системи контентної фільтрації, DLP система може запобігти спробі передачі секретної інформації.

2. Детектування спроб передачі секретної інформації за допомогою стеганографії. DLP-система повинна відстежувати і запобігати спробам передачі інформації, прихованої в медіа-файлах.

3. Детектування спроб передачі зашифрованої інформації. Інсайдер може зашифрувати секретну інформацію, а потім передати її по електронній пошті або іншими способами. DLP-система повинна відстежувати і запобігати цим спроби.

4. Розпізнавання тексту на зображеннях, переданих по електронній пошті і іншим каналам. Інсайдер може зняти скріншоти з секретних документів і передати їх за межі компанії.

5. Підтримка всіх мов світу. Інсайдер може перевести текст секретних документів на мову, який не підтримується DLP-системою, в результаті чого система контентної фільтрації не спрацює.

6. Підтримка всіх форматів документів. Інсайдер може конвертувати секретний документ в формат, який не підтримується DLP-системою, в результаті чого система контентної фільтрації може не спрацювати.

7. Підтримка всіх протоколів передачі даних. Очевидно, що DLP-система повинна відстежувати спроби передачі інформації за всіма технічними каналами, доступним інсайдеру (передача на знімні носії, передача по електронній пошті, передача інформації по протоколам http, https, tcp/ip, ftp, udp, передача по bluetooth і ін .).

Результати перевірки наявності вищеописаних показників у розглянутих DLP-систем наведено в таблиці 1.3.

Таблиця 1.3 - Результати детального огляду DLP-систем, представлених на ринку систем протидії інсайду

Продукт	Держава	Показники						
		1	2	3	4	5	6	7
Authentica ARM Platform	США	-	-	-	-	-	-	-
PortAuthority Technologies	США	+	-	-	-	-	+	+
Verdasys	США	-	-	-	-	-	-	-
Vontu	США	+	-	-	-	-	+	+
McAfee Data Loss Prevention (DLP) Host	США	+	-	-	-	-	+	+
PC Acme	Великобританія	-	-	-	-	-	-	-
Oakley Networks Sure View	США	+	-	-	-	-	-	-
Hackstrike	Ізраїль	+	-	-	-	-	-	-
Tablus	США	+	-	-	-	-	+	-
Proofpoint Messaging Security	США	+	-	-	-	-	+	+

На рисунку 1.24 наведена порівняльна характеристика ймовірностей реалізації загроз безпеці інформаційних ресурсів від ненавмисних дій внутрішніх порушників До та Після впровадження DLP-системи, яка відображає ефективність використання системи протидії витокам конфіденційної інформації на основі DLP.

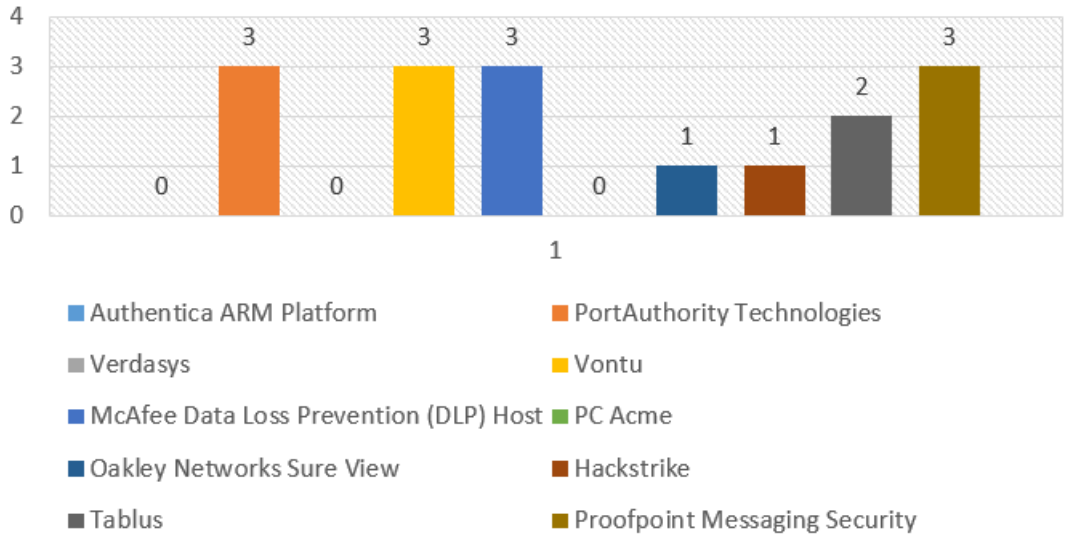


Рисунок 1.23. Аналіз DLP-систем за базовими критеріями

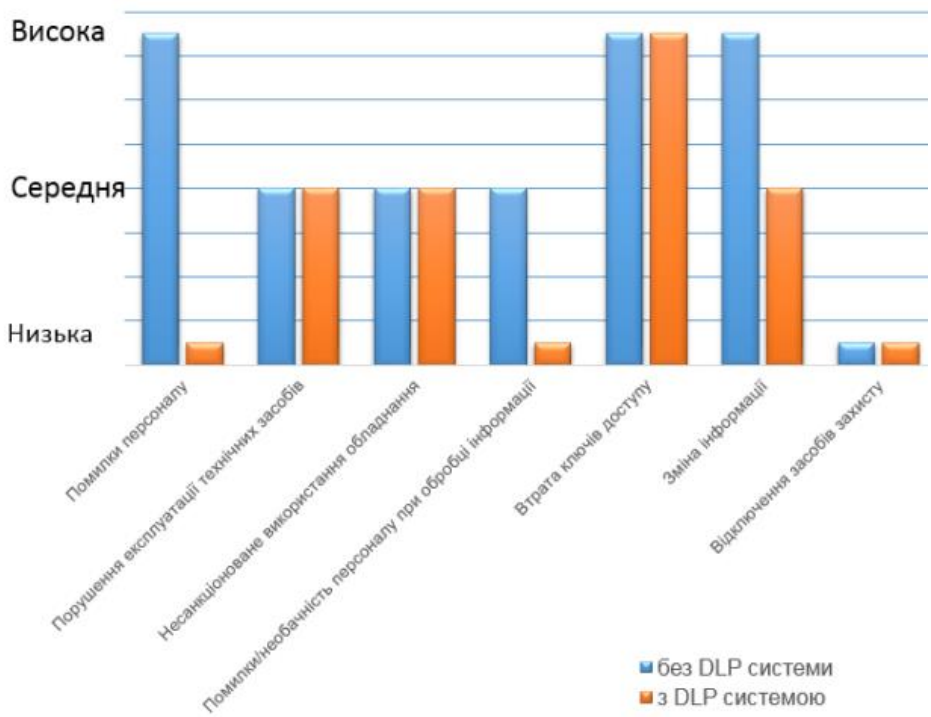


Рисунок 1.24. Порівняльний аналіз ймовірностей реалізації загроз від ненавмисних дій внутрішніх порушників

За результатами порівняльного аналізу, спостерігається значне зниження імовірності реалізації загроз ненавмисних дій персоналу в результаті необережних дій/недбалості, а також помилок при обробці інформації.

