Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«__» _____ 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Метод впровадження стратегій кібербезпеки підприємства малого бізнесу»

Виконавець: студент ІІ курсу, групи КБм-21

_____ **Владислав ЯКОВЕНКО**
(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Олександр ЛАПТЄВ	
Нормоконтроль	Іван БІЛОКОНЬ	

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«25» жовтня 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача(ки) КБм-21 (група) Яковенка Владислава Юрійовича (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Метод впровадження стратегій кібербезпеки підприємства малого бізнесу

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 4 від 24.10.2024 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес впровадження стратегій кібербезпеки підприємства малого бізнесу
Предмет досліджень	Методи впровадження стратегій кібербезпеки підприємства малого бізнесу
Мета	Розробка методу та видача рекомендацій щодо впровадження стратегій кібербезпеки підприємства малого бізнесу
Вихідні дані для проведення роботи	Методи впровадження стратегій кібербезпеки

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна	Наукова новизна полягає у розробці методології впровадження адаптованої стратегії кібербезпеки для підприємств малого бізнесу на базі NIST CSF 2.0
Практична цінність	Практична цінність полягає у наданні конкретного керівництва для ефективного впровадження кібербезпеки підприємствами малого бізнесу з обмеженими ресурсами.

4. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки завдання	25.10.2024 – 24.10.2024
Аналіз літературних джерел	29.01.2025 – 11.02.2025
Обґрунтування вибору рішення	12.02.2025 – 15.02.2025
Збір даних	16.02.2025 – 04.03.2025
Виконати аналітичний огляд методів впровадження стратегії кібербезпеки підприємства малого бізнесу	05.03.2025 – 21.03.2025
Проаналізувати методи впровадження стратегії кібербезпеки підприємства малого бізнесу.	22.03.2025 – 08.04.2025
Розробити метод впровадження стратегії кібербезпеки підприємства малого бізнесу.	09.04.2025 – 10.05.2025
Розробка методичних рекомендацій щодо впровадження стратегії кібербезпеки підприємства малого бізнесу.	09.04.2025 – 10.05.2025
Апробація роботи на науково-методичному семінарі.	10.05.2025 – 12.05.2025
Оформлення пояснювальної записки згідно методичних рекомендацій	13.05.2025 – 15.05.2025
Подача пакета документів на розгляд ЕК	15.05.2025 – 19.05.2025

Завдання видав _____ Олександр ЛАПТЄВ
(підпис) (Ім’я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Владислав ЯКОВЕНКО
(підпис) (Ім’я, ПРІЗВИЩЕ)

Дата видачі завдання: 25.10.2024 р.
Термін подання кваліфікаційної роботи до ЕК 19.05.2025

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Метод впровадження стратегій кібербезпеки підприємства малого бізнесу»: 114 сторінки, 9 таблиць. Список використаних джерел включає 27 найменування.

Методи дослідження кваліфікаційної роботи:

- аналіз літератури
- аналіз документів;
- порівняння;

Об’єкт дослідження : є процес впровадження стратегії кібербезпеки підприємства малого бізнесу.

Предмет дослідження – методи впровадження стратегії кібербезпеки підприємства малого бізнесу.

Практичне значення дослідження полягає у можливості використання отриманих результатів для покращення кібербезпеки малих підприємств та їхньої захищеності від кіберзагроз, що допоможе забезпечити стабільну роботу та захистити інформаційні активи.

У роботі проаналізована існуюча література з теорії методи впровадження стратегій кібербезпеки підприємства малого бізнесу, виконаний аналіз документів, порівняння, вивчення та узагальнення вітчизняної й зарубіжної практики з теми методи впровадження стратегій кібербезпеки підприємства малого бізнесу.

Розроблено цільовий профіль безпеки підприємства як один із методів впровадження кібербезпеки підприємства малого бізнесу.

Ключові слова: Кібербезпека малого бізнесу, Впровадження стратегій кібербезпеки, Методи впровадження, NIST Cybersecurity Framework 2.0, Оцінка ризиків кібербезпеки, Цільовий профіль безпеки, План впровадження, Засоби забезпечення інформаційної безпеки, KPI кібербезпеки, Управління кіберризиками, CIS Controls, ISO 27001, Практичний приклад.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

COBIT – Control Objectives for Information and related Technology
ISACA – Information Systems Audit and Control Association
CIS – Center for Internet Security (Центр Інтернет-безпеки)
IG – Implementation Group (Група впровадження CIS Controls)
NIST – National Institute of Standards and Technology
CSF – Cybersecurity Framework
GV – Govern (Функція NIST CSF 2.0 – Управління)
ID – Identify (Функція NIST CSF – Ідентифікація)
PR – Protect (Функція NIST CSF – Захист)
DE – Detect (Функція NIST CSF – Виявлення)
RS – Respond (Функція NIST CSF – Реагування)
RC – Recover (Функція NIST CSF – Відновлення)
SoA – Statement of Applicability
BYOD – Bring Your Own Device
MFA – Multi-Factor Authentication
RTO – Recovery Time Objective (Цільовий час відновлення)
RPO – Recovery Point Objective (Цільова точка відновлення)
CSA – Cloud Security Alliance
CCM – Cloud Controls Matrix (Матриця хмарних контролів CSA)
CSP – Cloud Service Provider (Постачальник хмарних послуг)
CSC – Cloud Service Consumer (Споживач хмарних послуг)
KPI – Key Performance Indicator
SIEM – Security Information and Event Management
IR – Incident Response (Реагування на інциденти)
ПЗ – Програмне забезпечення
МСП – Мале та середнє підприємство
ІТ – Інформаційні технології
СУІБ – Система управління інформаційною безпекою
CIA – Confidentiality, Integrity, Availability
PDCA – Plan-Do-Check-Act (Цикл плануй-виконуй-перевіряй-дій)

ЗМІСТ

ВСТУП

Розвиток цифрових технологій значно змінив підхід до управління даними та процесами в малому бізнесі, відкривши нові можливості для оптимізації, автоматизації та підвищення ефективності роботи. Однак разом із цими перевагами зростає і кількість кіберзагроз, пов’язаних із несанкціонованим доступом, витоками інформації, атак на інфраструктуру та іншими аномальними подіями. Забезпечення кібербезпеки є критично важливим завданням для малого бізнесу, яке потребує комплексного підходу та застосування сучасних технологій для моніторингу, аналізу та реагування на загрози.

Спершу важливо ідентифікувати та оцінити потенційні загрози, щоб розробити відповідні заходи захисту. Далі слід створити чіткі правила та процедури для захисту даних, управління доступом та реагування на інциденти, що є основою будь-якої стратегії кібербезпеки. Також регулярне навчання співробітників правилам кібербезпеки допомагає мінімізувати людський фактор та підвищити загальний рівень обізнаності про загрози. Застосування рішень на основі штучного інтелекту та машинного навчання дозволяє автоматизувати процеси виявлення та реагування на аномалії, підвищуючи ефективність захисту. Постійний моніторинг систем та аналіз подій допомагає оперативно виявляти та усувати загрози. Нарешті, регулярне створення резервних копій даних гарантує їхнє відновлення у разі втрати чи пошкодження.

Актуальність даної теми зумовлена необхідністю забезпечення захисту інформації та стабільної роботи малих підприємств в умовах зростання кіберзагроз. Впровадження ефективних стратегій кібербезпеки дозволить не лише підвищити рівень захисту, а й оптимізувати процеси управління безпекою, використовуючи сучасні інструменти та технології.

Мета роботи — є розробка методу та видача рекомендацій щодо впровадження стратегії кібербезпеки підприємства малого бізнесу.

Перелік питань, які мають бути розроблені:

• аналіз методів впровадження стратегії кібербезпеки підприємства малого бізнесу.

• розробка методу впровадження стратегії кібербезпеки підприємства малого бізнесу;

• розробка методичних рекомендацій щодо впровадження стратегії кібербезпеки підприємства малого бізнесу.

Об’єкт дослідження : є процес впровадження стратегії кібербезпеки підприємства малого бізнесу.

Предмет дослідження – методи впровадження стратегії кібербезпеки підприємства малого бізнесу.

Практичне значення дослідження полягає у можливості використання отриманих результатів для покращення кібербезпеки малих підприємств та їхньої захищеності від кіберзагроз, що допоможе забезпечити стабільну роботу та захистити інформаційні активи.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ МАЛОГО БІЗНЕСУ

1.1. Основні поняття та визначення кібербезпеки

У сучасному цифровому середовищі, де інформаційні технології пронизують усі бізнес-процеси, кібербезпека стає невід'ємною складовою успішного функціонування підприємств будь-якого масштабу. Особливо це стосується малого бізнесу, який через обмежені ресурси та відсутність спеціалізованих IT-підрозділів часто опиняється вразливим перед новітніми кіберзагрозами. Власники змушені одночасно розв'язувати питання операційної ефективності та захищеності даних від комерційної таємниці до персональної інформації клієнтів. Цифрова трансформація відкриває нові можливості для розвитку, але водночас породжує ризики: фішингові атаки, шкідливе ПЗ, несанкціонований доступ до мереж і вразливості в програмному забезпеченні. У цьому підрозділі ми визначимо ключові терміни та поняття кібербезпеки, проведемо їх відмежування від ширшої інформаційної безпеки, а також окреслимо три базові принципи — конфіденційність, цілісність і доступність які лежать в основі будь-якої стратегії захисту малого підприємства.

Кібербезпека – це сукупність заходів, спрямованих на захист IT-систем (апаратури, мереж, програмного забезпечення) та оброблюваної ними інформації від несанкціонованого доступу, модифікації та збоїв. Згідно з Законом України «Про основні засади забезпечення кібербезпеки України», [1] кібербезпека визначається як «захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час використання кіберпростору». Практично це означає, що кібербезпека охоплює заходи для забезпечення безпечного функціонування інформаційних технологій та запобігати цифровим загрозам. Водночас поняття інформаційної безпеки є ширшим і стосується захисту інформації в будь-яких формах та середовищах (не тільки цифрових) – зокрема фізичних носіїв і процесів роботи з даними. У цьому контексті кібербезпеку можна розглядати як підмножину

інформаційної безпеки, орієнтовану на сучасний IT-простір. Мова йде про забезпечення конфіденційності, цілісності та доступності інформації в цифровому просторі за допомогою технічних та організаційних засобів.

Основою будь-якої системи кіберзахисту є три базові принципи — -- конфіденційність, цілісність та доступність (C-I-A) даних. Ці принципи гарантовано забезпечують надійний захист даних безпеки IT інфраструктури організації. Згідно з фаховим підходом, вони формулюються таким чином:

Конфіденційність (Confidentiality) означає, що доступ до даних мають лише уповноважені особи, а будь-яке несанкціоноване ознайомлення з ними або витік вважається порушенням безпеки. У цифровому контексті концепція конфіденційності реалізується через механізми автентифікації, шифрування та ознак доступу.

Цілісність (Integrity) передбачає захист даних від несанкціонованих змін, підробки або випадкових пошкоджень. Системи забезпечення цілісності здійснюють контроль контрольних сум, цифрові підписи й записи в журналі змін, що дозволяють вчасно виявити та виправити будь-які спотворення вмісту.

Доступність (Availability) гарантує, що потрібна інформація або сервіс будуть доступні для уповноважених користувачів у потрібний момент. Для малих підприємств це особливо критично: простій фінансової системи чи CRM може призвести до збитків і втрати довіри клієнтів. Забезпечення доступності включає регулярне резервне копіювання, плани відновлення після збоїв (Disaster Recovery Plans) та мультиканальне дублювання критичних сервісів.[2]

Особливості малого бізнесу в контексті кібербезпеки

Малий бізнес (включаючи малі підприємства) на практиці характеризується обмеженим масштабом діяльності: за класифікацією ЄС це фірми з менш ніж 50 працівниками (при річному обороті до 10 мільйонів євро). У контексті кібербезпеки це означає суттєві обмеження ресурсів. Часто в такому бізнесі немає власного IT відділу чи відповідальних за безпеку фахівців, а бюджети на захист інформації мінімальні. Як наслідок, мережі та системи малого підприємства зазвичай вразливіші тому зловмисники сприймають їх як легку ціль і активно застосовують до них тактики соціальної інженерії та інші типові атаки.

- Обмежені ресурси. У фірмах з малою кількістю працівників часто відсутній повноцінний штат IT безпеки, тому безпекові заходи формально покладаються на одне Нестача коштів на кібербезпеку призводить до відсутності інвестицій у сучасні рішення (антивірус, фаєрволи, системи резервного копіювання тощо) і регулярне навчання персоналу.
- Вразливість до людського фактора. Співробітники малих компаній рідше мають високий рівень кібергігієни та спеціального навчання. Через це вони частіше піддаються фішинговим атакам та іншим формам соціальної інженерії. Згідно зі статистикою, працівники малих фірм піддаються набагато більшій кількості таких атак порівняно з великими організаціями.
- Наслідки атак. Емпіричні дані свідчать, що кіберінцидент для малого бізнесу може бути критичним: близько 60% малих підприємств вже зазнавали хоча б одного витоку конфіденційної інформації. Крім фінансових збитків, зазвичай відбувається суттєве падіння довіри клієнтів. Дослідження показують, що приблизно 60% уразливих малих компаній змушені припинити діяльність протягом шести місяців після серйозної кібератаки.

Таким чином, особливості малого бізнесу — невелика чисельність персоналу, обмежене фінансування і слабка захищеність визначають як специфічну спрямованість захисту (акцент на прості та доступні рішення, консалтинг, аутсорсинг), так і високі ризики реалізації кіберзагроз. У наступних розділах магістерської роботи ці фактори будуть враховані при розробці методів впровадження стратегій кібербезпеки для малих підприємств, адже успіх таких стратегій прямо залежить від реальних можливостей і характеру ризиків конкретного малого бізнесу.

1.2. Особливості кіберзагроз для малого бізнесу. Типи загроз (фішинг, ransomware, шкідливе ПЗ тощо).

У сучасному цифровому світі, де технології стають неодмінною складовою будь-якого бізнесу, інформаційна безпека стає дедалі важливішою. Підприємства

малого бізнесу, які займають значну частку економіки, не є винятком. Вони стикаються з різноманітними інформаційними загрозами, які можуть поставити під загрозу їхню діяльність, конфіденційність даних та репутацію ось огляд таких загроз:

Кібератака – це будь-яка навмисна спроба викрасти, викрити, змінити, вивести з ладу або знищити дані, програми чи інші активи шляхом несанкціонованого доступу до мережі, комп'ютерної системи чи цифрового пристрою.

Мотиви кібератак можуть бути різними, але є три основні категорії: кримінальні, політичні та особисті.

Кримінально мотивовані зловмисники прагнуть отримати фінансову вигоду через крадіжку грошей, крадіжку даних або зрив бізнесу. Кіберзлочинці можуть зламати банківський рахунок, щоб безпосередньо вкрасти гроші, або використовувати шахрайство соціальної інженерії, щоб обманом змусити людей надіслати їм гроші. Хакери можуть викрасти дані та використати їх для крадіжки особистих даних або продати їх у темній мережі чи зберігати їх для отримання викупу.

Вимагання — ще одна популярна тактика. Хакери можуть використовувати програми-вимагачі, атаки DDoS або інші тактики, щоб утримувати дані чи пристрої в заручниках, доки компанія не заплатить.[3]

Особисто мотивовані зловмисники, такі як незадоволені нинішні чи колишні працівники, насамперед прагнуть відплати за якусь уявну образу. Вони можуть взяти гроші, викрасти конфіденційні дані або порушити роботу систем компанії.

Політично мотивовані зловмисники часто асоціюються з кібервійною, кібертероризмом. У кібервійні суб'єкти національної держави часто атакують урядові установи чи критичну інфраструктуру своїх ворогів. Наприклад, з початку російсько-української війни обидві країни зазнали низки кібератак на життєво важливі установи. Хакери-активісти, яких називають «хактивістами», можуть не завдати значної шкоди своїм цілям. Натомість вони зазвичай прагнуть привернути увагу до своїх причин, оприлюднюючи свої напади громадськості.

Менш поширені мотиви кібератак включають корпоративне шпигунство, під час якого хакери викрадають інтелектуальну власність, щоб отримати несправедливу

перевагу над конкурентами, і пильних хакерів, які використовують вразливі місця системи, щоб попередити про них інших.

Здійснювати кібератаки можуть злочинні організації, державні суб'єкти та приватні особи. Один зі способів класифікувати суб'єктів загрози — класифікувати їх як сторонніх або внутрішніх загроз.