1.3.4 Забезпечення принципів безперервності бізнесу

Забезпечення безперервності діяльності - важлива складова функціонування великих підприємств і державних організацій аварійних ситуаціях. Специфіка конкретного бізнесу визначає пріоритети відновлення: те, що відновлювати насамперед, і те, що може зачекати. Елементами управління є дислокація, персонал, обладнання, а також процедури відновлення даних. Завдання BCM - пом'якшити наслідки переривання ділову активність, скоротити час заміни активів, і навіть зменшити витрати. Зруйновані активи (обладнання, приміщення і навіть персонал) практично завжди замінюються.

Період, після якого організація може остаточно втратити життєздатність, називається «максимально допустимим часом простою». Зрозуміло, що наближатися до нього небезпечно, тому керівництво має визначити «цільовий час відновлення», під час якого не буде перевищено також «рівень прийнятних збитків».

У плані забезпечення безперервності діяльності використовують FT та RTO. При цьому фінансові наслідки розраховуються для організації в цілому, а час – з урахуванням найгіршого сценарію розвитку подій та взаємозв'язку процесів. Що важливо, RTO визначається не часом, який потрібно відновити активи, а терміном відновлення ключових аспектів функціонування, для чого навіть можуть залучатися альтернативні технології. Таким чином, завданням БСМ є забезпечення безперервності діяльності організації після катастрофи за певний час. Варто зазначити, що RTO є синтетичним показником, єдиним для кожного бізнесу.

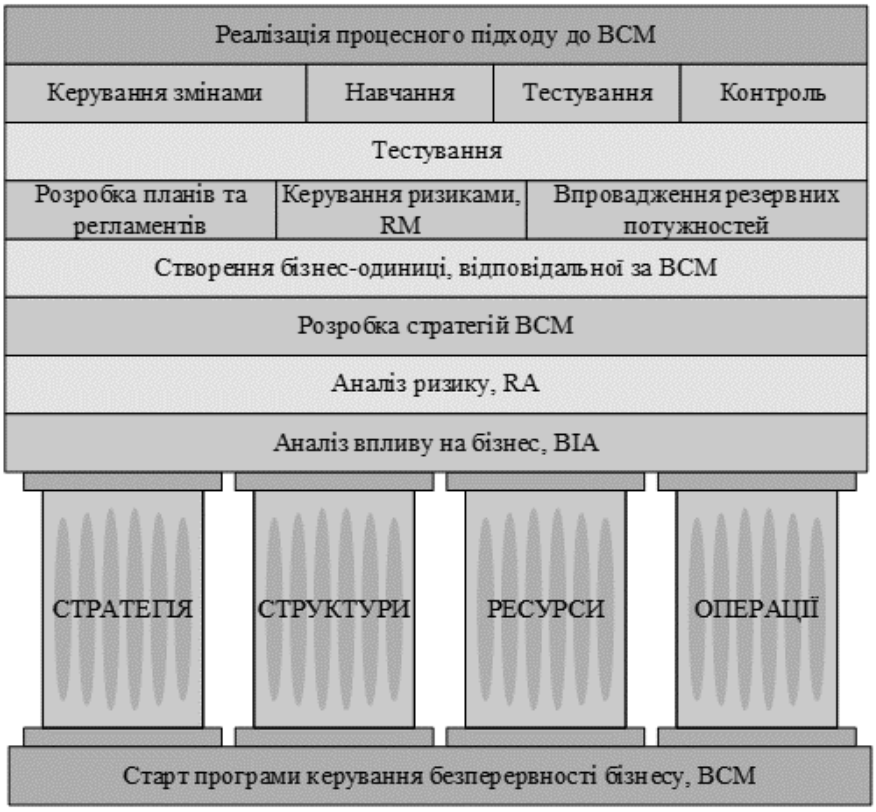


Рисунок 1.25. Стратегія реалізації ефективної програми BCM

Безперервність бізнесу - це здатність організації до відновлення критичних її діяльності процесів протягом нормативу RTO. Значення RTO не слід вибирати «із запасом», оскільки кожну годину зниження цього нормативу може призвести до серйозних витрат.

RTO: Максимальний час, який можна витрачати на відновлення ключових бізнес-процесів. Якщо припускаєте зупинку бізнесу на 4 години, ви встановите RTO о 4 годині.

Аварійне відновлення (Disaster Recovery, DR) – це невелика частина загальної безперервності бізнесу. Єдина мета DR – відновити дані у разі аварії. Максимально допустимий обсяг втрачених при катастрофі даних конкретного блоку функцій визначається цільовим відставанням резервної копії (Recovery Point Objective, RPO).

Ключовими параметрами Аварійного відновлення вважаються RPO: максимальне відставання резервної копії кожного блоку функцій. Значення RPO

можуть бути різними. Якщо ви можете дозволити собі втратити дані конкретного сервісу за день, ви встановите його RPO о 24 годині.

1.3.5 Підвищення рівня відмовостійкості на основі технології RAID

Одним з варіантів підвищення рівня відмовостійкості є використання технології RAID - надлишковий масив незалежних дисків) - масив з декількох дисків (запам'ятовуючих пристроїв), керованих контролером, пов'язаних між собою швидкісними каналами передачі даних і сприймаються зовнішньою системою як єдине ціле. Залежно від типу використовуваного масиву може забезпечувати різні ступені відмовостійкості і швидкодії.

Таблиця 1.4 – Рівні забезпечення відмовостійкості

Методи	Вартість (надмірність дисків, шт.)	Надійність (Кількість припустимих падінь), n - кількість дзеркал
RAID1	2n	n-1
RAID5	n+1	1
RAID6	n+2	2
RAID10	2n	n-1
RAID50	n+1	1

Таблиця 1.5 – Забезпечення стійкості при використанні різних методів

Методи	Простота розгортання	Простота використання	Консолідація ресурсів	Можливість масштабування	Вартість	Розподілена СЗД	Швидкість передач даних	Надійність
SAN	-	+	+	+	Висока	+	+	Висока
NAS	+	+	+	+	Низька	+	-	Середня
DAS/ SAS	+	-	-	-	Низька	-	+	Низька

2. ЕКОНОМІЧНА ЧАСТИНА

Метою даних розрахунків є обчислення вартості виконання науково-дослідної роботи «Модернізація IT-середовища сучасного підприємства на основі міжнародних стандартів з кібербезпеки». У роботі розглянуто класифікацію, склад та загрози інформаційного середовища компанії. Проведено аналіз міжнародних стандартів, політик та рекомендацій у сфері кібербезпеки. Розглянуто стандарти ISO 27001, ISO 27032, PCI DSS, HB 292:2006, серія T260, міжвідомчий звіт NIST(NISTIR) 7621, політики відповідності HIPAA, регламент захисту персональних даних GDPR. У рамках модернізації інформаційної інфраструктури компанії в аспекті кібербезпеки, викладених у низці стандартів, політик та рекомендацій, застосовані методи та засоби захисту, а саме – впроваджено алгоритми захисту з позиції NIST 7621, застосовано елементи фізичної безпеки та системи протидії витокам, технологію RAID та принципи безперервності бізнесу.

Даний вид проекту відноситься до науково-дослідницької розробки. Оцінка якості розробленого проекту включає визначення трудомісткості і вартості його створення.

Перелік етапів і робіт, що виконуються при проведенні НДР, приведений в таблиці 2.1.

Таблиця 2.1.- Розподіл робіт по етапах і видах виконавців.

Етап проведення НДР	**Вигляд робіт**	**Посада виконавця**
Розробка технічного завдання (ТЗ)	1.Складання і затвердження ТЗ для НДР «Модернізація IT-середовища сучасного підприємства на основі міжнародних стандартів з кібербезпеки».	Дипломник, керівник
Вибір напряму дослідження	1. Збір і вивчення науково-технічної літератури.	Дипломник

	2. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка. 3. Розробка плану проведення досліджень для подальшої розробки.	керівник
Теоретичні і експериментальні дослідження	1. Класифікація, склад та загрози інформаційного середовища сучасного підприємства 2. Аналіз міжнародних стандартів та рекомендацій з напрямку кібербпезпеки 3. Ключові методи та засоби підвищення рівня захисту інформаційної інфраструктури на основі стандартів з кібербезпеки	Дипломник керівник консультанти
Узагальнення і оцінка результатів досліджень	1. Узагальнення результатів 2. Оцінка повноти вирішення поставлених завдань. 3.Складання і оформлення звіту. Розгляд результатів проведеною НДР і прийняття результатів в цілому.	Дипломник керівник консультанти

Оцінка тривалості виконання робіт розраховується на основі вірогідних оцінок робіт, що задаються виконавцями.

Таблиця 2.2 - Очікувана трудомісткість робіт.

Вигляд роботи	Очікуваний час виконання (дні)
1. Складання і затвердження ТЗ для НДР «Модернізація ІТ-середовища сучасного підприємства на основі міжнародних	1

стандартів з кібербезпеки».	
2. Збір і вивчення науково – технічної літератури, технічної документації і інших матеріалів.	2
3. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка.	2
4. Класифікація, склад та загрози інформаційного середовища сучасного підприємства	4
5. Аналіз міжнародних стандартів та рекомендацій з напрямку кібербпезпеки	6
6. Ключові методи та засоби підвищення рівня захисту інформаційної інфраструктури на основі стандартів з кібербезпеки.	6
7.Узагальнення результатів. Оцінка повноти вирішення поставлених завдань	3
Всього:	24

Розрахунок собівартості і ціни виконання НДР. Виходячи з особливостей створення науково – технічної продукції і її залежності від інтелектуальної праці, розрахунок собівартості і ціни виконання НДР включає наступні статті витрат: витрати на матеріали, основна і додаткова заробітна плата, відрахування до єдиного соціального фонду страхування, витрати на роботи, що виконуються сторонніми організаціями, і деякі інші.

1) Витрати на матеріали складають 300 грн.

2) До витрат «Основна заробітна плата» відносяться оплата праці виконавців, безпосередньо притягнених до її виконання. Розмір основної зарплати встановлюється виходячи з чисельності різних категорій виконавців, трудомісткості, що витрачається ними на виконання різних видів робіт, а також їх середньої заробітної плати (ставки) за один робочий день. Відповідно до статті 8 «Закону про Державний бюджет України на 2023» встановлено мінімальну

заробітну плату у місячному розмірі з 1 січня 2023 року - 6700 гривень; мінімальну погодинну тарифну ставку – 40,43 грн.

Середня зарплата за один робочий день для кожного виконавця визначена по формулі:

Зден= п.т.с. * 8;

де п.т.с – погодинна тарифна ставка, грн..;

8 – тривалість робочого дня, год.

Зден дипломника = 41*8 = 328 грн.

Зден керівника = 70 *8 = 560 грн

Зден консультантів = 60*8 =480 грн.

Витрати на основну заробітну плату, НДР, що включаються в собівартість, приведені в таблиці 2.3.

Таблиця 2.3. - Витрати на основну заробітну плату.

Виконавець	**Погодинна тарифна ставка, грн**	**Денна ставка, грн**	**Трудомісткість робочих днів**	**Сума основної зарплати, грн**
Дипломник	41,00	328,00	24	7872,00
Керівник	70,00	560,00	1	560,00
Консультант по економіки	60,00	480,00	0,25	120,00
Консультант по охороні праці	60,00	480,00	0,25	120,00
Нормоконтроль	60,00	480,00	0,25	120,00
Всього (Зо)				8792,00

3) Витрати на додаткову заробітну плату визначаються у відсотках від основної. У наукових закладах додаткова заробітна плата складає 10-12% від основної заробітної плати.