Зовнішні загрози не мають права використовувати мережу чи пристрій, але все одно проникають. Зовнішні суб'єкти кіберзагрози включають організовані злочинні групи, професійних хакерів, спонсорованих державою акторів, хакерів-любителів і хактивістів.

Інсайдерські загрози — це користувачі, які мають авторизований і законний доступ до активів компанії та зловживають своїми привілеями навмисно чи випадково. До цієї категорії входять співробітники, ділові партнери, клієнти, підрядники та постачальники з доступом до системи.

Хоча недбалі користувачі можуть наражати свої компанії на небезпеку, кібератака вважається лише тоді, коли користувач навмисно використовує свої права для здійснення зловмисної діяльності. Співробітник, який недбало зберігає конфіденційну інформацію на незахищеному диску, не вчиняє кібератаку, але незадоволений працівник, який свідомо робить копії конфіденційних даних для особистої вигоди.[4]

Зловмисники зазвичай проникають у комп'ютерні мережі, тому що шукають щось конкретне.

Загальні цілі включають:

- Кошти;
- Фінансові дані підприємств;
- Списки клієнтів;
- Дані клієнта, включно з ідентифікаційною інформацією або іншими конфіденційними персональними даними;
- Адреси електронної пошти та облікові дані для входу;
- Інтелектуальна власність, як-от комерційна таємниця або дизайн продукту;

У деяких випадках кібератаки взагалі не хочуть нічого красти.

Швидше, вони просто хочуть порушити роботу інформаційних систем чи IT-інфраструктури, щоб завдати шкоди бізнесу, державній установі чи іншій цілі.

Кіберзлочинці використовують багато складних інструментів і методів для здійснення кібератак на корпоративні IT-системи, персональні комп'ютери та інші цілі. Деякі з найпоширеніших типів кібератак включають:

Зловмисне програмне забезпечення також відоме як шкідливий код або зловмисне програмне забезпечення. Зловмисне програмне забезпечення – це програма, яка вставляється в систему для порушення конфіденційності, цілісності або доступності даних. Це робиться таємно та може вплинути на ваші дані, програми чи операційну систему. Зловмисне програмне забезпечення стало однією з найбільш значущих зовнішніх загроз для систем. Зловмисне програмне забезпечення може завдати значних збитків і збоїв і потребує великих зусиль у більшості організацій.

Шпигунське програмне забезпечення, шкідливе програмне забезпечення, призначене для порушення конфіденційності, також стало серйозною проблемою для організацій. Хоча зловмисне програмне забезпечення, що порушує конфіденційність, використовується протягом багатьох років, останнім часом воно стало набагато поширенішим. Шпигунське програмне забезпечення проникає в багато систем для відстеження особистої діяльності та фінансового шахрайства.

Організації також стикаються з подібними загрозами від кількох форм нешкідливого програмного забезпечення. Ці форми кіберзагроз часто пов'язані зі зловмисним програмним забезпеченням. Більш поширеною формою є фішинг. Фішинг передбачає обманним шляхом змусити людей розкрити конфіденційну або особисту інформацію. Троянські коні маскуються під корисні програми або ховаються в законному програмному забезпеченні, щоб обманом змусити користувачів встановити їх. Троян віддаленого доступу (RAT) створює секретний бекдор на пристрої жертви, тоді як троян-дропер встановлює додаткове зловмисне програмне забезпечення, коли має точку опори. SQL ін'єкція — це тип кібератаки, яка використовує вразливості вебдодатків для вставки шкідливого коду SQL, що дозволяє зловмисникам маніпулювати базами даних і викрадати конфіденційну інформацію.

Цей тип атаки може мати серйозні наслідки, що призведе до витоку даних, несанкціонованого доступу до конфіденційних записів і навіть до повної втрати контролю над базою даних. Щоб запобігти атакам SQL-ін’єкцій, розробникам вкрай важливо очищати введені користувачем дані, використовувати параметризовані запити та здійснювати перевірку введених даних, щоб забезпечити обробку лише безпечних і очікуваних даних.

Брандмауери додатків і регулярні перевірки безпеки також можуть допомогти виявити та зменшити потенційні вразливості, сприяючи більш надійному захисту від кіберзагроз.

Атаки на паролі — це кібератаки, спрямовані на компрометацію паролів користувачів за допомогою таких методів, як атаки грубою силою або викрадення облікових даних, підкреслюючи вразливі місця в механізмах контролю доступу. Атаки грубої сили включають автоматизовані інструменти, які намагаються вгадати паролі незліченними комбінаціями символів, використовуючи слабкі або легко вгадані паролі. З іншого боку, викрадення облікових даних відбувається, коли хакери отримують несанкціонований доступ до збережених паролів, часто через фішингові шахрайства або зловмисне програмне забезпечення. Для захисту особистих і конфіденційних даних вирішальним є застосування безпечних паролів. Важливо створювати надійні паролі, які поєднують літери, цифри та спеціальні символи, уникаючи загальних слів або послідовностей. Використання унікальних паролів для кожного облікового запису та їх регулярне оновлення може значно зменшити ризик атак на пароль.

Внутрішні загрози стосуються того, що окремі особи в організації використовують свої привілеї доступу, щоб навмисно чи ненавмисно порушити безпеку даних, створюючи значний ризик у довіреному середовищі

Ці люди можуть мати різноманітні мотиви, такі як особиста вигода, помста, ідеологія або просто необережність. Вони можуть використовувати свої знання про системи організації, щоб отримати доступ до конфіденційної інформації або порушити роботу. Організації повинні впроваджувати надійні заходи безпеки для ефективного запобігання та виявлення внутрішніх загроз. Це включає ретельний

моніторинг діяльності співробітників, обмеження доступу за принципом найменших привілеїв, впровадження надійних механізмів автентифікації та проведення регулярних тренінгів з безпеки.

Програми-вимагачі — це складні шкідливі програми, які використовують надійне шифрування, щоб утримувати дані або системи в заручниках. Потім кіберзлочинці вимагають оплату в обмін на звільнення системи та відновлення функціональності.

Scareware використовує фальшиві повідомлення, щоб залякати жертв і змусити їх завантажити зловмисне програмне забезпечення або передати конфіденційну інформацію шахраям.

Шпигунське програмне забезпечення – це тип зловмисного програмного забезпечення, яке таємно збирає конфіденційну інформацію, як-от імена користувачів, паролі та номери кредитних карток. Потім він надсилає цю інформацію назад хакеру.

Руткіти — це пакети зловмисних програм, які дозволяють хакерам отримати доступ на рівні адміністратора до операційної системи комп’ютера чи інших ресурсів.

Хробаки — це шкідливий код, що самовідтворюється, який може автоматично поширюватися між програмами та пристроями.

Атаки соціальної інженерії спонукають людей робити те, чого вони не повинні робити, наприклад ділитися інформацією, якою вони не повинні ділитися, завантажувати програмне забезпечення, яке вони не повинні завантажувати, або надсилати гроші злочинцям.[5]

Фішинг є однією з найпоширеніших атак соціальної інженерії. Найпростіші фішингові шахрайства використовують фальшиві електронні листи або текстові повідомлення для викрадення облікових даних користувачів, викрадання конфіденційних даних або поширення зловмисного програмного забезпечення. Фішингові повідомлення часто створюються так, ніби вони надходять із законного джерела. Зазвичай вони спрямовують жертву натиснути гіперпосилання, яке переведе її на шкідливий вебсайт, або відкрити вкладення електронної пошти, яке виявляється шкідливим програмним забезпеченням.

Кіберзлочинці також розробили більш витончені методи фішингу.

Фішинг — це цілеспрямована атака, спрямована на маніпулювання конкретною особою, часто з використанням деталей із загальнодоступних профілів жертви в соціальних мережах, щоб зробити обман більш переконливим. Китовий фішинг – це тип стрімкого фішингу, спрямований спеціально на високопоставлених керівників компаній. У шахрайстві з компрометацією бізнес електронної пошти (BEC) кіберзлочинці видають себе за керівників, продавців або інших ділових партнерів, щоб обманом змусити жертв переказувати гроші або надати конфіденційні дані.

Атаки типу «відмова в обслуговуванні» (DoS) і розподілена «відмова в обслуговуванні» (DDoS) переповнюють ресурси системи шахрайським трафіком. Цей трафік перевантажує систему, перешкоджаючи відповідям на законні запити та знижуючи здатність системи працювати. Атака типу «відмова в обслуговуванні» може бути самоціллю або підготовкою до іншої атаки.

Різниця між DoS-атаками та DDoS-атаками полягає просто в тому, що DoS-атаки використовують одне джерело для створення шахрайського трафіку, тоді як DDoS-атаки використовують кілька джерел. DDoS-атаки часто здійснюються за допомогою ботнету, мережі підключених до Інтернету заражених шкідливим програмним забезпеченням пристроїв під контролем хакера. Ботнети можуть включати ноутбуки, смартфони та пристрої Інтернету речей (IoT). Жертви часто не знають, коли ботнет захопив їхні пристрої.

Під час атаки "людина посередині" (MiTM), яка також називається "атакою підслуховування", хакер таємно перехоплює зв'язок між двома людьми або між користувачем і сервером. Атаки MitM зазвичай здійснюються через незахищені публічні мережі Wi-Fi, де зловмисникам відносно легко шпигувати за трафіком.

Хакери можуть читати електронні листи користувача або навіть таємно змінювати електронні листи до того, як вони дійдуть до одержувача. Під час атаки з захопленням сеансу хакер перериває з’єднання між користувачем і сервером, на якому розміщені важливі активи, як-от конфіденційна база даних компанії. Хакер змінює свою IP-адресу на адресу користувача, змушуючи сервер думати, що це

законний користувач, який увійшов у законний сеанс. Це дає хакеру повну свободу для крадіжки даних або іншим чином сіяти хаос.

Щоб захистити себе від загроз кібербезпеці, потрібно вживати профілактичних заходів, наприклад використовувати надійні паролі, регулярно оновлювати програмне забезпечення та навчати себе та своїх співробітників найкращим практикам кібербезпеки.

Одним з важливих аспектів захисту кібербезпеки, який часто не помічають, є важливість регулярного моніторингу ваших облікових записів електронної пошти на наявність будь-якої підозрілої активності. Хакери часто атакують людей через фішингові електронні листи, намагаючись обманом змусити їх надати конфіденційну інформацію

Зберігаючи пильність і уникаючи натискання підозрілих посилань або вкладень, ви можете значно зменшити ризик стати жертвою таких загроз. Використання надійного брандмауера на ваших пристроях може стати першою лінією захисту від несанкціонованого доступу та атак зловмисного програмного забезпечення.

Використання надійних паролів є фундаментальним кроком у підвищенні кібербезпеки, захисті конфіденційних облікових записів і даних від несанкціонованого доступу шляхом використання складних і унікальних комбінацій паролів.

У сфері кібербезпеки надійність пароля часто визначає рівень захисту від зловмисників. Зі зростанням складності кіберзагроз вкрай важливо застосовувати надійні паролі для посилення безпеки в Інтернеті.

Важлива порада щодо створення надійних паролів — уникати використання інформації, яку легко вгадати, як-от дати народження чи загальні слова. Натомість оберіть комбінацію великих і малих літер, цифр і спеціальних символів для посилення складності.

Реалізація багатофакторної автентифікації додає додатковий рівень безпеки, вимагаючи від користувачів додаткового підтвердження, окрім простого пароля. Це значно знижує ризик несанкціонованого доступу, навіть якщо пароль зламано. У

сучасному цифровому середовищі, де кібератаки нестримні, цей додатковий етап автентифікації є важливим.

Регулярне оновлення програмного забезпечення має вирішальне значення для кібербезпеки, оскільки воно допомагає виправляти відомі вразливості, покращувати продуктивність системи та захищати від нових загроз, гарантуючи, що системи зміцнені останніми оновленнями безпеки.

Оновлення програмного забезпечення відіграють вирішальну роль у підтримці гігієни кібербезпеки в організації. Практики керування виправленнями є важливими в цьому відношенні, оскільки вони включають виявлення, отримання, тестування та встановлення оновлень для усунення вразливостей програмного забезпечення. Автоматизація процесів оновлення може оптимізувати це важливе завдання, гарантуючи постійний захист систем.

Ризики використання застарілого програмного забезпечення різноманітні, наражаючи організації на можливі порушення, втрату даних і невідповідність нормативним вимогам. Слідкуючи за оновленнями програмного забезпечення, компанії можуть значно зменшити свою сприйнятливість до кіберзагроз і зміцнити загальну безпеку.

Будьте обережні з підозрілими електронними листами та вебсайт

Обережність щодо підозрілих електронних листів і вебсайт є важливою для обізнаності про кібербезпеку, оскільки шкідливі електронні листи та вебсайт можуть приховувати спроби фішингу, завантаження зловмисного програмного забезпечення та схеми соціальної інженерії, які загрожують особистій і організаційній безпеці.[6]

Оцінюючи легітимність електронного листа, зверніть увагу на адресу електронної пошти відправника, особливо якщо вона здається незвичною або якщо доменне ім’я написане з помилкою. Фішингові електронні листи часто містять термінові висловлювання або запити на конфіденційну інформацію, створені для того, щоб створити відчуття терміновості та спонукати вас діяти без критичних роздумів. Дуже важливо уникати натискання посилань або завантаження вкладених файлів із невідомих джерел, оскільки вони можуть призвести до інфікування вашого пристрою зловмисним програмним забезпеченням.

Використання брандмауера є критично важливим заходом кібербезпеки, який діє як бар’єр між мережею та потенційними загрозами, відстежуючи та контролюючи вхідний і вихідний трафік для захисту систем від несанкціонованого доступу та зловмисних дій.

Брандмауери відіграють важливу роль у безпеці мережі, аналізуючи пакети даних і визначаючи, чи дозволити їм проходження на основі попередньо визначених правил безпеки. Існує декілька типів брандмауерів, таких як брандмауери з фільтрацією пакетів, брандмауери проксі, брандмауери перевірки стану та брандмауери наступного покоління, кожен із яких має свої сильні та слабкі сторони.

Впроваджуючи освітні та навчальні програми з кібербезпеки, компанії можуть значно знизити ризик стати жертвою кібератак. Ці програми не тільки озброюють співробітників знаннями щодо виявлення та пом’якшення потенційних загроз, але й прищеплюють почуття відповідальності за захист конфіденційних даних і активів компанії.

Таким чином малі підприємства потрапляють під тиск кіберзагроз через поєднання обмежених ресурсів і високої зацікавленості з боку зловмисників. Комплексний аналіз типів атак, мотивів та цілей, а також розуміння внутрішніх вразливостей дозволить надалі сформувати адаптовані стратегії захисту, що враховуватимуть баланс між ефективністю заходів і економічними можливостями малого бізнесу.

1.3. Огляд стратегій та стандартів кібербезпеки

Управління інформаційною безпекою та IT є критично важливим для стабільності та успіху будь-якої сучасної організації. Міжнародні стандарти та фреймворки надають структуровані підходи та найкращі практики для досягнення цих цілей. Розглянемо детальніше чотири з найбільш впливових: ISO/IEC 27001, COBIT, CIS Controls та NIST Cybersecurity Framework 2.0.

1. ISO/IEC 27001:2022 – Системи управління інформаційною безпекою (СУІБ)

Призначення та Специфіка:

ISO/IEC 27001 є провідним міжнародним стандартом, який визначає вимоги до встановлення, впровадження, функціонування, моніторингу, перегляду, підтримки та покращення документованої системи управління інформаційною безпекою (СУІБ) в контексті загальних бізнес-ризиків організації. Основна мета стандарту – допомогти організаціям захистити свої інформаційні активи шляхом впровадження систематичного підходу до управління інформаційною безпекою, що враховує загрози, уразливості та впливи.[7]

Стандарт базується на циклі Plan-Do-Check-Act (PDCA), який сприяє постійному поліпшенню СУІБ. Він орієнтований на захист конфіденційності, цілісності та доступності (Тріада CIA) інформації.

Ключові Принципи:

Системний підхід: ISO 27001 не є просто переліком контролів, а вимагає побудови цілісної системи управління.

Управління ризиками: В основі СУІБ лежить процес управління ризиками інформаційної безпеки, який включає ідентифікацію, аналіз, оцінку та обробку ризиків.

Постійне поліпшення: СУІБ повинна регулярно переглядатися та вдосконалюватися відповідно до мінливих умов та нових загроз.

Відповідність: Стандарт допомагає організаціям відповідати законодавчим, нормативним та договірним вимогам, пов'язаним з інформаційною безпекою.

Залучення керівництва: Вимагає активної участі та підтримки вищого керівництва.

Структура стандарту (на основі ISO/IEC 27001:2022):

Стандарт складається з 11 розділів та Додатку А:

Розділ 1-3: Вступ, сфера застосування, нормативні посилання, терміни та визначення.