Зд=10% *Зо =8792,00 * 0.1 = 879,20грн

4)До складу собівартості НДР включаються податки, збори і інші обов'язкові платежі, встановлені системою оподаткування що діє. Відрахування до єдиного соціального внеску складає:

Зєсв=0,22*(Зо+Зд) = 0,22 *(8792,00 +879,20) = 2127,62 грн

5) До накладних витрат відносять витрати на управління і господарське обслуговування, що відноситься до всіх виконуваних НДР. У наукових закладах накладні витрати складають 40 -120% від основної і додаткової заробітної плати.

Рнакл= (Зо+Зд)*0,4 = (8792,00 +879,20)*0,4 = 3868,42 грн

На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості в цілому НДР за формою, приведеною в таблиці 2.4.

Таблиця 2.4. - Калькуляція планової собівартості

Статті витрат	Сума, грн.
1. Матеріали	300,00
2. Основна заробітна плата	8792,00
3. Додаткова заробітна плата	879,20
4. Відрахування до єдиного соціального внеску	2127,62
5. Накладні витрати	3868,42
Планова собівартість (Спл)	15967,22

Плановий прибуток визначений по формулі:

Ппл = 0,1*Спл = 0,1 * 15967,22= 1596,72грн

Де 0,1 – норматив, який враховує граничний рівень рентабельності, встановлений чинним законодавством для науково-дослідницької роботи.

Договірна ціна визначається по формулі

Цндр = Спл + Ппл = 15967,22+1596,72= 17563, 94грн.

Ціну реалізації встановлюємо з урахуванням ПДВ

Цр = Цндр + ПДВ = 17563, 94+17563, 94* 0,2=21076,73грн.

3 ОХОРОНА ПРАЦІ

Україна приділяє велику увагу питанням охорони життя і здоров'я своїх громадян, створенню безпечних умов праці роботодавцями, керівниками установ, організацій, проте кількість нещасних випадків, що трапляються на виробництві, залишається дуже великою.

Поліпшення умов та охорона праці стає одним з важливих напрямків матеріального та культурного рівня життя народу, а це, у свою чергу, сприяє зростанню якості та продуктивності праці, підвищенню соціально-економічних показників виробництва, зменшенню коштів на витрати від травматизму, професійних захворювань і аварій. Дипломним проектом передбачена модернізація інформаційного середовища компанії на основі міжнародних стандартів з кібербезпеки, тому в даному розділі розглянемо питання створення безпечних умов праці для користувача ПК.

3.1 Аналіз небезпечних і шкідливих факторів

В процесі роботи на користувачів ПК можуть мати вплив наступні небезпечні та шкідливі фактори:

- невідповідність параметрів мікроклімату нормам;
- недостатній рівень освітленості;
- ураження електрострумом;
- статична електрика;

3.2 Гігієнічні вимоги до виробничого середовища

Потрібно враховувати санітарні нормативи освітлення, вимоги до параметрів мікроклімату (температура, відносна вологість), ступеня і сили вібрації, звукового шуму і вогнестійкості приміщення, а також характеристики електромагнітного, ультрафіолетового та інфрачервоного полів. Конкретні показники зазначених санітарних норм викладені в Державних санітарних правилах і нормах роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98.

Заборонено установлювати комп'ютери в приміщеннях, розташованих у підвалах будинків. Для уникнення можливих аварій та замикань, поряд з приміщеннями, де вестиметься робота з комп'ютером (над чи під ними), також не дозволяється проведення робіт, що потребують здійснення надмірно вологих технологічних процесів. Відповідне приміщення повинно бути укомплектоване системами центрального або індивідуального опалення, кондиціонування чи вентиляції повітря.

У кожній кімнаті, де обладнуватимуться робочі місця співробітників, що працюватимуть на комп'ютері, повинні бути наявні елементи природного та штучного освітлення. При цьому, на вікнах слід встановити легко регульовані жалюзі чи штори, які дозволять працівникам коригувати рівень освітлення в приміщенні. Бажано розмістити комп'ютери в кімнаті таким чином, щоб світло потрапляло на екрани моніторів з півдня чи північного сходу.

У разі надмірного шуму чи вібрації технічного обладнання, роботодавець повинен забезпечити працівників антивібраційними килимками.

Виробничі приміщення необхідно обладнати аптечками першої медичної допомоги.

3.3 Вимоги до організації робочого місця працівника

Роботодавець, який використовує найману працю робітників, повинен забезпечити відповідність їхніх робочих місць комфортним та безпечним умовам. Розмір одного робочого місця має становити не менше 6 квадратних метрів. При необхідності, суміжні робочі місця співробітників, що працюють з комп'ютером, слід розділити перегородками висотою до 2 метрів. При визначенні достатнього розміру приміщення і робочого місця на одну особу необхідно додатково враховувати шафи, сейфи, тумби або інші предмети меблів чи обладнання, які знаходяться в кімнаті. На столі працівника можливо розмістити допоміжні для роботи пристрої (принтери, колонки, сканери), а також місця для зберігання документів, за умови, що це не обмежуватиме видимість екрану і не заважатиме працівнику. Робочий стілець співробітника має бути підйомно-поворотним, легко регульованим за висотою та забезпечувати

належну підтримку та зручне положення спини і хребта особи. Щодня необхідно проводити вологе прибирання приміщення, та очищати робоче місце та безпосередньо монітор комп'ютера від запиленості.

На підприємстві забороняється: проводити ремонт та технічне обслуговування комп'ютера за робочим місцем працівника; самочинно ремонтувати або намагатись здійснити технічне налагодження комп'ютера без залучення компетентних спеціалістів; складувати на робочому місці зайві документи, деталі та предмети, що не потрібні для роботи; використовувати монітори з нечітким зображенням та монітори, у яких наявні поламки екрану; працювати з матричним принтером без антивібраційного покриття та зі знятою кришкою.

Допускати до роботи осіб, які не пройшли затверджений на підприємстві курс охорони праці для роботи з комп'ютером, не дозволяється.

Рисунок 3.1. Організація безпечного робочого місця

3.4 Електробезпека

Вимоги електробезпеки у приміщеннях, де встановлені електронно-обчислювальні машини і персональні комп'ютери (далі — ЕОМ) відображені у *ДНАОП 0.00-1.31-99*. Відповідно до цього нормативного документу під час проектування систем електропостачання, монтажу основного електрообладнання та електричного освітлення будівель та приміщень для ЕОМ необхідно дотримуватись вимог Правил влаштування електроустановок *(ПВЕ), ГОСТ*

12.1.006-84, ГОСТ 12.1.019-79, ГОСТ 12.1.030-81, ГОСТ 12.1.045-84, ПТЕ, ПБЕ, ВСН 59-88 "Электрооборудованиежилых и общественных зданий. Нормы проектирования", СН 357-77 "Инструкция по проектированию силового осветительного оборудования промишленных предприятий", Правил пожежної безпеки в Україні та інших нормативних документів, що стосуються штучного освітлення і електротехнічних пристроїв, а також вимог нормативно-технічної експлуатаційної документації заводу-виробника.

Лінія електромережі для живлення ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ виконується як окрема групова трипровідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів і прокладається від стійки групового розподільчого щита, розподільчого пункту до розеток живлення

У приміщенні, де одночасно експлуатується або обслуговується більше п'яти персональних ЕОМ, на помітному та доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення.

Металеві труби та гнучкі металеві рукави повинні бути заземлені. Заземлення повинно відповідати вимогам ДНАОП 0.00-1.21-98 "Правила безпечної експлуатації електроустановок споживачів". Заземлені конструкції, що знаходяться у приміщеннях (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном тощо), мають бути надійно захищені діелектричними щитками або сітками від випадкового дотику.

Є неприпустимими:

— експлуатація кабелів та проводів з пошкодженою або такою, що втратила захисні властивості за час експлуатації, ізоляцією; залишення під напругою кабелів та проводів з неізольованими провідниками;

— застосування саморобних продовжувачів, які не відповідають вимогам ПВЕ до переносних електропроводок;

— застосування для опалення приміщення нестандартного (саморобного) електронагрівального обладнання або ламп розжарювання;

— користування пошкодженими розетками, розгалужувальними та з'єднувальними коробками, вимикачами та іншими електровиробами, а також лампами, скло яких має сліди затемнення або випинання;

3.5 Пожежна безпека

Джерелами займання можуть бути електричні іскри, дуги, коротке замикання, струмові перевантаження, перегріті опірні поверхні, несправність обладнання. Окислювачем звичайно служить кисень. Але потужність і тривалість дії цих джерел займання порівняно малі, тому горіння, як правило, не розвивається. Виникнення пожежі в електронних пристроях можливо, якщо використовуються спалимі і важкоспалимі матеріали і вироби.

Забезпечення пожежної безпеки на підприємствах здійснюється наступними основними компонентами виробництва:

- технічною системою, яка передбачає надійність обладнання, використання безпечних технологій, визначає обсяг вибухопожежонебезпечних речовин, проектні рішення, впровадження систем виявлення та гасіння пожеж тощо;
- персоналом, його підготовкою, забезпеченням регламентами і правилами роботи;
- системою управління.

До засобів гасіння пожежі відносяться внутрішні пожежні водопроводи (крани - ПК), вогнегасники (вуглекислотні та порошкові), сухий пісок тощо.

Для гасіння пожеж на початкових стадіях широко застосовуються вогнегасники. У виробничих приміщеннях це головним чином вуглекислотні вогнегасники, достоїнством яких є висока ефективність гасіння пожежі, збереження електричного устаткування. Розташовують вогнегасники на видних місцях, на висоті не більше як 1,5 м від полу.

ВИСНОВКИ

Сьогодні інформаційна інфраструктура з її мережами, серверами, робочими станціями, роутерами та рештою компонентів стала основою роботи компанії, незалежно від виду діяльності. Але в той же час, крім переваг, є і зворотний бік у вигляді загроз і ризиків кіберсередовища. Знання міжнародних стандартів та застосування принципів, викладених у них, дає можливість під фокусом безпеки будувати та модернізувати IT-середовище. У роботі розглянуто класифікацію, склад та загрози інформаційного середовища компанії. Проведено аналіз міжнародних стандартів, політик та рекомендацій у сфері кібербезпеки. Розглянуто стандарти ISO 27001, ISO 27032, PCI DSS, HB 292:2006, серія T260, міжвідомчий звіт NIST(NISTIR) 7621, політики відповідності HIPAA, регламент захисту персональних даних GDPR.

У рамках модернізації інформаційної інфраструктури компанії в аспекті кібербезпеки, викладених у низці стандартів, політик та рекомендацій, застосовані методи та засоби захисту, а саме – впроваджено алгоритми захисту з позиції NIST 7621, застосовано елементи фізичної безпеки та системи протидії витокам, технологію RAID та принципи безперервності бізнесу.

Застосовані методи та засоби протидії загрозам в кіберсередовищі, які обрані на основі міжнародних стандартів, суттєво підвищують рівень захисту інформаційної інфраструктури та можуть бути застосовані в компаніях різного масштабу та виду господарської діяльності.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання, Довгий С.О., Воробієнко П.П., Гуляєв К.Д., за загальною редакцією члена-кореспондента НАН України Довгого С.О., Київ “АзимутУкраїна”, 607 стор., 2013 р.

2 Стайкуца С.В., Аверьянов В.А. Анализ IT-инфраструктуры современного предприятия с позиции "жизненного" цикла // 71-ша науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів.. - Одесса: ОНАС им. А.С. Попова, 2016.

3 Стайкуца С. В. Работа с персональными данными в аспекте введения GDPR / С. В. Стайкуца, Т.Н. Лемеха, К.Р. Баньковский. // Інноваційний розвиток науки нового тисячоліття. – 2018. – С. 97-101.

4 Морозов Д. ИТ-инфраструктура современных компаний: общие тенденции / Дмитрий Морозов. // Intelligent Enterprise/Корпоративные системы. – 2013.

5 Баньковский К.Р. Требования к защите персональных данных клиентов в аспекте GDPR как основа кадровых изменений на рынке безопасности / К.Р. Баньковский, Т.Н. Лемеха, М.А. Лайтан, И.В. Шевченко // Матеріали четвертої всеукраїнської науково-практичної конференції “ Перспективні напрями захисту інформації ”, ОНАЗ ім. О.С.Попова. – 2018

6 Меры по ИБ для малого бизнеса (по NIST) . – 2014 [електроний ресурс]. Режим доступу:: http://80na20.blogspot.ru/ 2014/12/nist.html

7 GDPR Compliance [Електронний ресурс] // HubSpot. – 2018. – Режим доступу до ресурсу: https://www.hubspot.com/data-privacy/gdpr.

8 Петренко С.А. Лучшая практика создания корпоративных программ BCM // Защита Информации. Inside. – 2009. – № 2. – С. 12–29.