Розділ 4: Контекст організації: Розуміння організації та її контексту, потреб та очікувань зацікавлених сторін, визначення сфери застосування СУІБ.

Розділ 5: Лідерство: Зобов'язання керівництва, політика інформаційної безпеки, ролі, відповідальність та повноваження в організації.

Розділ 6: Планування: Дії для визначення ризиків та можливостей, цілі інформаційної безпеки та плани їх досягнення, планування змін.

Розділ 7: Підтримка: Ресурси, компетентність, обізнаність, комунікації, документована інформація.

Розділ 8: Функціонування: Планування та контроль функціонування, оцінка ризиків інформаційної безпеки, обробка ризиків інформаційної безпеки.

Розділ 9: Оцінка результативності: Моніторинг, вимірювання, аналіз та оцінка, внутрішній аудит, аналіз з боку керівництва.

Розділ 10: Поліпшення: Невідповідності та коригувальні дії, постійне поліпшення.

Додаток А: Заходи контролю інформаційної безпеки: Цей додаток (який деталізовано в ISO/IEC 27002) містить перелік заходів контролю, організованих за чотирма темами:

- А.5 Організаційні заходи контролю
- А.6 Особистісні заходи контролю
- А.7 Фізичні заходи контролю
- А.8 Технологічні заходи контролю

Організація повинна вибрати відповідні заходи контролю з додатком А (або інші заходи), ґрунтуючись на результатах оцінки ризиків, та задокументувати свій вибір у Заяві про застосовність (SoA).

Переваги:

- Підвищення рівня інформаційної безпеки.
- Зменшення ризиків інцидентів безпеки.
- Демонстрація відповідності вимогам клієнтів та регуляторів.
- Підвищення довіри з боку партнерів та клієнтів.
- Систематизація процесів управління безпекою.
- Можливість отримання міжнародної сертифікації.

2. COBIT 2019 – Фреймворк для управління та врядування корпоративними IT

Призначення та Специфіка:

COBIT (Control Objectives for Information and related Technology) є світовим фреймворком від ISACA, який надає комплексний підхід до управління та врядування інформацією та технологіями (IT) на корпоративному рівні. COBIT 2019 є останньою версією, яка розвиває попередні ітерації, надаючи гнучкіший та відкритіший фреймворк.[8]

Основна мета COBIT – допомогти організаціям досягти їхніх цілей шляхом ефективного використання IT, забезпечуючи при цьому баланс між реалізацією переваг, оптимізацією рівня ризиків та використанням ресурсів. Він надає структурований підхід до врядування та управління IT для всієї організації, а не лише для IT-департаменту.

Ключові Принципи Системи Врядування:

COBIT 2019 базується на шести принципах для системи врядування:

1. Надання цінності зацікавленим сторонам: Кожна організація існує для створення цінності для своїх зацікавлених сторін. Система врядування повинна враховувати потреби всіх зацікавлених сторін та трансформувати їх у діяльні цілі.

2. Цілісний підхід: Система врядування складається з низки взаємодіючих компонентів. Ці компоненти повинні розглядатися цілісно для ефективного врядування та управління.

3. Динамічна система врядування: Зміни в зовнішньому середовищі або всередині організації можуть призвести до необхідності модифікації системи врядування.

4. Чітке розмежування врядування та управління: Врядування полягає в оцінці потреб, визначенні напрямку та моніторингу результативності. Управління полягає в плануванні, побудові, запуску та моніторингу діяльності відповідно до напрямку, визначеного врядуванням.

5. Адаптація до потреб підприємства: Фреймворк повинен бути достатньо гнучким, щоб бути адаптованим до конкретних потреб організації за допомогою факторів дизайну.

6. Наскрізне врядування: Система врядування та управління IT повинна охоплювати всю організацію, включаючи всі функції та процеси, де використовується IT.

Компоненти Системи Врядування та Управління:

COBIT 2019 визначає сім типів компонентів, які окремо та колективно підтримують систему врядування та управління IT:

1. Процеси: Набір дій, спрямованих на досягнення певних результатів.
2. Організаційні структури: Ключові особи та групи в організації.
3. Інформація: Інформація, необхідна для підтримки ефективного функціонування системи врядування та управління.
4. Культура, етика та поведінка: Індивідуальна та колективна поведінка в організації.
5. Навички та компетенції: Необхідні навички та знання персоналу.
6. Послуги, інфраструктура та додатки: Технології, що забезпечують обробку інформації та надання послуг.
7. Політики та процедури: Формальні правила та методи діяльності.

Структура COBIT 2019:

COBIT 2019 Framework: Introduction and Methodology: Представляє основні концепції та термінологію.

COBIT 2019 Framework: Governance and Management Objectives: Описує цілі врядування та управління, а також компоненти системи врядування.

COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution: Надає настанови щодо розробки індивідуальної системи врядування для організації, використовуючи фактори дизайну.

COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution: Надає настанови щодо впровадження та постійного покращення системи врядування.

COBIT 2019 є більш орієнтованим на бізнес та управління, надаючи фреймворк для забезпечення цінності від IT, оптимізації ризиків та використання ресурсів. Він часто використовується як основа для інтеграції інших фреймворків та стандартів.

3. CIS Controls v8 – Заходи контролю кібербезпеки

Призначення та Специфіка:

CIS Controls (Center for Internet Security Controls), раніше відомі як SANS Top 20 Controls, є пріоритизованим набором заходів контролю кібербезпеки, розроблених на основі даних про реальні загрози та ефективність різних захисних заходів. Їхня основна мета – надати організаціям чіткий, дієвий та відносно простий у впровадженні набір технічних та організаційних заходів для ефективного захисту від найпоширеніших кібератак. Філософія CIS Controls базується на концепції "оборони, інформованої про загрози" (threat-informed defense), зосереджуючись на заходах, які мають найбільший вплив на зниження ризиків від відомих кіберзагроз.[9]

Ключові Принципи:

Пріоритизація: Заходи контролю пріоритизовані, дозволяючи організаціям зосередитися на найбільш критичних діях першочергово.

Дієвість: CIS Controls надають конкретні, вимірювані та технічно реалізовувані заходи.

Настанови, засновані на загрозах: Контролі розроблені на основі аналізу реальних кібератак та способів їх запобігання або пом'якшення.

Постійне вдосконалення: CIS Controls регулярно оновлюються спільнотою експертів, щоб відображати зміни в ландшафті загроз та технологіях.

Доступність: CIS Controls є безкоштовними та доступними для використання будь-якою організацією.

Структура CIS Controls v8:

У цілому v8 містить 18 широких категорій, від інвентаризації та контролю активів до тестування на проникнення та реагування на інциденти. Під кожним таким пунктом стоїть набір конкретних кроків - Safeguards - їх більше сотні, але не потрібно впроваджувати все одразу.

Групи Впровадження (Implementation Groups - IGs):

Для допомоги організаціям у пріоритизації впровадження контролів, CIS Controls v8 використовує три Групи Впровадження, засновані на профілі ризику та ресурсах організації:

- IG1: Організації з обмеженими IT-ресурсами та низьким профілем ризику. IG1 містить 56 Safeguards, які вважаються базовою кібергігієною.
- IG2: Організації з помірними IT-ресурсами та зростаючим профілем ризику. IG2 включає всі Safeguards з IG1 плюс додаткові (всього 130 Safeguards).
- IG3: Організації зі значними IT-ресурсами та високим профілем ризику (наприклад, об'єкти критичної інфраструктури). IG3 включає всі Safeguards з IG1 та IG2 плюс додаткові (всього 153 Safeguards).

CIS Controls є дуже практичним інструментом для технічних команд та менеджерів, які прагнуть впровадити конкретні заходи для підвищення рівня кіберзахисту.

4. NIST Cybersecurity Framework 2.0 – Фреймворк для покращення кібербезпеки критичної інфраструктури (розширено на всі організації)

Призначення та Специфіка:

NIST Cybersecurity Framework (CSF) був спочатку розроблений NIST у відповідь на виконавчий указ США для покращення кібербезпеки критичної інфраструктури. Версія 2.0 значно розширює сферу його застосування, роблячи його універсальним інструментом для управління кіберризиками для організацій будь-якого розміру, сектору та складності.

NIST CSF не є стандартом відповідності (як ISO 27001) або набором конкретних контролів (як CIS Controls), а скоріше гнучким, добровільним фреймворком, який допомагає організаціям зрозуміти, управляти та знижувати свої кіберризики. Він надає спільну мову та структурований підхід для покращення кібербезпеки.

Ключові Принципи:

Гнучкість та адаптивність: Фреймворк може бути адаптований до унікальних потреб та обставин будь-якої організації.

Заснований на ризиках: Підхід до кібербезпеки базується на розумінні та управлінні ризиками.

Сприяння комунікації: Надає спільну мову для внутрішньої та зовнішньої комунікації щодо кіберризиків.

Інтеграція з іншими стандартами та практиками: Фреймворк використовує та посилається на існуючі стандарти, настанови та практики.

Постійне покращення: Заохочує організації до регулярної оцінки та вдосконалення своїх заходів кібербезпеки.

Врядування як основа: Версія 2.0 виділяє функцію "Govern", підкреслюючи важливість інтеграції кіберризик менеджменту в загальну систему врядування організації.

Загальна Структура NIST Cybersecurity Framework 2.0:

NIST CSF 2.0 складається з трьох основних взаємопов'язаних компонентів:

1. Framework Core (Ядро Фреймворку): Це набір бажаних результатів кібербезпеки, організованих в ієрархічну структуру:

Функції (Functions): Наймасштабніший рівень. Вони представляють п'ять або шість (у v2.0) ключових стовпів кібербезпеки, які можуть виконуватися одночасно. У версії 2.0 додано функцію "Govern". Шість функцій:

GV (Govern): Охоплює стратегію управління кіберризиками, очікування та політику. Включає діяльність, спрямовану на встановлення та моніторинг політик, процедур та структур для управління кіберризиками на рівні всієї організації. Це включає управління ролями та відповідальністю, політиками, процесами управління ризиками та комунікаціями.

ID (Identify): Допомагає організаціям зрозуміти свій контекст управління кіберризиками. Включає діяльність, спрямовану на ідентифікацію фізичних та програмних активів, бізнес-середовища, урядування, оцінку ризиків та стратегію управління ризиками.

PR (Protect): Описує відповідні заходи безпеки для забезпечення надання критично важливих послуг. Включає діяльність, спрямовану на управління ідентифікацією та доступом, обізнаність та навчання, безпеку даних, процеси та процедури захисту інформації, обслуговування та захисні технології.

DE (Detect): Визначає діяльність для своєчасного виявлення подій кібербезпеки. Включає діяльність, спрямовану на аномалії та події, заходи моніторингу безпеки та процеси виявлення.

RS (Respond): Встановлює діяльність для вжиття заходів щодо виявленої події кібербезпеки. Включає діяльність, спрямовану на планування реагування, комунікації, аналіз, пом'якшення наслідків та покращення.

RC (Recover): Визначає відповідну діяльність для забезпечення стійкості та відновлення порушених можливостей або послуг. Включає діяльність, спрямовану на планування відновлення, покращення та комунікації.

Категорії (Categories): Підрозділи функцій, які є логічними угрупованнями результатів кібербезпеки. Наприклад, функція Identify включає категорії Asset Management, Business Environment, Governance, Risk Assessment, та Risk Management Strategy.[10]

Підкатегорії (Subcategories): Детальніші результати в рамках кожної Категорії. Вони є специфічними технічними або управлінськими діями.

Інформативні Посилання (Informative References): Конкретні розділи в інших стандартах, настановах та практиках (таких як ISO 27001, COBIT, CIS Controls, NIST SP 800-53 тощо), які демонструють, як досягти результатів, описаних у Підкатегоріях.

2. Implementation Tiers (Рівні Впровадження): Описують ступінь зрілості підходів організації до управління кіберризиками. Вони допомагають організаціям зрозуміти поточний стан та визначити цільовий рівень. Рівні не є оцінкою зрілості програми кібербезпеки, а скоріше ступенем інтеграції практик управління ризиками кібербезпеки в загальні процеси організації. Існує чотири рівні:

Tier 1: Partial (Частковий): Управління кіберризиками є неформальним, реактивним та нерегулярним.

Tier 2: Risk Informed (Інформований про ризики): Рішення щодо управління кіберризиками приймаються на основі інформації, але процес може бути неформальним та не повністю інтегрованим.

Tier 3: Repeatable (Повторюваний): Процеси управління кіберризиками формалізовані та можуть повторюватися.

Tier 4: Adaptive (Адаптивний): Організація адаптує свої практики кібербезпеки на основі уроків, отриманих з попередньої діяльності та прогнозних показників.

3. Profiles (Профілі): Являють собою вибір Категорій та Підкатегорій з Ядра Фреймворку, які організація визначила як найбільш відповідні для досягнення своїх цілей управління кіберризиками. Профілі допомагають організації узгодити свою діяльність з кібербезпеки з бізнес-вимогами, толерантністю до ризиків та ресурсами.

Current Profile (Поточний Профіль): Вказує на результати Категорій та Підкатегорій, які організація наразі досягає.

Target Profile (Цільовий Профіль): Вказує на результати Категорій та Підкатегорій, які організація прагне досягти.

Порівняння поточного та цільового профілів дозволяє організації ідентифікувати "розриви" та розробити план дій для їх усунення, пріоритизуючи інвестиції в кібербезпеку.

Переваги NIST CSF 2.0:

- Надає гнучку та адаптивну основу для управління кіберризиками.
- Сприяє покращенню комунікації щодо кіберризиків.
- Підтримує інтеграцію з існуючими процесами та іншими фреймворками.
- Допомагає організаціям визначати пріоритети для інвестицій у кібербезпеку.
- Розширює сферу застосування на всі організації, не лише критичну інфраструктуру.
- Посилює фокус на врядуванні.

Таблиця 1.1

Порівняльна таблиця стандартів для впровадження у МСП

Критерії	ISO/IEC 27001	COBIT	CIS Controls	NIST CSF 2.0
Рівень	Системний ISMS	Управління IT	Тактичний контроль	Рамкова модель
Мета	Сертифікація	Бізнес-орієнтація	Швидкий запуск	Кіберстійкість
Ресурси	Високі	Високі	Помірні	Гнучкі

продовження таблиці 1.1

Складність впровадження	Висока	Висока	Середня	Середня/Низька
Підтримка МСП	Так, адаптовано	Так, скорочено	Так, адаптовано	Так, за допомогою профілів

Взаємозв'язок та компліментарність:

Ці фреймворки та стандарти не є конкурентами, а часто використовуються взаємодоповнюючим чином:

- NIST CSF може виступати як загальна рамка управління кіберризиками, використовуючи CIS Controls для впровадження конкретних технічних заходів контролю та посилаючись на вимоги ISO 27001 для побудови формалізованої СУІБ.
- COBIT може надавати високорівневий фреймворк для всього врядування та управління IT, в рамках якого впроваджується кібербезпека з використанням ISO 27001, CIS Controls та NIST CSF.
- ISO 27001 надає вимоги до СУІБ, які можуть бути реалізовані за допомогою контролів з CIS Controls та процесів, визначених у COBIT.
- CIS Controls надають дієві кроки, які можуть допомогти організаціям досягти результатів, описаних у NIST CSF та заходах контролю ISO 27001.

Вибір та комбінація цих підходів залежить від конкретних потреб, ресурсів, профілю ризику та стратегічних цілей організації. Ефективне управління інформаційною безпекою та IT часто вимагає інтеграції елементів з різних фреймворків для створення надійної та адаптивної системи захисту.

1.4. Кращі практики кібербезпеки для малого бізнесу

Малий бізнес є привабливою мішенню для кіберзлочинців, оскільки часто має слабший захист порівняно з великими корпораціями. Втрата даних, переривання

діяльності або фінансові збитки від кібератаки можуть мати руйнівні наслідки для невеликої компанії. Впровадження базових, але ефективних заходів кібербезпеки є життєво необхідним. Розглянемо найкращі практики за трьома ключовими напрямками: Технологічні заходи, Організаційні заходи та Людський фактор.[11]

1. Технологічні заходи

Технологічні заходи є фундаментом кіберзахисту. Вони включають використання відповідного програмного та апаратного забезпечення для запобігання, виявлення та реагування на кіберзагрози. Для малого бізнесу важливо обирати рішення, які є ефективними, але при цьому доступними та відносно простими в управлінні.