9 Rastogi A. Complying with ISO27001 while on AWS [Електронний ресурс] / Aseem Rastogi. – 2018. – Режим доступу до ресурсу:

https://www.linkedin.com/pulse/complying-iso27001-while-aws-aseem-rastogi/?articleId=6465513359474294784.

10 ISO/IEC 27001:2022 [Електронний ресурс] // SecAware – Режим доступу до ресурсу: https://www.iso27001security.com/html/27001.html.

11 Что такое соответствие HIPAA? Контрольный список и руководство по соблюдению требований HIPAA [Електронний ресурс] // Блог Atlantic.Net. – 2020. – Режим доступу до ресурсу: https://www.atlantic.net/hipaa-compliant-hosting/hipaa-compliance-guide-what-is-hipaa/.

12 HIPAA: як захищають медичні дані пацієнтів в США? [Електронний ресурс] // EverLegal. – 2020. – Режим доступу до ресурсу: https://everlegal.ua/hipaa-yak-zakhyschayut-medychni-dani-patsientiv-v-ssha.

13 Краудсорсинговое тестирование на проникновение и соответствие PCI DSS [Електронний ресурс] // Cobalt. – 2021. – Режим доступу до ресурсу: https://www.cobalt.io/blog/crowdsourced-penetration-testing-and-pci-dss-compliance.

14 Предотвращение утечек данных [Електронний ресурс] – Режим доступу до ресурсу: http://www.sovit.net/articles/technologies/data_loss_prevention/

15 Системы DLP - Who? What? Where? How? [Електронний ресурс] – Режим доступу до ресурсу: http://www.topsbi.ru/default.asp?artID=1675.

ДОДАТОК А. Слайди мультимедійної презентації

МОДЕРНІЗАЦІЯ ІТ-СЕРЕДОВИЩА СУЧАСНОГО ПІДПРИЄМСТВА НА ОСНОВІ МІЖНАРОДНИХ СТАНДАРТІВ З КІБЕРБЕЗПЕКИ

ДИПЛОМНИЙ ПРОЕКТ

Керівник: Стайкуца С.В.

Виконав: Арнаутов Д.Р.

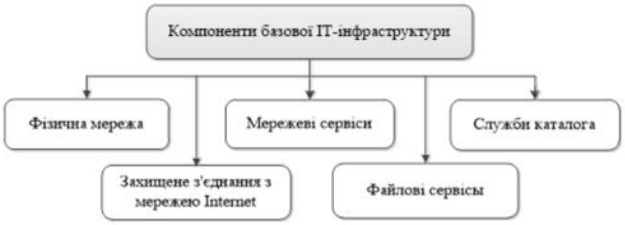
2023

МОДЕЛЬ ПІДПРИЄМСТВА НА ОСНОВІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ.

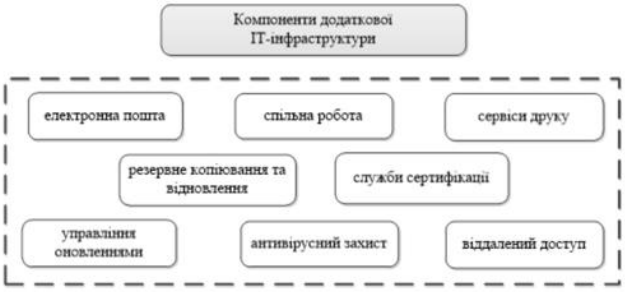
ІТ-ІНФРАСТРУКТУРА

ІТ-ІНФРАСТРУКТУРА - ЦЕ КОМПЛЕКСНА СТРУКТУРА, ЯКА ОБ'ЄДНУЄ ВСІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА РЕСУРСИ, ЩО ВИКОРИСТОВУЮТЬСЯ КОНКРЕТНОЮ ОРГАНІЗАЦІЄЮ АБО КОМПАНІЄЮ

ОСНОВНІ ТА ДОДАТКОВІ КОМПОНЕНТИ IT-ІНФРАСТРУКТУРИ.



Компоненти базової IT-інфраструктури



Компоненти додаткової IT-інфраструктури

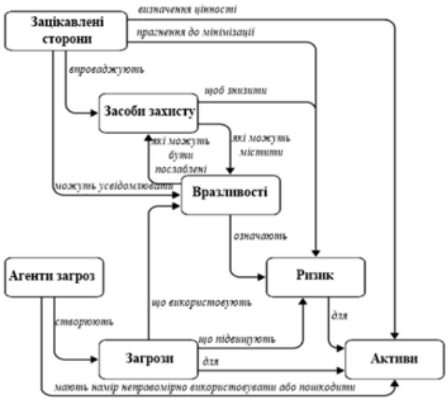
Класифікація IT-систем за рівнем безперервності

АНАЛІЗ МІЖНАРОДНИХ СТАНДАРТІВ ТА РЕКОМЕНТАЦІЙ З НАПРЯМКУ КІБЕРБЕЗПЕКИ.

АНАЛІЗ МІЖНАРОДНИХ СТАНДАРТІВ ТА РЕКОМЕНТАЦІЙ З НАПРЯМКУ КІБЕРБЕЗПЕКИ. ISO 27032.

ISO/IEC 27032:2012

Information technology -- Security techniques -- Guidelines for cybersecurity



Основні поняття безпеки і характер зв'язків між ними

АНАЛІЗ МІЖНАРОДНИХ СТАНДАРТІВ ТА РЕКОМЕНТАЦІЙ З НАПРЯМКУ КІБЕРБЕЗПЕКИ. ISO 27032.

Безпека додатків

Безпека серверів

Безпека кінцевих користувачів

Захист від соціальної інженерії

Підвищення готовності

АНАЛІЗ МІЖНАРОДНИХ СТАНДАРТІВ ТА РЕКОМЕНТАЦІЙ З НАПРЯМКУ КІБЕРБЕЗПЕКИ. РЕГЛАМЕНТ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ GDPR.

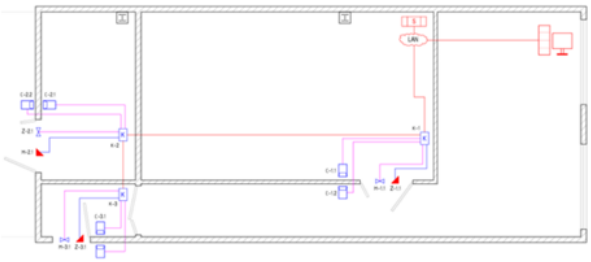
Ключові статті GDPR

Етапи успішного впровадження GDPR

МЕТОДИ ТА ЗАСОБИ ПІДПИЩЕННЯ РІВНЯ ЗАХИСТУ IT-ІНФРАСТРУКТУРИ НА ОСНОВІ СТАНДАРТІВ З КІБЕРБЕЗПЕКИ. ФОРМУВАННЯ ЗАХИСТУ ЗГІДНО NIST 7621.

Основні та додаткові етапи формування захисту згідно NIST 7621

МЕТОДИ ТА ЗАСОБИ ПІДПИЩЕННЯ РІВНЯ ЗАХИСТУ IT-ІНФРАСТРУКТУРИ НА ОСНОВІ СТАНДАРТІВ З КІБЕРБЕЗПЕКИ. ФІЗИЧНИЙ ЗАХИСТ ТА ПРИНЦИПИ НЕПЕРЕРВНОСТІ

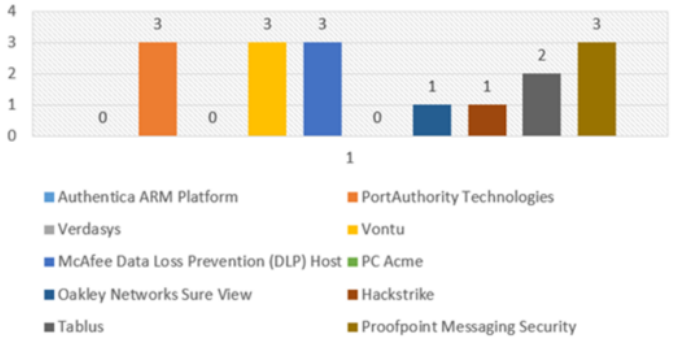


Формування фізичної безпеки та безпеки інфраструктури елементами СККД

Стратегія реалізації ефективної програми BCM

МЕТОДИ ТА ЗАСОБИ ПІДПИЩЕННЯ РІВНЯ ЗАХИСТУ IT-ІНФРАСТРУКТУРИ НА ОСНОВІ СТАНДАРТІВ З КІБЕРБЕЗПЕКИ. ЗАСТОСУВАННЯ СИСТЕМ ПРОТИДІЇ ВИТОКАМ (DLP)

Продукт	Держава	Показники						
		1	2	3	4	5	6	7
Authentica ARM Platform	США	-	-	-	-	-	-	-
PortAuthority Technologies	США	+	-	-	-	-	+	+
Verdasys	США	-	-	-	-	-	-	-
Vontu	США	+	-	-	-	-	+	+
McAfee Data Loss Prevention (DLP) Host	США	+	-	-	-	-	+	+
PC Acme	Великобританія	-	-	-	-	-	-	-
Oakley Networks Sure View	США	+	-	-	-	-	-	-
Hackstrike	Ізраїль	+	-	-	-	-	-	-
Tablus	США	+	-	-	-	-	+	-
Proofpoint Messaging Security	США	+	-	-	-	-	+	+

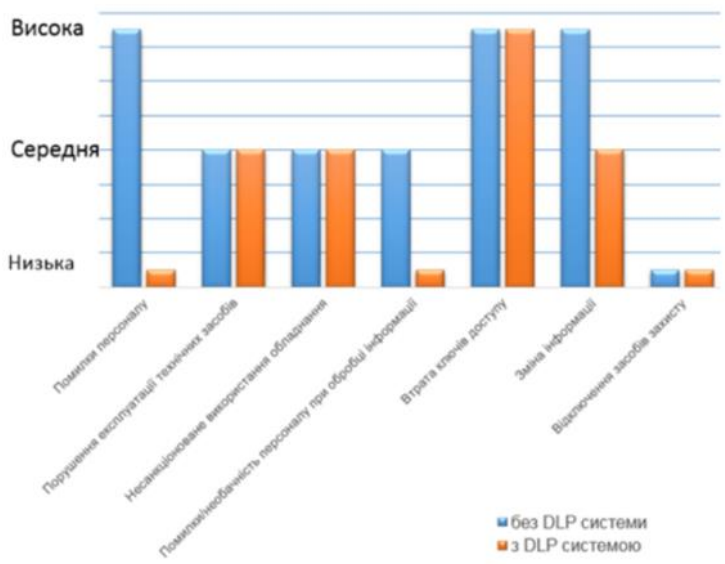


DATA LEAK PREVENTION (DLP)

ТЕХНОЛОГІЇ ЗАПОБІГАННЯ ВИТОКІВ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ З ІНФОРМАЦІЙНОЇ СИСТЕМИ ЗОВНІ, А ТАКОЖ ТЕХНІЧНІ ПРИСТРОЇ (ПРОГРАМНІ АБО ПРОГРАМНО-АПАРАТНІ) ДЛЯ ТАКОГО ЗАПОБІГАННЯ ВИТОКІВ

Критерії для порівняння DLP-систем

1. Наявність механізму контентної фільтрації.
2. Детектування спроб передачі секретної інформації за допомогою стеганографії.
3. Детектування спроб передачі зашифрованої інформації.
4. Розпізнавання тексту на зображеннях, переданих по електронній пошті і іншим каналам.
5. Підтримка всіх мов світу.
6. Підтримка всіх форматів документів.
7. Підтримка всіх протоколів передачі даних.



ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

В дипломному проекті запропоновано обрати методи та засоби модернізації ІТ- інфраструктури підприємства на основі міжнародних стандартів з кібербезпеки. Результати роботи такі:

1) Класифікація та склад ІТ-інфраструктури дозволяє зрозуміти вихідні дані на підприємстві
2) В рамках аналізу міжнародних стандартів та рекомендацій з напрямку кібербезпеки розглянуто документи ISO 27001, ISO 27032, НВ 292:2006, політику відповідності HIPAA, міжвідомчий звіт NIST(NISTIR) 7621, регламент захисту персональних даних (GDPR)
3) В рамках модернізації ІТ- інфраструктури підприємства застосовано елементи фізичної безпеки, технологію RAID, принципи неперервності бізнесу BCM, системи протидії витокам (DLP), впроваджено основні та додаткові етапи формування захисту згідно NIST 7621
4) При застосуванні DLP-систем вирішується проблематика помилок персоналу та зміни інформації в системі
5) Проведений аналіз стандартів дозволяє на основі рекомендацій проводити подальшу модернізацію інформаційної інфраструктури та формувати захищене середовище