Специфіка та Принципи для малого бізнесу:

- Принцип простоти: Обирайте технологічні рішення, які не вимагають глибоких технічних знань для налаштування та підтримки.
- Принцип доступності: Шукайте рентабельні або навіть безплатні рішення, де це можливо, але не жертвуйте базовою безпекою.
- Принцип автоматизації: Використовуйте інструменти, які автоматизують рутинні завдання, такі як оновлення та сканування, щоб зменшити навантаження на персонал.

Детальні Технологічні Заходи:

Антивірусне та Антишкідливе Програмне Забезпечення:

Призначення: Захист від вірусів, програм-вимагачів (ransomware), шпигунського ПЗ та іншого шкідливого програмного забезпечення.

Специфіка для малого бізнесу: Важливо встановити надійний антивірус на всі пристрої, що використовуються для роботи (комп'ютери, ноутбуки, смартфони). Багато постачальників пропонують комплексні пакети безпеки, які включають не тільки антивірус, але й функції захисту від фішингу та шкідливих вебсайтів. Регулярне оновлення антивірусних баз є критично важливим.

Переваги: Базовий рівень захисту від широкого спектра загроз, зменшення ризику зараження пристроїв та втрати даних.

Патч менеджмент та Оновлення Програмного Забезпечення:

Призначення: Усунення уразливостей у програмному забезпеченні, які можуть бути використані зловмисниками.

Специфіка для малого бізнесу: Регулярно оновлюйте операційні системи (Windows, macOS, Linux, мобільні ОС), веббраузери, офісні додатки та інше програмне забезпечення. Увімкніть автоматичні оновлення, де це можливо. Особливу увагу приділяйте оновленню програм, які часто стають мішенню (наприклад, Adobe Reader, Java).[12]

Переваги: Закриття "дірок" у безпеці, які можуть бути експлуатовані, зменшення ризику успішних кібератак, підвищення стабільності роботи ПЗ.

Налаштування та Використання Брандмауера (Firewall):

Призначення: Контроль мережевого трафіку та блокування несанкціонованого доступу до мережі.

Специфіка для малого бізнесу: Переконайтеся, що брандмауер увімкнений на всіх пристроях (вбудований в ОС) та на мережевому обладнанні (роутер). Використовуйте надійні налаштування брандмауера, які обмежують доступ лише до необхідних служб та портів.

Переваги: Захист мережі від зовнішніх загроз, контроль вхідного та вихідного трафіку.

Резервне Копіювання Даних:

Призначення: Можливість відновлення даних у разі їх втрати, пошкодження або шифрування (наприклад, під час атаки програм-вимагачів).

Специфіка для малого бізнесу: Впровадьте регулярне резервне копіювання критично важливих даних. Використовуйте правило "3-2-1": щонайменше 3 копії даних, на 2 різних типах носіїв, з 1 копією поза межами офісу (наприклад, у хмарі або на зовнішньому носії, що зберігається окремо). Перевіряйте можливість відновлення з резервних копій.

Переваги: Зменшення впливу втрати даних, можливість швидкого відновлення після інциденту, забезпечення безперервності бізнес-процесів.[13]

Захист Бездротових Мереж (Wi-Fi):

Призначення: Запобігання несанкціонованому доступу до мережі через Wi-Fi.

Специфіка для малого бізнесу: Використовуйте надійне шифрування (WPA2 або WPA3). Змініть стандартне ім'я мережі (SSID) та встановіть сильний пароль. Створіть окрему мережу для гостей, щоб відокремити їхній трафік від основної бізнес-мережі.

Переваги: Захист мережі від сторонніх, запобігання перехопленню даних.

Багатофакторна Автентифікація (MFA):

Призначення: Додавання додаткового рівня безпеки при вході в облікові записи, вимагаючи більше одного типу перевірки (наприклад, пароль + код з телефону).

Специфіка для малого бізнесу: Увімкніть MFA скрізь, де це можливо, особливо для доступу до важливих систем, хмарних сервісів (електронна пошта, файлові сховища) та адміністративних панелей.

Переваги: Значно ускладнює несанкціонований доступ до облікових записів, навіть якщо пароль скомпрометовано.

Безпечна Конфігурація Пристроїв та Сервісів:

Призначення: Налаштування систем таким чином, щоб зменшити поверхню атаки.

Специфіка для малого бізнесу: Використовуйте надійні, нестандартні паролі для всіх пристроїв та облікових записів. Вимкніть непотрібні служби та функції. Використовуйте мінімальні необхідні дозволи для користувачів та додатків.

2. Організаційні заходи

Технології самі по собі не можуть забезпечити повну безпеку. Організаційні заходи визначають політики, процедури та процеси, які регулюють використання технологій та поведінку співробітників. Для малого бізнесу ці заходи мають бути простими, зрозумілими та реалістичними.[14]

Специфіка та Принципи для малого бізнесу:

Принцип простоти та зрозумілості: Політики мають бути легко зрозумілими для всіх співробітників, без надмірної технічної термінології.

Принцип відповідності бізнес-процесам: Політики та процедури повинні бути інтегровані в повсякденні бізнес-процеси, а не створювати зайві перешкоди.

Принцип документування: Навіть прості політики мають бути задокументовані та доведені до відома співробітників.

Детальні Організаційні Заходи:

Розробка Базових Політик Безпеки:

Призначення: Встановлення правил та очікувань щодо безпечної поведінки та використання ІТ-ресурсів.

Специфіка для малого бізнесу: Розробіть кілька ключових політик, наприклад, політику паролів, політику використання електронної пошти та Інтернету, політику використання особистих пристроїв (BYOD), політику реагування на інциденти. Політики мають бути короткими та чіткими.

Переваги: Встановлення єдиних правил для всіх співробітників, зменшення людського фактора ризику, основа для навчання персоналу.

Планування Реагування на Інциденти (Базовий рівень):

Призначення: Визначення кроків, які необхідно зробити у разі виникнення інциденту кібербезпеки (наприклад, атаки програм-вимагачів, витоку даних).

Специфіка для малого бізнесу: Навіть простий план, що включає контактні дані для звернення по допомогу (наприклад, до ІТ-спеціаліста або компанії з кібербезпеки), кроки для ізоляції заражених систем та порядок інформування відповідних сторін, є кращим, ніж його відсутність.[15]

Переваги: Зменшення часу реакції на інцидент, мінімізація збитків, забезпечення більш організованого відновлення.

Управління Доступом:

Призначення: Надання користувачам лише тих прав доступу до систем та даних, які необхідні для виконання їхніх посадових обов'язків (принцип мінімальних привілеїв).

Специфіка для малого бізнесу: Регулярно переглядайте права доступу співробітників, особливо при зміні їхніх обов'язків або звільненні. Використовуйте унікальні облікові записи для кожного співробітника.

Переваги: Зменшення ризику несанкціонованого доступу до конфіденційних даних, обмеження потенційних збитків у разі компрометації облікового запису.

Фізична Безпека:

Призначення: Захист фізичних активів (комп'ютерів, серверів, документів) від несанкціонованого доступу та крадіжки.

Специфіка для малого бізнесу: Забезпечте фізичний доступ до офісу та приміщень, де зберігається важливе обладнання або документи, обмеженим колом осіб. Використовуйте надійні замки, сигналізацію, можливо, базове відеоспостереження. Не залишайте пристрої без нагляду в публічних місцях.

Переваги: Захист обладнання та даних від фізичних загроз.

Базове Управління Постачальниками (Вендорами):

Призначення: Оцінка та управління ризиками, пов'язаними з третіми сторонами, які мають доступ до даних або систем організації. Специфіка для малого бізнесу: При роботі з постачальниками послуг (наприклад, хмарних сервісів) перевіряйте їхні базові практики безпеки. Укладайте договори, що передбачають відповідальність за безпеку даних.

Переваги: Зменшення ризиків, пов'язаних з ланцюгом постачання.

3. Людський фактор

Співробітники є як першою лінією захисту, так і потенційною найбільшою уразливістю. Навчання та підвищення обізнаності персоналу є критично важливим для ефективної кібербезпеки. Навіть найкращі технології та політики не допоможуть, якщо співробітник стане жертвою фішингової атаки або випадково скомпрометує дані.

Специфіка та Принципи для малого бізнесу:

Принцип регулярності: Навчання має бути не одноразовою подією, а постійним процесом.

Принцип актуальності: Навчання має відображати поточні загрози та методи атак.

Принцип практичності: Надавайте співробітникам конкретні приклади та інструкції, які вони можуть застосовувати в повсякденній роботі.

Принцип позитивної культури: Заохочуйте співробітників повідомляти про підозрілу активність без страху покарання.

Детальні Заходи, пов'язані з Людським фактором:

Навчання та Підвищення Обізнаності з Кібербезпеки:

Призначення: Надання співробітникам знань та навичок, необхідних для розпізнавання та уникнення загроз.

Специфіка для малого бізнесу: Проводьте регулярні короткі тренінги або інформаційні сесії. Зосередьтеся на найпоширеніших загрозах:

Фішинг та соціальна інженерія: Як розпізнавати підозрілі електронні листи, повідомлення та телефонні дзвінки. Поясніть, чому не можна переходити за підозрілими посиланнями або відкривати вкладення від невідомих відправників.

Важливість сильних та унікальних паролів: Навчіть створювати та безпечно зберігати надійні паролі. Поясніть ризики використання одного пароля для багатьох сервісів.

Безпечне використання Інтернету та електронної пошти: Поясніть ризики відвідування небезпечних вебсайтів та завантаження файлів з неперевірених джерел. Навчіть обережності при надсиланні конфіденційної інформації електронною поштою.[16]

Безпечне використання мобільних пристроїв: Поясніть ризики публічних Wi-Fi мереж та важливість захисту пристроїв паролями або біометричними даними.

Переваги: Зменшення ймовірності успішних атак, спричинених людськими помилками, підвищення загальної культури безпеки в організації.

Стимулювання Культури Безпеки:

Призначення: Створення середовища, в якому співробітники усвідомлюють важливість безпеки та активно долучаються до її забезпечення.

Специфіка для малого бізнесу: Регулярно нагадуйте про правила безпеки. Заохочуйте співробітників ставити запитання та повідомляти про будь-які підозрілі ситуації без страху. Керівництво має демонструвати приклад безпечної поведінки.

Переваги: Проактивний підхід до безпеки, раннє виявлення потенційних загроз.

Призначення: Встановлення правил щодо того, як співробітники повинні обробляти, зберігати та передавати конфіденційні дані клієнтів, партнерів та власні дані компанії.

Специфіка для малого бізнесу: Чітко визначте, яка інформація вважається конфіденційною. Надайте інструкції щодо її безпечного зберігання (наприклад, шифрування файлів, використання захищених папок) та передачі (наприклад, використання зашифрованих каналів зв'язку).

Переваги: Зменшення ризику витоку даних, захист репутації компанії, забезпечення відповідності вимогам законодавства щодо захисту даних.

Впровадження цих найкращих практик, навіть на базовому рівні, може значно підвищити рівень кібербезпеки малого бізнесу та зменшити його вразливість до широкого спектра кіберзагроз. Важливо пам'ятати, що кібербезпека – це не одноразова дія, а постійний процес, який потребує регулярного перегляду та адаптації до нових викликів.[17]

Висновок до розділу 1

Підсумовуючи основні ідеї розділів можна виокремити кілька ключових спостережень.

По-перше, чітке розуміння відмінності між інформаційною безпекою та кібербезпекою, а також усвідомлення трьох базових принципів (конфіденційність, цілісність, доступність) і специфіки малого бізнесу дають нам теоретичну основу для побудови захисту.

По-друге, аналіз загроз — від фішингу та соціальної інженерії до ransomware, DDoS-атак і інсайдерських ризиків — показує, що саме людський фактор і недостатня технологічна готовність найчастіше призводять до інцидентів, а реальні кейси підтверджують критичність цих вразливостей.

По-третє, огляд міжнародних стандартів і фреймворків (ISO/IEC 27001, COBIT, CIS Controls та NIST CSF 2.0) дозволяє побачити спектр підходів: від комплексних систем управління до пріоритетних «швидких перемог», які особливо корисні для МСП. А адаптація профілів у NIST CSF 2.0 допомагає гнучко підлаштовувати стандарт під реальні можливості й потреби.

Нарешті, викладені найкращі практики — технологічні заходи (антивірус, оновлення, резервне копіювання, MFA), організаційні політики та процеси (парольна дисципліна, інцидент-респонс, контроль прав доступу) і систематичне навчання співробітників — становлять практичний «чек-лист», який кожне мале підприємство може запровадити без великих інвестицій.

Таким чином, інтегрувавши теоретичні концепти, аналіз загроз, міжнародні рекомендації та прикладні кроки, ми створили єдину логічний ланцюжок: від розуміння проблем до конкретних рішень. У наступних розділах роботи ці рекомендації будуть застосовані до моделювання цільового профілю безпеки для уявного малого підприємства, що дозволить перевірити їхню ефективність на практиці.

РОЗДІЛ 2
АНАЛІЗ ТА ПОРІВНЯННЯ МЕТОДІВ ВПРОВАДЖЕННЯ СТРАТЕГІЙ

2.1. Мета порівняльного аналізу

Попередній розділ надав детальний огляд чотирьох впливових міжнародних стандартів та підходів: ISO/IEC 27001, COBIT, CIS Controls та NIST Cybersecurity Framework 2.0, розкривши їхню специфіку, принципи та структуру. Розуміння сутності кожного з них є першим кроком до вибору та впровадження ефективної стратегії кібербезпеки та управління IT в організації.

Однак, простого знання про існування цих фреймворків недостатньо. Для прийняття обґрунтованого рішення щодо того, який підхід найкраще відповідає потребам конкретної організації, необхідно провести порівняльний аналіз методів їх впровадження. Метою цього розділу є саме такий аналіз, який допоможе оцінити сильні та слабкі сторони кожного фреймворку з практичної точки зору.

Порівняльний аналіз методів впровадження дозволить виявити, як кожен з підходів допомагає досягти цілей кібербезпеки та управління IT, які ресурси необхідні для їх реалізації, наскільки складним є процес імплементації, а також наскільки вони адаптовані для організацій різного масштабу, зокрема для малого та середнього бізнесу (МСП). Фокус на методах впровадження дозволить перейти від теоретичного розуміння "що це таке" до практичного "як це реалізувати" та "що це буде коштувати".[18]

Далі ми визначимо ключові критерії, за якими буде проводитися це порівняння, щоб забезпечити системний та об'єктивний підхід до оцінки кожного з фреймворків.

2.2. Опис критеріїв порівняння

Для проведення ефективного та релевантного порівняльного аналізу методів впровадження стратегій кібербезпеки та управління IT на основі ISO/IEC 27001,

COBIT, CIS Controls та NIST Cybersecurity Framework 2.0, визначимо наступні ключові критерії:

1. Охоплення функцій CSF (Govern, Identify, Protect, Detect, Respond, Recover): Цей критерій оцінює, наскільки повно кожен із розглянутих фреймворків охоплює шість ключових функцій управління кіберризиками, визначених у NIST Cybersecurity Framework 2.0. Оскільки NIST CSF є широко визнаним фреймворком для управління кіберризиками, використання його функцій як осі порівняння дозволить оцінити комплексність та широту застосування кожного з підходів у контексті життєвого циклу кібербезпеки. Буде розглянуто, наскільки детально та системно кожен фреймворк надає настанови та заходи для реалізації активностей у кожній з цих функцій: від визначення стратегії та врядування (Govern) до ідентифікації ризиків (Identify), впровадження захисних заходів (Protect), виявлення інцидентів (Detect), реагування на них (Respond) та відновлення після атак (Recover).

2. Вартість і ресурсомісткість: Цей критерій оцінює фінансові витрати та обсяг ресурсів (людських, часових, технічних), необхідних для впровадження та підтримки кожного фреймворку. Враховуватимуться витрати на придбання документації стандартів (якщо вони не є безкоштовними), оплату консультаційних послуг, навчання персоналу, придбання або оновлення технічних засобів захисту, а також витрати на проходження аудиту та отримання сертифікації (якщо це передбачено фреймворком і є бажаним). Для малого та середнього бізнесу цей критерій є одним з найважливіших при виборі підходу.[19]

3. Складність впровадження: Цей критерій оцінює рівень технічної та організаційної складності процесу впровадження фреймворку. Враховуватиметься необхідність глибоких технічних знань, обсяг необхідної документації, складність процесів управління, вимоги до зміни організаційної структури або культури. Фреймворки, що вимагають значних змін у внутрішніх процесах або мають складну ієрархічну структуру, можуть бути складнішими для впровадження, особливо для організацій без попереднього досвіду у сфері формалізованого управління безпекою чи IT.