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на дипломний проект (роботу) здобувача (здобувачки) освіти

відділення комп'ютерних систем

Арнаутова Дмитра Руслановича

(прізвище, ім`я та по батькові)

Спеціальність 123 "Комп'ютерна інженерія"

Освітня програма «Обслуговування комп'ютерних систем і мереж»

Керівник дипломного проекту (роботи) Стайкуца Сергій Володимирович

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи) Модернізація IT-середовища сучасного підприємства на основі міжнародних стандартів з кібербезпеки

Обсяг розрахунково-пояснювальної записки 79 сторінок

Обсяг графічної (презентаційної) частини 13 аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту (роботи) завданню

Представлений на рецензію дипломний проект повністю відповідає меті проектування та технічному завданню. Тематика дипломного проекту є актуальною та присвячена вибору оптимальних методів та засобів кібербезпеки на основі міжнародних стандартів

б) характеристика виконання кожного розділу дипломного проекту (роботи)

Дипломний проект складається зі вступу, трьох розділів, висновків, переліку використаних джерел. У технологічному розділі виконано огляд і аналіз міжнародних стандартів та рекомендацій з напрямку кібербезпеки та впроваджено певні методи та засоби підвищення рівня захисту IT-інфраструктури: організаційні на основі NIST 7621, технічні засоби охорони, системи протидії витокам, принципів безперервності бізнесу тощо.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту (роботи) Графічна частина виконана на достатньо високому рівні у вигляді презентації із використанням офісного пакету Microsoft PowerPoint та Visio. Пояснювальна записка виконана акуратно та у відповідності до норм оформлення документів із використанням офісного пакету Microsoft Word. Загальна якість виконання документації – добра, академічного плагіату у роботі не виявлено

г) перелік позитивних якостей дипломного проекту (роботи)

1. Детально розглянуто існуючі міжнародні стандарти з кібербезпеки
2. Виконання рекомендацій для захисту на основі міжвідомчого звіту NIST(NISTIR) 7621 дозволить більш ніж на 90% знизити ризики кібербезпеки
3. Актуальним є використання принципів BCM

д) основні недоліки дипломного проекту (роботи)

1. Розглянуто не всі стандарти кібербезпеки, наприклад, відсутня серія Т260
2. При розгляді напряму організації фізичного захисту треба було навести повний компонентний склад

Оцінка розрахункової частини відмінно

Оцінка графічної частини відмінно

Загальна оцінка відмінно

Прізвище, ім'я, по батькові рецензента Кривченко Юрій Вікторович

Місце роботи і посада рецензента

ВСП "Одеський технічний фаховий коледж ОНТУ", голова циклової комісії комп'ютерних технологій та програмної інженерії

Підпис:

« 16 » червня 2023 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Арнаутова Дмитра Руслановича

(прізвище, ім'я та по батькові)

Спеціальність: *123 "Комп'ютерна інженерія"*

Освітня програма: *«Обслуговування комп'ютерних систем і мереж»*

Тема дипломного проекту: *Модернізація IT-середовища сучасного підприємства на основі міжнародних стандартів з кібербезпеки*

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки) *Дипломний проект виконано відповідно технічному завданню. Пояснювальна записка містить 79 сторінок. У пояснювальній записці наведено етапи створення захищеного інформаційного середовища на основі міжнародних стандартів та рекомендацій. Графічна частина складається з слайдів мультимедійної презентації, які також містять креслення, передбачені технічним завданням. Якість виконання пояснювальної записки та графічної частини добра, розробку виконано в повному обсязі.*

б) самостійність роботи над проектом: *Протягом всього строку дипломного проектування та переддипломної практики здобувач освіти Арнаутов Д.Р. поступово та послідовно виконував всі етапи розробки. Всі роботи студент виконував самостійно, з оглядом на рекомендації керівника*

в) теоретична підготовка випускника (випускниці): *Здобувач освіти Арнаутов Д.Р. під час роботи над дипломним проектом вивчив достатню кількість літературних джерел та матеріалів за даною тематикою.*

Вважаю, що теоретична підготовка дипломника добра і він готовий до захисту дипломного проекту

UNICHECK

Ім'я користувача:
Наталія Вікторівна Копусь

ID перевірки:
1015421316

Дата перевірки:
05.06.2023 08:53:51 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
05.06.2023 08:57:58 EEST

ID користувача:
100011688

Назва документа: 4ФКС-56 Арнаутов Дмитро

Кількість сторінок: 79 Кількість слів: 11954 Кількість символів: 93961 Розмір файлу: 2.34 MB ID файлу: 1015083812

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

16.9%
Схожість

Найбільша схожість: 4.11% з Інтернет-джерелом (http://elartu.tntu.edu.ua/bitstream/lib/38307/1/bak_2022_SN-41_Orlin...

16.9% Джерела з Інтернету | 385 ..... Сторінка 81

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 2

Підозріле форматування | 12 сторінок

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Арнаутов Дмитро Русланович
здобувач освіти гр. ФКС-56, та

Стайкуца Сергій Володимирович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи фахового молодшого бакалавра на тему:

«Модернізація IT-середовища сучасного підприємства на основі міжнародних стандартів з кібербезпеки» (автор роботи – Арнаутов Д.Р., керівник роботи – Стайкуца С.В.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2023 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи, і даємо згоду на обробку персональних даних.

Виконавець _____ / Арнаутов Д.Р./

Керівник _____ / Стайкуца С.В./

«12» 06 2023 р.

г) вміння розв'язувати виробничі та конструкторські питання _____

Під час дипломного проектування здобувач освіти Арнаутов Д.Р. мав змогу самостійно приймати окремі рішення з вибору оптимальних рішень зі стандартів та показав вміння організовано працювати над поставленим завданням, складати креслення, вивчати програмні рішення в напрямку систем протидії витокам, апаратні реалізації в напрямку технічних засобів охорони об'єктів тощо

Оцінка розрахункової частини *Відмінно*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Відмінно*

Прізвище, ім'я, по батькові керівника дипломного проекту _____

Стайкуца Сергій Володимирович

Місце роботи і посада керівника дипломного проекту _____

"Державний університет інтелектуальних технологій і зв'язку",
доцент кафедри кібербезпеки та технічного захисту інформації,
помічник декана факультету інформаційних технологій та кібербезпеки

Підпис _____

«12» 06 2023 р.