4. Масштабованість для МСП: Цей критерій оцінює, наскільки легко та ефективно кожен фреймворк може бути адаптований та впроваджений в організаціях малого та середнього бізнесу, які, як правило, мають обмежені ресурси та менш складні IT-інфраструктури порівняно з великими підприємствами. Буде розглянуто, чи передбачає фреймворк гнучкість у виборі заходів контролю або рівнів впровадження, чи існують спеціальні настанови або спрощені версії для МСП, а також наскільки початкові витрати та складність є бар'єром для входу для невеликих компаній. Фреймворки, що пропонують поетапне впровадження або можливість фокусуватися на базових заходах, можуть бути більш привабливими для МСП.

Давайте детальніше розглянемо перший критерій порівняння: Охоплення функцій CSF (Govern, Identify, Protect, Detect, Respond, Recover).

Цей критерій є важливим, оскільки функції NIST Cybersecurity Framework 2.0 надають визнану на міжнародному рівні таксономію високорівневих результатів управління кіберризиками. Оцінка того, наскільки повно кожен із фреймворків (ISO/IEC 27001, COBIT, CIS Controls) охоплює ці функції, дозволяє зрозуміти їхню сферу застосування та комплексність з погляду повного життєвого циклу кібербезпеки.[20]

Розглянемо коротко кожну з шести функцій NIST CSF 2.0:

1. Govern (Управління): Ця функція є новою у CSF 2.0 і підкреслює важливість інтеграції кіберризик менеджменту в загальну стратегію, політику та процеси прийняття рішень організації. Вона охоплює встановлення політик, ролей та відповідальності, управління ризиками на всіх рівнях, забезпечення відповідності вимогам, а також моніторинг та комунікацію щодо стану кібербезпеки. Це функція високого рівня, яка задає тон та напрямок для всіх інших функцій.

2. Identify (Ідентифікація): Ця функція стосується розробки розуміння організацією її поточного стану кіберризиків. Це включає ідентифікацію та управління активами (фізичними, програмними, інформаційними), визначення бізнес-середовища та залежностей, проведення оцінки ризиків, розробку стратегії управління ризиками та розуміння ролей і відповідальності. Мета – створити основу для прийняття обґрунтованих рішень щодо управління ризиками.

3. Protect (Захист): Ця функція охоплює впровадження відповідних заходів безпеки для забезпечення надання критично важливих послуг та захисту активів. Вона включає управління ідентифікацією та доступом, навчання та обізнаність, безпеку даних, захисні технології, процеси та процедури захисту, а також підтримку безпеки платформ та інфраструктури.

4. Detect (Виявлення): Ця функція зосереджена на своєчасному виявленні подій кібербезпеки. Вона включає моніторинг аномалій та подій, впровадження процесів виявлення та регулярне тестування захисних механізмів.

5. Respond (Реагування): Ця функція стосується вжиття заходів щодо виявленої події кібербезпеки. Вона охоплює планування реагування на інциденти, управління комунікаціями, аналіз інцидентів, дії з пом'якшення їх наслідків та постійне покращення процесів реагування.

6. Recover (Відновлення): Ця функція зосереджена на забезпеченні стійкості та відновленні порушених можливостей або послуг після інциденту кібербезпеки. Вона включає планування відновлення, впровадження дій з відновлення, управління комунікаціями під час відновлення та аналіз уроків для майбутнього покращення.

Тепер оцінимо, як кожен із розглянутих фреймворків охоплює ці функції:

ISO/IEC 27001:2022:

Govern: ISO 27001 повною мірою охоплює аспекти врядування через вимоги до Контексту організації (Розділ 4), Лідерства (Розділ 5) та Планування (Розділ 6) [21]. Стандарт вимагає від вищого керівництва встановлення політики безпеки, визначення ролей та відповідальності, а також інтеграції вимог безпеки в бізнес-процеси. Процес управління ризиками, який є центральним в ISO 27001, також тісно пов'язаний з функцією Govern.

Identify: Функція Identify добре охоплена в ISO 27001 через вимоги до Контексту організації (Розділ 4), зокрема розуміння потреб та очікувань зацікавлених сторін, а також через ключовий процес Оцінки ризиків інформаційної безпеки (Розділ 8.2). Цей процес включає ідентифікацію активів, загроз, уразливостей та оцінку потенційних наслідків.

Protect: Функція Protect є однією з найсильніших сторін ISO 27001, особливо через Додаток А, який надає широкий перелік заходів контролю. Ці заходи охоплюють контроль доступу, криптографію, фізичну безпеку, безпеку операцій, безпеку комунікацій тощо. Вимоги до впровадження обраних контролів містяться в Розділі 8 (Функціонування).

Detect: Аспекти виявлення інцидентів безпеки присутні в ISO 27001, зокрема через вимоги до Моніторингу, вимірювання, аналізу та оцінки (Розділ 9.1) та управління подіями інформаційної безпеки в Додатку А (А.16). Однак, порівняно з фреймворками, які мають сильний фокус на моніторингу та виявленні в реальному часі (як NIST CSF та CIS Controls), деталізація може бути меншою.

Respond: Управління інцидентами інформаційної безпеки включено до ISO 27001 в Додатку А (А.16) та опосередковано через вимоги до Невідповідностей та коригувальних дій (Розділ 10.1). Стандарт вимагає наявності процесів для реагування на інциденти, але рівень деталізації може бути меншим, ніж у спеціалізованих фреймворках з реагування на інциденти.

Recover: Аспекти управління безперервністю бізнесу та відновлення після інцидентів також присутні в ISO 27001 в Додатку А (А.17). Це включає вимоги до планування безперервності бізнесу, резервного копіювання та відновлення.[22]

COBIT 2019:

Govern: COBIT має дуже сильний фокус на врядуванні. Функція Govern CSF повністю відповідає принципам та цілям врядування в COBIT, зокрема Принципу 4 (Чітке розмежування врядування та управління) та Цілям врядування (наприклад, EDM01-EDM05), які стосуються оцінки, визначення напрямку та моніторингу.

Identify: Аспекти ідентифікації ризиків та управління активами включені до COBIT в рамках цілей управління, пов'язаних з управлінням ризиками (наприклад, APO12 Managed Risk) та управлінням активами (наприклад, BAI09 Managed Assets). COBIT надає фреймворк для інтеграції цих процесів в загальну систему управління IT.

Protect: Захисні заходи охоплені в COBIT в рамках різних цілей управління, зокрема тих, що стосуються управління безпекою (наприклад, DSS05 Managed

Security Services), управління ідентифікацією та доступом (наприклад, DSS05.01 Managed Identity and Access) та інших. COBIT надає високорівневі цілі, але не детальні технічні контролі, як CIS Controls.

Detect: Виявлення подій безпеки включено до COBIT в рамках управління безпекою (наприклад, DSS05 Managed Security Services) та моніторингу (наприклад, DSS05.02 Managed Detection of Security Events). COBIT визначає необхідність таких процесів, але не надає конкретних технічних методів виявлення.

Respond: Реагування на інциденти включено до COBIT в рамках управління безпекою (наприклад, DSS05 Managed Security Services) та управління інцидентами (наприклад, DSS02 Managed Service Requests and Incidents). COBIT надає настанови щодо процесу управління інцидентами, але не детальні процедури реагування.

Recover: Відновлення та забезпечення безперервності включені до COBIT в рамках управління безперервністю (наприклад, BAI04 Managed Availability and Capacity, DSS04 Managed Continuity). COBIT надає цілі та компоненти для побудови процесів відновлення та безперервності.[23]

CIS Controls v8:

Govern: CIS Controls не мають окремої функції або розділу, присвяченого врядуванню на такому ж високому рівні, як NIST CSF або COBIT. Їхній фокус – на конкретних діях. Однак, впровадження CIS Controls вимагає певного рівня врядування та прийняття рішень (наприклад, вибір Групи Впровадження). Деякі контролі (наприклад, Control 15: Service Provider Management) опосередковано стосуються аспектів врядування.

Identify: Аспекти ідентифікації добре представлені в CIS Controls, зокрема через Control 1 (Inventory and Control of Enterprise Assets) та Control 2 (Inventory and Control of Software Assets), які є фундаментальними для розуміння активів. Також Control 7 (Continuous Vulnerability Management) стосується ідентифікації уразливостей. Однак, повна оцінка ризиків як процесу в цілому менш виражена, ніж в ISO 27001 або NIST CSF.

Protect: Функція Protect є центральною для CIS Controls. Більшість контролів (наприклад, Controls 3, 4, 5, 6, 9, 10, 11, 12, 13, 14, 16) надають конкретні, дієві заходи

для захисту активів та систем. Це сильна сторона CIS Controls – вони надають практичні кроки для реалізації захисту.

Detect: CIS Controls включають заходи, спрямовані на виявлення, зокрема Control 8 (Audit Log Management) та Control 13 (Network Monitoring and Analysis). Ці контролі надають конкретні рекомендації щодо збору, зберігання та аналізу логів, а також моніторингу мережевої активності для виявлення підозрілої поведінки.

Respond: Управління реагуванням на інциденти включено до CIS Controls в рамках Control 17 (Incident Response Management). Цей контроль надає настанови щодо розробки плану реагування на інциденти, формування команди реагування та проведення відповідних заходів.

Recover: CIS Controls включають аспекти відновлення в рамках Control 10 (Data Recovery Management). Цей контроль зосереджений на важливості резервного копіювання та планування відновлення даних для забезпечення можливості повернення до нормальної діяльності після інциденту.[24]

NIST Cybersecurity Framework 2.0:

Govern: Функція Govern є однією з шести основних функцій NIST CSF 2.0, що прямо вказує на її важливість та повне охоплення в рамках фреймворку. CSF надає детальні підкатегорії та інформативні посилання для реалізації ефективного врядування кіберризиками.

Identify: Функція Identify також є однією з шести основних функцій CSF 2.0 і повністю охоплена фреймворком. Він надає структурований підхід з категоріями та підкатегоріями для ідентифікації активів, бізнес-середовища, ризиків тощо.

Protect: Функція Protect є центральною для багатьох заходів безпеки й повністю охоплена в CSF 2.0. Фреймворк надає категорії та підкатегорії, що стосуються контролю доступу, захисту даних, навчання, технічної безпеки тощо, з посиланнями на інші стандарти для деталізації.

Detect: Функція Detect є однією з шести основних функцій CSF 2.0 і повною мірою включена до фреймворку. Вона охоплює моніторинг, процеси виявлення та тестування.

Respond: Функція Respond є однією з шести основних функцій CSF 2.0 і повністю охоплена в рамках фреймворку. Вона надає структуру для планування та виконання дій з реагування на інциденти.

Recover: Функція Recover є однією з шести основних функцій CSF 2.0 і повною мірою включена до фреймворку. Вона охоплює планування та реалізацію заходів з відновлення після інцидентів.

Висновок за критерієм "Охоплення функцій CSF":

NIST CSF 2.0 за визначенням охоплює всі шість функцій управління кіберризиками, оскільки вони є його структурними елементами.

ISO/IEC 27001 добре охоплює функції Govern, Identify, Protect, Respond та Recover через вимоги до СУІБ та заходи контролю в Додатку А. Функція Detect також присутня, але може бути менш деталізованою в плані технічного виявлення в реальному часі порівняно з NIST CSF та CIS Controls.

COBIT 2019 надає високорівневий фреймворк, який охоплює всі шість функцій CSF в рамках своїх цілей врядування та управління. Він сильний у функції Govern та інтеграції кібербезпеки в загальне управління IT, але менш деталізований у конкретних технічних заходах порівняно з CIS Controls або навіть ISO 27001 (через Додаток А).

CIS Controls v8 дуже сильний у функціях Identify, Protect, Detect, Respond та Recover, надаючи конкретні та дієві заходи. Функція Govern охоплена опосередковано через необхідність прийняття рішень щодо впровадження контролів, але не є центральним елементом фреймворку на рівні стратегічного врядування.

Таким чином, за критерієм охоплення функцій CSF, NIST CSF 2.0 є найбільш повним за визначенням. ISO 27001 та COBIT охоплюють всі функції на різних рівнях деталізації (ISO 27001 більше технічних заходів, COBIT більше врядування), тоді як CIS Controls сильні в операційних функціях (Identify, Protect, Detect, Respond, Recover), але менш сфокусовані на високорівневому врядуванні.

Давайте розглянемо другий критерій порівняння: Вартість і ресурсомісткість.

Цей критерій є критично важливим для будь-якої організації при виборі та впровадженні стратегії кібербезпеки чи управління IT, і особливо актуальним для

малого та середнього бізнесу (МСП) з їхніми часто обмеженими бюджетами та штатом. Вартість і ресурсомісткість охоплюють не лише прямі фінансові витрати, але й обсяг людських зусиль, часу та технічних ресурсів, необхідних для успішної імплементації та подальшої підтримки обраного підходу.

Складові вартості та ресурсомісткості:

При оцінці вартості та ресурсомісткості впровадження фреймворку або стандарту зазвичай враховують наступне:

Вартість документації: Деякі фреймворки є безплатний для завантаження та використання (наприклад, NIST CSF, CIS Controls), тоді як інші (наприклад, ISO/IEC 27001, COBIT) вимагають придбання офіційних документів.

Консультаційні послуги: Багато організацій залучають зовнішніх консультантів для допомоги у розумінні, адаптації та впровадженні складних фреймворків, що може становити значну частину загальної вартості.

Навчання персоналу: Необхідно інвестувати в навчання співробітників, які відповідатимуть за впровадження та підтримку фреймворку, а також в підвищення загальної обізнаності персоналу.

Технічні засоби: Впровадження вимог фреймворку може потребувати придбання нового програмного забезпечення (наприклад, для моніторингу, управління уразливостями), апаратного забезпечення (наприклад, брандмауерів) або оновлення існуючої інфраструктури.

Час персоналу: Найбільш значним ресурсом часто є час внутрішнього персоналу, який буде залучений до процесу впровадження – від IT-фахівців до менеджерів та керівництва.

Аудит та сертифікація (для ISO 27001): Проходження сертифікаційного аудиту за ISO 27001 та отримання сертифіката є додатковою, часто суттєвою статтею витрат, яка включає як оплату послуг аудиторів, так і зусилля на підготовку до аудиту.

Постійна підтримка та аудит: Після впровадження фреймворк потребує постійної підтримки, моніторингу та регулярних внутрішніх та, можливо, зовнішніх аудитів, що також пов'язано з витратами та ресурсами.

Оцінимо тепер вартість та ресурсомісткість для кожного з розглянутих підходів:

ISO/IEC 27001:2022:

Вартість документації: Офіційні стандарти ISO/IEC 27001 та ISO/IEC 27002 є платними.

Консультаційні послуги: Часто потрібні, особливо для організацій без досвіду впровадження систем управління. Вартість послуг консультантів може бути значною.

Навчання персоналу: Вимагає навчання співробітників, відповідальних за СУІБ, внутрішніх аудиторів, а також загального навчання персоналу з інформаційної безпеки.

Технічні засоби: Може потребувати інвестицій у технічні засоби для реалізації заходів контролю (наприклад, SIEM-системи, системи управління ідентифікацією).

Час персоналу: Впровадження СУІБ за ISO 27001 є ресурсомістким процесом, що вимагає значного часу від IT-відділу, відділу безпеки та інших підрозділів.

Аудит та сертифікація: Сертифікація за ISO 27001 є добровільною, але якщо організація прагне її отримати, це додає суттєві витрати на зовнішні аудити (первинний, наглядові) та підготовку до них.

Постійна підтримка: Підтримка СУІБ вимагає регулярних зусиль для моніторингу, внутрішніх аудитів, аналізу з боку керівництва та постійного поліпшення.

Загалом: Впровадження ISO/IEC 27001, особливо з метою сертифікації, є одним з найбільш ресурсовартісних підходів серед розглянутих, особливо для МСП.

COBIT 2019:

Вартість документації: Основні публікації COBIT 2019 (фреймворк, настанови з дизайну та впровадження) є платними.

Консультаційні послуги: Залучення консультантів є поширеною практикою, особливо для адаптації фреймворку до специфічних потреб організації та побудови системи врядування. Це може бути значною статтею витрат.

Навчання персоналу: Вимагає навчання персоналу з управління IT, аудиторів та інших зацікавлених сторін щодо принципів та використання COBIT.

Технічні засоби: COBIT є фреймворком врядування, тому він сам по собі не вимагає специфічних технічних засобів, але його впровадження може виявити необхідність інвестицій у технології для підтримки процесів управління.

Час персоналу: Впровадження COBIT, особливо в повному обсязі, є ресурсомістким процесом, що вимагає значного часу від менеджменту, IT-персоналу та інших підрозділів, залучених до процесів врядування та управління.

Аудит та сертифікація: COBIT не передбачає офіційної сертифікації організації на відповідність фреймворку, але його можна використовувати як основу для внутрішніх або зовнішніх аудитів процесів управління IT.

Постійна підтримка: Підтримка системи врядування на основі COBIT вимагає постійного моніторингу процесів, оцінки результативності та адаптації.

Загалом: Повне впровадження COBIT може бути дуже ресурсовартісне рішення, порівнянним з ISO 27001, але його масштаби залежать від обсягу застосування фреймворку. Для МСП може бути доцільним застосування окремих частин або принципів COBIT.

CIS Controls v8:

Вартість документації: CIS Controls та супутні матеріали (посібники з впровадження) є безплатним.

Консультаційні послуги: Можуть знадобитися для допомоги в оцінці поточного стану, виборі Групи Впровадження та технічній реалізації контролів, але часто в меншому обсязі, ніж для ISO 27001 або COBIT.

Навчання персоналу: Потребує навчання IT-персоналу та команд безпеки щодо конкретних технічних заходів, а також підвищення обізнаності всіх співробітників.

Технічні засоби: Впровадження CIS Controls часто вимагає інвестицій у конкретні технічні засоби (наприклад, системи управління уразливостями, інструменти моніторингу логів, рішення для багатофакторної автентифікації). Вартість цих засобів може варіюватися.

Час персоналу: Впровадження потребує значного часу від технічного персоналу та команд безпеки для налаштування та конфігурації систем відповідно до Safeguards.

Аудит та сертифікація: CIS Controls не передбачають офіційної сертифікації, але існують методики оцінки відповідності та атестації.

Постійна підтримка: Підтримка відповідності CIS Controls вимагає постійного моніторингу, управління уразливостями та актуалізації заходів відповідно до змін у середовищі та загрозах.

Загалом: CIS Controls можуть бути менш вартісними та ресурсоємними для початкового впровадження базових рівнів (особливо IG1) порівняно з повним впровадженням ISO 27001 або COBIT, оскільки вони більш сфокусовані на конкретних діях. Однак, реалізація всіх контролів для вищих груп впровадження може потребувати значних інвестицій у технічні засоби та ресурси персоналу.

NIST Cybersecurity Framework 2.0:

Вартість документації: NIST CSF 2.0 та супутні матеріали є безкоштовними.

Консультаційні послуги: Можуть бути корисними для допомоги у розумінні фреймворку, розробці профілів та проведенні оцінки розривів, але не є обов'язковими. Гнучкість фреймворку дозволяє організаціям використовувати його самостійно.

Навчання персоналу: Потребує навчання персоналу, відповідального за управління ризиками та кібербезпеку, щодо структури та використання фреймворку.

Технічні засоби: NIST CSF не вимагає специфічних технічних засобів. Його впровадження полягає у використанні фреймворку для управління ризиками та оцінки поточного стану, що може виявити необхідність інвестицій у технічні засоби (які вже можуть бути передбачені іншими фреймворками, на які посилається NIST CSF). Час персоналу: Початкова оцінка поточного стану та розробка профілів вимагає часу від відповідного персоналу. Подальші зусилля залежать від плану дій, розробленого на основі аналізу розривів. Аудит та сертифікація: NIST CSF не передбачає офіційної сертифікації, але може використовуватися як основа для внутрішніх або зовнішніх оцінок стану кібербезпеки.

Постійна підтримка: Підтримка впровадження NIST CSF полягає в регулярному перегляді профілів, проведенні оцінки ризиків та моніторингу виконання плану дій.

Загалом: NIST CSF 2.0, ймовірно, є одним з найменш вартісним та ресурсомістким для початкового впровадження як фреймворку для управління

ризиками та оцінки. Його гнучкість дозволяє організаціям самостійно визначати обсяг використання та інтеграції з іншими підходами. Фактичні витрати та ресурси будуть залежати від масштабу проблем, виявлених за допомогою CSF, та інвестицій, необхідних для їх вирішення.

Висновки за критерієм "Вартість і ресурсомісткість":

Найбільш вартісним та ресурсомісткий (потенційно): ISO/IEC 27001 (особливо з сертифікацією) та повне впровадження COBIT. Вони вимагають значних інвестицій у процеси, документацію, навчання та, можливо, консультантів.

Помірна вартість та ресурсомісткість: CIS Controls. Хоча сам фреймворк безкоштовний, реалізація технічних заходів контролю може потребувати суттєвих інвестицій у технології та час технічного персоналу, особливо для вищих рівнів впровадження.

Найменш вартісним та ресурсоємним є (для початкового впровадження): NIST Cybersecurity Framework 2.0. Фреймворк безкоштовний, зосереджений на управлінні ризиками та оцінці, що не вимагає значних початкових інвестицій у нові системи чи процеси, якщо вони вже існують. Витрати виникають при реалізації плану дій, визначеного за допомогою фреймворку.

Давайте розглянемо третій критерій порівняння: Складність впровадження.

Цей критерій оцінює, наскільки технічно та організаційно складним є процес переходу від початкового стану до стану, коли фреймворк або стандарт ефективно функціонує в організації. Складність впровадження залежить від багатьох факторів, включаючи обсяг необхідних змін у процесах, структурах та технологіях, обсяг необхідної документації, рівень необхідної технічної експертизи та легкість розуміння та адаптації принципів фреймворку персоналом організації. Для організацій з обмеженими ресурсами або низьким рівнем зрілості у сфері кібербезпеки та управління IT, складність впровадження може бути значним бар'єром.

Ключові аспекти, що впливають на складність впровадження:

Обсяг необхідних змін: Наскільки сильно впровадження фреймворку вимагає зміни існуючих бізнес-процесів, організаційної структури або IT-інфраструктури.

Документаційні вимоги: Кількість та складність політик, процедур, настанов та записів, які необхідно створити та підтримувати.

Технічна експертиза: Рівень спеціалізованих знань, необхідних для розуміння фреймворку та технічної реалізації його вимог.

Організаційна культура та управління змінами: Необхідність зміни поведінки персоналу та подолання опору змінам.

Гнучкість фреймворку: Наскільки легко фреймворк може бути адаптований до специфічних потреб та масштабу організації.

Вимоги до інтеграції: Необхідність інтеграції з іншими існуючими системами управління або процесами.

Оцінимо тепер складність впровадження для кожного з розглянутих підходів:

ISO/IEC 27001:2022:

Обсяг необхідних змін: Впровадження СУІБ за ISO 27001 часто вимагає значних змін у підходах до управління інформаційною безпекою, формалізації процесів, визначення ролей та відповідальності. Це системний підхід, який впливає на всю організацію.

Документаційні вимоги: ISO 27001 є стандартом, що вимагає значного обсягу документованої інформації, включаючи політику безпеки, процедури управління ризиками, Заяву про застосовність (SoA), плани дій, записи про діяльність СУІБ тощо. Це може бути складним завданням.

Технічна експертиза: Вимагає розуміння принципів управління інформаційною безпекою, процесу управління ризиками та вміння адаптувати заходи контролю з додатком А до контексту організації. Також потрібна технічна експертиза для реалізації обраних заходів контролю.

Організаційна культура та управління змінами: Впровадження СУІБ потребує сильної підтримки керівництва та залучення персоналу на всіх рівнях, що може вимагати значних зусиль з управління змінами.

Гнучкість фреймворку: Хоча ISO 27001 є гнучким у виборі конкретних заходів контролю на основі ризиків, сама структура СУІБ та вимоги до документування є досить жорсткими.

Вимоги до інтеграції: Потребує інтеграції СУІБ з іншими системами управління організації (наприклад, управління якістю, управління послугами).

Загалом: Впровадження ISO/IEC 27001 вважається відносно складним, особливо для організацій, які не мають досвіду у впровадженні систем управління. Значні вимоги до документування та необхідність глибоких змін у процесах можуть бути викликом.

COBIT 2019:

Обсяг необхідних змін: Повне впровадження COBIT може вимагати значних змін у процесах врядування та управління IT по всій організації, включаючи визначення ролей, відповідальності, процесів прийняття рішень та метрик.

Документаційні вимоги: COBIT надає моделі процесів та компонентів, які потребують документування, але обсяг документації залежить від глибини впровадження. Це може бути значним, але менш формалізованим, ніж в ISO 27001.

Технічна експертиза: Вимагає розуміння принципів врядування та управління IT, а також здатності адаптувати фреймворк до специфічного контексту організації. Менш сфокусований на глибокій технічній реалізації порівняно з CIS Controls.

Організаційна культура та управління змінами: Впровадження COBIT часто пов'язане зі змінами у взаємодії між бізнес-підрозділами та IT, що вимагає ефективного управління змінами та залучення керівництва.

Гнучкість фреймворку: COBIT є гнучким у плані адаптації за допомогою факторів дизайну, але його комплексність може зробити процес адаптації складним.

Вимоги до інтеграції: Розроблений для інтеграції з іншими фреймворками та стандартами (включаючи ISO 27001 та NIST CSF), що може як спростити (за наявності досвіду), так і ускладнити (за відсутності) процес.

Загалом: Впровадження COBIT може бути складним через його широкий обсяг та фокус на врядуванні та управлінні на корпоративному рівні. Необхідність узгодження IT з бізнес-цілями та інтеграції різних процесів може вимагати значних зусиль.

CIS Controls v8:

Обсяг необхідних змін: Впровадження CIS Controls зосереджено на конкретних технічних та організаційних діях. Обсяг змін залежить від поточного рівня безпеки організації та обраної Групи Впровадження. Для IG1 зміни можуть бути відносно невеликими для деяких організацій.

Документаційні вимоги: Потребує документування реалізованих Safeguards, але обсяг документації значно менший, ніж в ISO 27001 або COBIT. Основний фокус – на діях, а не на формальних процедурах управління.

Технічна експертиза: Вимагає значної технічної експертизи для правильного розуміння та реалізації багатьох Safeguards, які стосуються конфігурації систем, моніторингу, управління уразливостями тощо.

Організаційна культура та управління змінами: Менш виражені вимоги до зміни організаційної культури порівняно з системними фреймворками, але потребує дисципліни для постійного виконання технічних завдань та певного рівня обізнаності персоналу.

Гнучкість фреймворку: CIS Controls є відносно гнучкими завдяки Групам Впровадження, які дозволяють організаціям починати з базових заходів та поступово рухатися до більш складних.

Вимоги до інтеграції: Можуть бути інтегровані з іншими фреймворками як набір конкретних заходів контролю.

Загалом: CIS Controls можуть бути менш складними для початку впровадження (особливо IG1) завдяки їхній дієвості та меншим документаційним вимогам. Однак, реалізація всіх контролів для вищих груп впровадження може бути технічно складною та вимагати значних зусиль від технічного персоналу.

NIST Cybersecurity Framework 2.0:

Обсяг необхідних змін: NIST CSF є гнучким фреймворком, який використовує існуючі процеси та контролі організації. Впровадження полягає, перш за все, у використанні його для оцінки поточного стану, визначення цільового стану та планування дій. Обсяг необхідних змін залежить від виявлених "розривів" між поточним та цільовим профілями.

Документаційні вимоги: Фреймворк сам по собі не вимагає значного обсягу нової документації, але результати оцінки, профілі та плани дій мають бути задокументовані. Він заохочує використання існуючої документації інших стандартів.

Технічна експертиза: Вимагає розуміння принципів управління ризиками кібербезпеки та здатності застосовувати фреймворк для оцінки та планування. Не вимагає глибокої технічної експертизи для самого фреймворку, але імплементація заходів, визначених за допомогою CSF, потребує відповідних технічних знань.

Організаційна культура та управління змінами: Потребує залучення різних підрозділів для розробки профілів та оцінки ризиків, що може вимагати певних зусиль з координації та комунікації.

Гнучкість фреймворку: NIST CSF є дуже гнучким та адаптивним, що є його сильною стороною, але може вимагати від організації більшої самостійності у прийнятті рішень щодо його застосування.

Вимоги до інтеграції: Розроблений для інтеграції з іншими стандартами та фреймворками (ISO 27001, CIS Controls, COBIT та іншими) через інформативні посилання.

Загалом: NIST Cybersecurity Framework 2.0 вважається відносно менш складним для початкового впровадження як інструменту оцінки та планування завдяки його гнучкості, відсутності жорстких вимог до документування та можливості використання існуючих практик. Складність зростає при реалізації комплексного плану дій, визначеного за допомогою фреймворку.

Висновки за критерієм "Складність впровадження":

Найбільш складні: ISO/IEC 27001 (через системний характер та вимоги до документування) та COBIT (через широкий обсяг та фокус на врядуванні корпоративними IT).

Помірно складні: CIS Controls (технічна складність реалізації багатьох контролів) та NIST Cybersecurity Framework 2.0 (складність у використанні як комплексного інструменту управління ризиками, хоча початкова імплементація може бути простішою).

Відносно прості для початку: CIS Controls (особливо IG1) та NIST Cybersecurity Framework 2.0 (для базової оцінки та профілювання).

Вибір фреймворку з урахуванням складності впровадження має базуватися на поточній зрілості організації, її ресурсах та наявності необхідної експертизи. Для організацій, які тільки починають свій шлях у формалізованій кібербезпеці, простіші для впровадження підходи можуть бути більш доцільними.

Давайте розглянемо четвертий критерій порівняння: Масштабованість для МСП (малих та середніх підприємств).

Цей критерій оцінює, наскільки легко та ефективно кожен із розглянутих фреймворків або стандартів може бути адаптований, впроваджений та підтримуваний організаціями малого та середнього бізнесу. Для МСП, які, як правило, мають обмежені фінансові та людські ресурси, менш складну IT-інфраструктуру та, можливо, нижчий рівень спеціалізованої експертизи у сфері кібербезпеки порівняно з великими корпораціями, масштабність та відповідність їхнім можливостям є критично важливим фактором при виборі стратегії.

Ключові аспекти масштабованості для МСП:

Відповідність ресурсним обмеженням: Чи вимагає фреймворк ресурсів, які, ймовірно, відсутні в МСП?

Можливість поетапного впровадження: Чи можна впроваджувати фреймворк частинами, починаючи з базових елементів, і поступово розширювати його застосування?

Наявність спрощених настанов: Чи існують спеціальні рекомендації, адаптовані для потреб та можливостей МСП?

Складність та обсяг: Чи є загальна складність та обсяг фреймворку перепоною для МСП?

Необхідність зовнішньої експертизи: Наскільки сильно МСП залежить від залучення дорогих зовнішніх консультантів для впровадження?

Оцінимо тепер масштабованість для МСП для кожного з розглянутих підходів:

ISO/IEC 27001:2022:

Масштабованість: Хоча ISO 27001 є універсальним стандартом, призначеним для організацій будь-якого розміру, його повне впровадження може бути досить складним та ресурсомістким для МСП. Вимоги до створення та підтримки формалізованої СУІБ, значний обсяг необхідної документації та процес управління ризиками можуть виявитися надмірними для невеликих компаній з обмеженим штатом.

Поетапне впровадження: Впровадження ISO 27001 можна певною мірою масштабувати за рахунок визначення вужчої сфери застосування СУІБ на початкових етапах (наприклад, обмеживши її певними критично важливими системами або даними). Однак, базові вимоги до системи управління все одно мають бути виконані.

Спрощені настанови: Попри існування посібників з впровадження ISO 27001, спеціальних "спрощених" версій стандарту для МСП немає.

Вартість та експертиза: Вартість сертифікації (якщо є метою) та необхідність залучення консультантів можуть бути значним фінансовим бар'єром для МСП. Також може бракувати внутрішньої експертизи для розуміння та впровадження всіх вимог стандарту.

Загалом для МСП: Впровадження ISO/IEC 27001 є складнішим та більш ресурсомістким для МСП порівняно з великими організаціями. Хоча це можливо, це вимагає значної відданості та інвестицій. МСП можуть розглядати впровадження ключових принципів стандарту без офіційної сертифікації на початковому етапі.

COBIT 2019:

Масштабованість: COBIT є комплексним фреймворком врядування корпоративними IT, розробленим, в першу чергу, для великих та складних організацій. Його повне впровадження, що охоплює всі процеси врядування та управління IT, є надзвичайно ресурсомістким та складним для більшості МСП.

Поетапне впровадження: Можливе вибіркове застосування окремих частин або принципів COBIT, які є найбільш релевантними для потреб МСП (наприклад, процеси управління ризиками або управління послугами). Однак, без комплексного підходу, повна цінність фреймворку не буде реалізована.

Спрощені настанови: Хоча COBIT 2019 є більш гнучким, ніж попередні версії, спеціальних, значно спрощених настанов для МСП, які б охоплювали весь фреймворк, немає.

Вартість та експертиза: Висока вартість офіційних публікацій та потреба у висококваліфікованій експертизі з врядування IT можуть бути значними бар'єрами для МСП.

Загалом для МСП: COBIT є найменш масштабованим для повного впровадження в МСП через його комплексність та корпоративний фокус. МСП можуть отримати цінність, застосовуючи окремі принципи або моделі процесів, але повна імплементація є, як правило, непрактичною.

CIS Controls v8:

Масштабованість: CIS Controls є дуже добре масштабованими для МСП, і вони, фактично, розроблені з урахуванням потреб менших організацій. Система Груп Впровадження (IG) дозволяє МСП починати з базового рівня (IG1), який включає найважливіші заходи кібергігієни, які є досяжними для більшості невеликих компаній з обмеженими IT-ресурсами.

Поетапне впровадження: Поетапне впровадження є центральним принципом CIS Controls завдяки Групам Впровадження. Організації можуть поступово впроваджувати Safeguards з IG2 та IG3 в міру зростання своєї зрілості та ресурсів.

Спрощені настанови: CIS надає посібники та інші ресурси, які є досить практичними та зрозумілими, що полегшує їх використання МСП.

Вартість та експертиза: Сам фреймворк безплатний. Вартість впровадження залежить від необхідних технічних засобів, але для IG1 багато Safeguards можуть бути реалізовані за допомогою існуючих технологій або доступних рішень. Потреба у високоспеціалізованій експертизі зростає з вищими IG, але базові рівні є досяжними для IT-персоналу МСП.

Загалом для МСП: CIS Controls є одним з найбільш масштабованих та рекомендованих фреймворків для МСП. Вони пропонують чіткий, пріоритизований та поетапний підхід до підвищення рівня кібербезпеки, що відповідає ресурсним обмеженням невеликих компаній.

NIST Cybersecurity Framework 2.0:

Масштабованість: NIST CSF 2.0 є дуже добре масштабованим для МСП, і однією з ключових змін у версії 2.0 є розширення його сфери застосування та адаптація для організацій будь-якого розміру, включаючи МСП. Гнучкість фреймворку дозволяє МСП використовувати його для оцінки своїх унікальних ризиків та пріоритизації дій.

Поетапне впровадження: CSF за своєю природою заохочує поетапний підхід через використання Профілів (поточний та цільовий) та Рівнів Впровадження. МСП можуть зосередитися на досягненні базових результатів у найбільш критичних сферах, визначених у їхньому Профілі.

Спрощені настанови: NIST надає настанови та ресурси, які допомагають організаціям різного розміру використовувати фреймворк, включаючи, ймовірно, майбутні ресурси, спеціально адаптовані для МСП (враховуючи розширення сфери застосування у v2.0).

Вартість та експертиза: Сам фреймворк безплатний. Вартість та ресурсомісткість залежать від результатів оцінки та плану дій, визначеного за допомогою CSF. Потреба у зовнішній експертизі менш виражена для використання самого фреймворку порівняно з ISO 27001 або COBIT, але може знадобитися для реалізації складних технічних заходів, на які CSF посилається.

Загалом для МСП: NIST Cybersecurity Framework 2.0 є також дуже масштабованим та підхожий для МСП. Він надає гнучку основу для розуміння та управління кіберризиками, дозволяючи МСП зосередитися на найважливіших для них аспектах та використовувати його для інтеграції інших, більш технічних ресурсів, таких як CIS Controls.

Висновки за критерієм "Масштабованість для МСП":

Найбільш масштабовані для МСП: CIS Controls та NIST Cybersecurity Framework 2.0. Обидва пропонують гнучкі, поетапні підходи, які відповідають ресурсним обмеженням та можливостям невеликих компаній. CIS Controls більш орієнтовані на конкретні, дієві захисні заходи, тоді як NIST CSF надає ширшу основу для управління ризиками.

Менш масштабовані для повного впровадження в МСП: ISO/IEC 27001 та COBIT 2019. Їхня комплексність, формалізовані вимоги (особливо у випадку ISO 27001) та значна ресурсомісткість роблять повне впровадження складним та, можливо, недоцільним для більшості МСП. Однак, МСП можуть отримати користь, застосовуючи окремі принципи або елементи цих фреймворків.

Для МСП часто найкращим підходом є початок з впровадження CIS Controls (особливо IG1) для швидкого підвищення базового рівня безпеки, а потім використання NIST CSF як інструменту для оцінки ризиків, планування подальших дій та інтеграції інших відповідних стандартів та практик.

2.3. Методи та підходи до впровадження

Впровадження стратегій кібербезпеки та управління IT може здійснюватися за допомогою різних методологій та підходів, кожен з яких має свої особливості та застосування. Розглянемо три основні категорії: процесно-орієнтований, організаційно-методичний та хмарний підхід.

Процесний підхід (PDCA, NIST CSF)

Визначення:

Процесний підхід зосереджений на розгляді діяльності організації як набору взаємопов'язаних процесів, спрямованих на досягнення певних результатів. В контексті кібербезпеки та управління IT, це означає створення, моніторинг, аналіз та постійне покращення процесів, пов'язаних із забезпеченням безпеки та ефективності IT. Цей підхід часто реалізується через ітераційні цикли, такі як цикл Демінга-Шухарта (PDCA – Plan-Do-Check-Act).

Застосування та Специфіка:

Процесний підхід є фундаментальним для побудови систем управління, оскільки він забезпечує структурований та повторюваний спосіб досягнення цілей.

Цикл PDCA (Plan-Do-Check-Act):

Plan (Планування): Визначення цілей, процесів та ресурсів, необхідних для досягнення результатів відповідно до політики організації.

Включає ідентифікацію ризиків та можливостей.

Do (Виконання): Впровадження запланованих процесів та заходів.

Check (Перевірка): Моніторинг та вимірювання процесів та результатів порівняно з політиками, цілями та вимогами, а також повідомлення про результати. Включає проведення внутрішніх аудитів.

Act (Дія): Вжиття заходів для постійного покращення результативності процесів. Включає коригувальні дії.

Застосування в ISO/IEC 27001: Стандарт ISO/IEC 27001 прямо базується на циклі PDCA для створення, впровадження, функціонування, моніторингу, перегляду, підтримки та покращення СУІБ. Розділи стандарту (наприклад, Планування, Функціонування, Оцінка результативності, Поліпшення) чітко відповідають фазам PDCA.

Застосування в NIST CSF: Хоча NIST CSF не нав'язує конкретний цикл, його структура функцій (Govern, Identify, Protect, Detect, Respond, Recover) передбачає циклічний та ітераційний процес управління кіберризиками. Організації ідентифікують ризики, впроваджують захист, виявляють інциденти, реагують на них, відновлюються, а потім, на основі отриманого досвіду та зміни контексту (Govern), повторно ідентифікують ризики, таким чином постійно покращуючи свою кібербезпеку.

Характеристики та Переваги:

Системність: Забезпечує структурований та послідовний підхід до управління.

Постійне покращення: Вбудований механізм для безперервного вдосконалення.

Вимірюваність: Дозволяє встановлювати показники ефективності та моніторити їх досягнення.

Адаптивність: Дозволяє адаптувати процеси до мінливих умов.

Організаційно-методичний підхід (COBIT, CIS Controls)

Визначення:

Організаційно-методичний підхід зосереджений на наданні структурованих фреймворків, настанов та конкретних методів для побудови системи врядування та управління ІТ та/або кібербезпеки. Він визначає, які процеси, структури та ролі мають

бути наявні в організації для досягнення певних цілей. Цей підхід часто менш циклічний у своїй основі порівняно з процесним, але надає більш чіткі рамки та конкретніші "будівельні блоки".

Застосування та Специфіка:

Організаційно-методичні фреймворки надають організації готову структуру та набір рекомендацій для впровадження.

Застосування в COBIT: COBIT є яскравим прикладом організаційно-методичного підходу до врядування та управління IT. Він визначає принципи, компоненти системи врядування (процеси, організаційні структури, інформація тощо) та цілі врядування/управління. COBIT надає моделі процесів та описує діяльність, яка має виконуватися, а також необхідні організаційні структури та інформаційні потоки. Він допомагає організації визначити, хто за що відповідає і як мають взаємодіяти різні частини організації для ефективного управління IT.

Застосування в CIS Controls: CIS Controls, хоч і є набором технічних та організаційних заходів контролю, також можуть розглядатися як частина організаційно-методичного підходу. Вони надають конкретні, пріоритизовані "методи" (контролі та Safeguards) для захисту від загроз. CIS Controls визначають, що саме потрібно зробити на технічному та організаційному рівнях, щоб підвищити рівень кібербезпеки. Групи впровадження (IG) надають методику пріоритизації та послідовності дій.

Характеристики та Переваги:

Структурованість: Надає чіткі рамки та готові моделі для впровадження.

Комплексність: Охоплює різні аспекти врядування та управління (для COBIT) або конкретні захисні заходи (для CIS Controls).

Настанови: Надає конкретні рекомендації та методики.

Можливість порівняння: Дозволяє порівнювати поточний стан організації з моделлю фреймворку.

Хмарний підхід (CSA Cloud Controls)

Хмарний підхід до впровадження кібербезпеки та управління IT зосереджений на специфічних аспектах безпеки, пов'язаних з використанням хмарних обчислень.

Він враховує унікальні виклики та моделі відповідальності, які виникають при використанні публічних, приватних або гібридних хмар. Цей підхід часто доповнює традиційні фреймворки, надаючи детальніші настанови для хмарних середовищ.

Застосування та Специфіка:

Використання хмарних сервісів вимагає адаптації традиційних підходів до безпеки. Хмарний підхід враховує такі аспекти, як спільна відповідальність між постачальником хмарних послуг (CSP) та споживачем хмарних послуг (CSC), безпека даних у хмарі, управління ідентифікацією та доступом у хмарних середовищах, безпека самих хмарних інфраструктур та додатків, розгорнутих у хмарі.

CSA Cloud Controls Matrix (CCM): Cloud Security Alliance (CSA) є провідною організацією у сфері безпеки хмарних обчислень. CSA Cloud Controls Matrix (CCM) є визнаним фреймворком контролів безпеки, спеціально розробленим для хмарних середовищ.

Призначення CCM: Надати структурований набір контролів безпеки, який охоплює різні аспекти хмарних обчислень. CCM допомагає організаціям (як постачальникам, так і споживачам хмарних послуг) оцінювати та покращувати свою безпекову позицію в хмарі.

Структура CCM: CCM складається з набору доменів контролів, що охоплюють такі області як управління безпекою, відповідність, врядування ризиками, безпека даних, безпека операцій, управління доступом та ідентифікацією, безпека додатків тощо. Для кожного контролю надається опис та його відповідність іншим стандартам (таким як ISO 27001, NIST CSF, COBIT).

Специфіка для хмарного підходу: CCM допомагає зрозуміти, які заходи контролю мають бути реалізовані постачальником хмарних послуг, а які – споживачем, відповідно до моделі спільної відповідальності (shared responsibility model). Він також надає настанови щодо оцінки безпеки хмарних провайдерів.

Характеристики та Переваги:

Спеціалізація: Фокусується на унікальних викликах та аспектах безпеки хмарних обчислень.

Актуальність: Відображає сучасні практики та рекомендації для хмарних середовищ.

Допомога у виборі провайдера: Надає інструменти для оцінки безпеки хмарних постачальників.

Чіткість відповідальності: Допомагає розмежувати зони відповідальності між постачальником та споживачем хмарних послуг.

Взаємозв'язок між підходами:

Ці підходи можуть інтегруватися. Наприклад, організація може використовувати:

NIST CSF або ISO 27001 як загальну рамку управління кіберризиками (процесний підхід).

COBIT для вдосконалення загального врядування та управління IT (організаційно-методичний підхід).

CIS Controls для впровадження конкретних технічних заходів контролю, які підтримують цілі NIST CSF або ISO 27001 (організаційно-методичний підхід, що реалізує процеси).

CSA CCM для забезпечення безпеки своїх хмарних середовищ, інтегруючи ці контролі в загальну систему управління безпекою (хмарний підхід, що доповнює процеси та методи). Вибір підходу або їх комбінації залежить від зрілості організації, її бізнес-моделі (зокрема, використання хмарних технологій) та конкретних цілей у сфері кібербезпеки та управління IT.

2.4. Детальний огляд NIST CSF 2.0 для МСП

NIST Cybersecurity Framework (CSF) 2.0 — це оновлена версія оригінальної структури, представленої Національним інститутом стандартів і технологій (NIST). Він розроблений, щоб допомогти організаціям керувати ризиками кібербезпеки та зменшувати їх. NIST Cybersecurity Framework (NIST CSF) — це гнучкий набір інструкцій і найкращих практик, розроблених, щоб допомогти організаціям підвищити інформаційну безпеку та керувати ризиками кібербезпеки.

NIST CSF v2.0 представляє оновлення, які зосереджують увагу на управлінні (додаючи шосту основну функцію під назвою «Управління»), управлінні ризиками в ланцюжку постачання та вимірюванні результатів кібербезпеки, при цьому вони більше відповідають міжнародним стандартам і підвищують гнучкість для різноманітних організацій.

Історія NIST Framework

NIST Cybersecurity Framework був представлений у 2014 році як добровільне керівництво для організацій щодо покращення практики кібербезпеки. NIST CSF 1.0 швидко став широко поширеним інструментом у різних галузях, пропонуючи структурований підхід до управління та пом'якшення ризиків кібербезпеки. У 2018 році NIST випустив CSF 1.1, який включав оновлення, спрямовані на зростання важливості управління ризиками в ланцюзі постачання і надання додаткових вказівок щодо автентифікації, авторизації та підтвердження особи.

опублікована як загальнодоступний проєкт у 2023 році та остаточна версія в лютому 2024 року, представляє функцію «Управління», розширює існуючі основні функції та узгоджує структуру з сучасними викликами кібербезпеки.

NIST CSF 2.0 структурований навколо шести основних функцій, кожна з яких представляє критичний аспект ефективної програми кібербезпеки. Це містить п'ять оригінальних основ з NIST 1.1 - ідентифікацію, захист, виявлення, реагування та відновлення і вводить нещодавно додану функцію «Управління». Структура забезпечує комплексний підхід до управління ризиками кібербезпеки. Ці стовпи представляють ключові етапи надійної програми кібербезпеки, керуючи організаціями в розумінні, управлінні та зниженні ризиків кібербезпеки. Кожен стовп має важливі дії, які є критично важливими для ефективної стратегії кібербезпеки.[25]

Функція Govern у NIST CSF 2.0 - це не якийсь громіздкий набір правил для великих корпорацій, а насамперед запрошення керівництву малого бізнесу взяти на себе відповідальність за кібербезпеку. Уявіть собі: у вас немає окремого IT-департаменту, але є власник чи менеджер, який усе вирішує. Саме ця людина (або невелика група, наприклад у складі вашого IT-адміністратора та зовнішнього консультанта) має взяти на себе роль «господаря» безпеки від стратегії до контролю.

Спершу слід зрозуміти, що для вас справді важливо. Навіть за обмежених ресурсів можна провести просту інвентаризацію — скласти список комп'ютерів, систем, облікових записів і даних клієнтів, які безпосередньо впливають на роботу бізнесу. Саме на цьому етапі ви визначаєте, від чого залежить ваша діяльність найсильніше: чи це CRM-система з усіма контактами, чи фінансові звіти, чи база рецептів вашого виробництва.

Далі настане час перенести все це на папір, але не у вигляді довжелезного документа. Досить кількох сторінок із чітко прописаними правилами: хто відповідає за оновлення паролів і резервне копіювання, як ми реагуємо на підозрілий лист, хто і коли перевіряє логи, хто затверджує закупівлю нових засобів захисту. Ці правила стають вашим внутрішнім «маніфестом», до якого можна повернутися, якщо раптом знадобиться швидко зорієнтуватися в кризовій ситуації.

Нарешті, коли у вас є відповідальний, інвентар активів і кілька базових політик, прийняття рішень переходить у більш усвідомлений режим: чи варто зараз інвестувати у багатофакторну автентифікацію, чи краще відкласти покупку нового брандмауера, а може зосередитися на тренінгах для персоналу. Саме так маленькими кроками рамках функції Govern ви інтегруєте кібербезпеку в загальну стратегію бізнесу, а не залишаєте її «на технарів». Адже коли керівництво розуміє ризики й бере на себе відповідальність, усі наступні заходи з кіберзахисту працюють ефективніше й узгоджені з цілями компанії.

Функція Identify у NIST CSF 2.0 зазвичай сприймається як формальна частина аудиту, але насправді вона починається з дуже простої ідеї: «якщо ми не знаємо, що у нас є, ми не зможемо це захистити». Уявіть, що у вас є кілька комп'ютерів, кілька серверів, а ще ноутбуки співробітників і хмарні сервіси та ви навіть не впевнені, звідки приходять оновлення Windows чи хто має доступ до загальної папки зі звітами. Саме це й трапляється з багатьма маленькими фірмами, які починають будувати свій кіберзахист «зверху вниз», але забувають про найважливіше: інвентар активів.

Для МСП перелік усіх пристроїв і програмного забезпечення — не просто технічна деталізація, а базовий документ, який повинен жити й дихати разом із бізнесом. Уявіть, що ви відкриваєте Excel із трьома стовпцями: «Пристрій/Сервіс»,

«Відповідальний» і «Розташування (онлайн чи офлайн)». Це не має бути щось складне: інвентар можна вести навіть вручну, дописуючи туди нові ноутбуки, коли їх купують, і стираючи пристрої, коли вони виводяться з експлуатації. Але головне — зафіксувати, хто конкретно відповідає за кожен елемент: власник онлайн-сервісу, адміністратор ПК, відповідальний за CRM-систему.

Далі варто поглянути на дані, які зберігаються в цих пристроях і сервісах. Чи є у вас база контактів клієнтів у Google Workspace? Чи розрахунки по зарплаті в окремому Excel-файлі на локальному сервері? Важливо зрозуміти, який рівень ризику несе кожен із цих активів: втрата технічного звіту навряд чи поставить під загрозу компанію, а от втрата або викрадення клієнтських даних може стати початком великого скандалу.

Не забувайте включити в інвентаризацію і хмарні сервіси: пошту, спільні диски, CRM, навіть корпоративні сторінки в соцмережах. Вони можуть здатися менш «важкими», ніж сервери, але в разі витоку даних саме там часто трапляються найбільші проблеми. І, звісно, цей список потрібно оновлювати щоразу, коли з’являється нова програма або коли у вас змінюється команда.

Коли у вас на руках є такий «життєвий» перелік активів і ризикових даних, починається справжнє управління ризиками — ви розумієте, що слід захищати в першу чергу, а де можна обмежитися базовими заходами. Без цієї базової «картки місцевості» всі ваші подальші кроки — від налаштування брандмауера до впровадження багатофакторної автентифікації — ризикують стати хаотичними або навіть марними. Саме тому функція Identify є справжнім фундаментом у побудові кібербезпеки для малих і середніх підприємств.

Уявіть, що ви вже побудували інвентар активів і знаєте, що саме потрібно захищати (Identify). Тепер прийшов час перейти до Protect - впровадження практичних засобів, які дійсно створять захисний “щит” навколо вашого бізнесу.

Для малого бізнесу це означає три ключові речі: чіткі правила доступу, багатофакторну автентифікацію та своєчасні оновлення (патчі).

По-перше, політики доступу.

Намалюйте уявну карту ролей у вашій компанії: хто є простим користувачем, хто адміністратором, а хто тим, хто має доступ лише до вузького кола інформації (наприклад, бухгалтерії чи клієнтських баз). Далі продумайте, як ці ролі мають змінюватися, коли люди приходять чи йдуть (процедура надання і відкликання прав). Не забувайте: якщо колега звільняється, його облікові записи мають бути “зачинені” того ж дня, а усі фізичні носії - здані назад.

По-друге, (MFA).

Ви вже чули, що пароль “qwerty123” - це майже двері із відкритим замком. Тому найважливіші облікові записи (адмінпанелі, пошта, хмарні сервіси) обов’язково ставте під захист другого фактора: код із SMS, додаток-генератор чи навіть апаратний ключ. Навіть якщо зловмисники викрадуть ваш пароль, без другого “токена” до системи не потраплять.

По-третє, патчі й оновлення.

Будь-яке програмне забезпечення час від часу “зливає” в мережу інформацію про свої слабкі сторони. Якщо ви не встигнете заклеїти цю “дірку” оновленням, за неї хтось обов’язково вчепиться. Тому варто налаштувати автоматичні апдейти або призначити відповідального, який кожного тижня перевіряє наявність нових патчів та встановлює їх одразу після тесту.

Ці три кроки — найпростіший, але вкрай потужний набір дій у розділі Protect. Вони не потребують роками навчання чи сотень тисяч гривень у бюджеті, але дозволяють позначити чіткі межі того, хто і як може взаємодіяти з вашими IT-ресурсами. Згодом, коли захисний каркас буде готовий, саме ці базові контролі стануть фундаментом для впровадження більш просунутих технологій і процедур.

Уявіть, що у вашому бізнесі відбувається дивна активність: хтось намагається зайти не зі свого робочого комп’ютера, або сервер раптово відправляє величезний обсяг даних у невідомому напрямі. Саме такими «сигналами тривоги» займається функція Detect. Її завдання — налаштувати постійний «радар» на всіх критичних ланках вашої мережі й серверів, щоб помічати підозрілі події ще на ранній стадії.

Для малого бізнесу це не означає купівлю складної та дорогої системи захисту достатньо почати з базового моніторингу: збирати логи з ваших серверів, роутерів,

фаєрволів і навіть робочих ПК, а потім одному разу на день або тиждень швидко переглядати, чи немає там «чужих» спроб доступу чи аномалій. Є безліч простих та недорогих інструментів, які допомагають це зробити: вони автоматично збирають інформацію й видають попередження, якщо, наприклад, хтось намагається залогінитися двічі невірним паролем або якщо з'являються незвичні патерни трафіку.

Якщо дозволяє бюджет або ви готові залучити зовнішніх фахівців, спробуйте кероване SIEM-рішення (Managed SIEM). Це фактично хмарний сервіс, який бере на себе збір і кореляцію логів із різних джерел, автоматично шукає складніші сигнатури атак та навіть пропонує базові поради з реагування. Для МСП ще корисніше — не витрачатися на дорогу інфраструктуру, а підписатися на сервіс, де за прийнятну щомісячну плату ви отримаєте готовий моніторинг і звіти.

Головне в Detect - не ігнорувати «дрібні» сигнали. Якщо ви помітили, що працівник дивно поводиться з обліковим записом, або трафік із вашого сайту пішов не туди, куди треба — це ваш шанс гальмувати атаку, поки вона не стала справжньою катастрофою. Навіть кілька хвилин раннього попередження можуть заощадити вам години роботи з відновлення та тисячі гривень на ліквідацію наслідків.

У житті будь-якого малого бізнесу може настати момент, коли ви раптом дізнаєтеся: трапився інцидент від незрозумілого збою сервера до підозрілого спаму, який розсилається від імені вашої компанії. Саме для таких випадків у NIST CSF 2.0 існує функція Respond «Реагування». Вона не про те, щоб створювати громіздкі плани для великих корпорацій, а скоріше про те, щоб мати під рукою простий чіткий алгоритм дій, коли все піде не за планом.

Уявіть собі: ви побачили сплеск трафіку на сервері або отримали повідомлення про те, що всі файли на комп'ютері зашифровані. Замість паніки ви дістаєте свій «інцидент чек ліст» — короткий документ, в якому вже прописано, куди й кому дзвонити, які машини слід відключити від мережі й де лежать резервні копії.

По-перше, варто заздалегідь визначити, хто в команді що робить. Наприклад, власник бізнесу перевіряє політику інформування клієнтів, IT-спеціаліст ізолює заражені пристрої, а ваш зовнішній консультант на зв'язку, щоб підказати, як видалити шкідливе ПЗ. У чек-лісті обов'язково мають бути телефони (або мейли) не

лише внутрішніх співробітників, а й зовнішніх партнерів: IT-підтримки, юриста чи навіть страхових агентів, якщо ви користуєтеся кіберстрахуванням.

По-друге, сам план можна розбити на кілька простих етапів:

1. Ідентифікація — підтвердити, що це дійсно інцидент, а не помилка користувача чи тимчасовий збій.

2. Стримування — відключити пошкоджені пристрої від мережі, зупинити поширення атаки.

3. Ліквідація — знайти й видалити шкідливе програмне забезпечення, закрити вразливості.

4. Відновлення — повернути дані з резервних копій, перевірити цілісність систем.

5. Уроки — обговорити, що пішло не так, і внести зміни до політик та процедур, щоб наступного разу діяти ще швидше й ефективніше.

Не забудьте, що під час інциденту доступ до цифрових ресурсів може бути обмеженим — наприклад, сервери можуть бути недоступні. Тому тримайте друковану копію плану у сейфі чи на робочому столі, а також електронний варіант у хмарі. І нарешті — проведіть невелике тренування або розсилку з поясненням ролей, щоб кожен у команді знав: коли «спрацювала тривога», є чітка інструкція, кому що робити.

Саме така «під рукою» готовність без зайвої бюрократії дозволяє малому бізнесу не лише швидше впоратися з проблемою, а й показати клієнтам, що ви відповідаєте за безпеку своїх послуг.[18]

Функція Recover у NIST CSF 2.0 - це про те, як швидко повернути все до ладу, якщо вже трапився інцидент. Для малого бізнесу важливо не просто мати копії файлів, а вміти їх реально відновлювати, щоб не втрачати клієнтів і не простоювати довго.

Уявіть: ваш сервер раптом «ліг», і дані, які там були, пішли у небуття (через збій, атаку чи будь-що інше). Якщо ви вчасно не увімкнули бекапи, то доведеться працювати «наосліп». Тому перше завдання — налаштувати автоматичне резервне

копіювання всього критичного: баз даних, конфігів серверів, робочих документів куди завгодно, лише б це було поза вашим офісом.

Саме тут корисні поняття RTO (скільки часу максимум ви готові простоювати) і RPO (яку кількість даних ви можете втратити). Наприклад, якщо ваш RTO - 4 години, значить, після збою ви хочете повернутися до роботи не пізніше ніж за 4 години. А якщо RPO - 12 годин, копії мають робитися хоча б двічі на добу, щоб за збою ви втратили не більше пів доби інформації.

Коли бекапи налаштовані, обов’язково раз на місяць (а краще частіше) проганяйте відновлення на тестовій машині. Без такої перевірки про будь-які копії можна забути: може виявитися, що файли неповні або пошкоджені.

І ще немає сенсу складати багатосторінковий план дій. Достатньо простого короткого сценарію:

1. Хто бере на себе відновлення (наприклад, IT-адмін чи зовнішній сервіс).

2. Звідки брати копії (шлях у хмарі або локальний змонтований диск).

3. Послідовність кроків: зупинити уражену систему, змонтувати бекап, закачати його, перевірити працездатність сервісу.

Якщо все зробити так, ви отримаєте живий «план порятунку»: навіть у розпалі кризи можна за кілька годин повернути бізнес до життя, а не тижнями морочити голову над втраченими даними.

Використання NIST CSF 2.0 з фокусом на цих ключових активностях дозволяє МСП побудувати ефективну програму кібербезпеки, яка відповідає їхнім потребам та ресурсам, забезпечуючи при цьому захист від найбільш актуальних загроз. Важливо пам'ятати про ітеративний характер фреймворку – процеси ідентифікації, захисту, виявлення, реагування та відновлення мають постійно переглядатися та вдосконалюватися під наглядом функції Govern.[19]

2.5. Критерії ефективності та KPI

Коли ми говоримо про реальну користь від усіх наших фреймворків і процесів: ISO 27001, NIST CSF, CIS Controls чи COBIT - основне питання звучить так: як

зрозуміти, що ми дійсно рухаємося в правильному напрямку? Саме тут на сцену виходять критерії ефективності та KPI - це наші маяки, що показують, яке плавання вдале, а де слід підкоригувати курс.[26]

Уявіть: ви запровадили моніторинг, MFA, бекапи, навчили команду, але досі не знаєте, чи швидше реагуєте на атаки, чи справді їх стало менше, чи ваші люди не натраплять на фішинговий лист. Щоб дати однозначні відповіді, варто стежити хоча б за трьома речами:

1. Час виявлення та реагування.

Уявіть, що злодій підкрадається до вашої мережі — чи ви його помітите через 10 хвилин, чи через три дні? Тож найперше KPI: Time to Detect (TTD) - скільки проходить часу від «щось пішло не так» до «ми знаємо, що сталося». І Time to Respond (TTR) - від перших тривожних сповіщень до повного гасіння пожежі й запуску бізнес-процесів. Якщо ці значення зменшуються, означає, що моніторинг і план реагування працюють.

2. Кількість інцидентів

Здавалося б, менше інцидентів — добре. Але ще треба бути впевненим, що не “не бачимо” проблем. Тому при підрахунку слід розділяти їх за типами (фішинг, malware, внутрішні помилки) і рівнем критичності. Якщо за місяць стало на чверть менше спрацювань фаєрволу або хтось не натрапив на черговий фішинговий лист — це вже знак прогресу. Проте завжди порівнюйте з TTD/TTR: іноді низька цифра може означати просто недобрий моніторинг. Світ кіберзагроз дуже динамічний, і навіть найкрутіші технології не допоможуть, якщо співробітники не розпізнають простий фішинг. Тож ще один KPI - рівень обізнаності.

Запустіть симуляцію фішингового розсилання та порахуйте, скільки людей натиснули на «підозріле» посилання.

Потім проведіть короткі тести після навчання і подивіться на відсоток правильних відповідей.

Нарешті, відстежувати, скільки разів працівники повідомляли про підозрілу активність: чим більше таких повідомлень, тим вище їхня «кіберуважність».

Збираючи ці дані, ви отримуєте «живі» метрики, які постійно підказують: чи працюють ваші політики доступу і моніторинг, чи справді захист від фішингу покращився, чи не потребує план реагування доопрацювання.

По-перше, ви перестанете «ліпити» заходи наосліп кожне нове рішення можна перевірити: чи скоротило воно час реагування або не дало системі впасти.

По-друге, керівництво бачить цифри: «Ми скоротили TTR із 8 до 4 годин» - це конкретний успіх, який полегшує обґрунтування бюджету на подальші покращення.

По-третє, із таким підходом поступово виходить ідеальний цикл PDCA: ви плануєте заходи, виконуєте, перевіряєте за KPI й вдосконалюєте процеси далі.[42]

Отже, замість абстрактних заяв про «покращення безпеки» тримайте на контролі кілька простих, але інформативних показників і ваша кіберстратегія засяє реальними результатами.[27]

Висновок до розділу 2

Провідні фреймворки кібербезпеки та управління IT, такі як ISO/IEC 27001, COBIT, CIS Controls та NIST Cybersecurity Framework 2.0, пропонують різні, але цінні підходи. Вибір залежить від потреб організації, її розміру (зокрема, МСП), ресурсів та цілей, оскільки фреймворки відрізняються за складністю, вартістю та масштабованістю.

ISO 27001 та COBIT є більш комплексними та ресурсомісткими, тоді як CIS Controls та NIST CSF 2.0 більш гнучкі та масштабовані, що робить їх привабливішими для МСП.

Незалежно від обраного підходу, критично важливо оцінювати ефективність впроваджених заходів. Ключові Показники Ефективності (KPI), такі як час виявлення та реагування на інциденти, кількість інцидентів та рівень підготовки персоналу, надають об'єктивну інформацію про стан безпеки. Моніторинг KPI дозволяє виявляти слабкі місця, приймати обґрунтовані рішення, демонструвати цінність інвестицій у безпеку та забезпечувати постійне вдосконалення програми кібербезпеки у відповідь на мінливі загрози.

РОЗДІЛ 3
РОЗРОБКА МЕТОДУ ЩОДО ВПРОВАДЖЕННЯ СТРАТЕГІЙ КІБЕРБЕЗПЕКИ МСП

3.1. Опис уявного малого підприємства

Для цілей нашої практичної частини, створім профіль типового малого підприємства. Це допоможе зробити процес впровадження цільового профілю безпеки більш наочним та релевантним до реальних викликів, з якими стикається подібний бізнес.

Назва підприємства: "ЕкоДім Буд"

Тип діяльності: Компанія, що спеціалізується на проєктуванні та будівництві енергоефективних та екологічно чистих приватних будинків. Діяльність включає роботу з клієнтами, архітектурне проєктування, управління проєктами будівництва, закупівлі матеріалів та координацію роботи підрядників.

Розмір підприємства: 15 співробітників. Включає керівництво, менеджерів проєктів, архітекторів, адміністративний персонал та фахівців із закупівель.

IT-інфраструктура:

Близько 20 робочих станцій (переважно ноутбуки на Windows та кілька Mac для архітекторів).

Один файловий сервер для зберігання проєктної документації, договорів, фінансових даних та іншої внутрішньої інформації.

Мережеве обладнання (роутер з Wi-Fi) для доступу до Інтернету.

Хмарні сервіси:

Корпоративна електронна пошта (Google Workspace).

Хмарне сховище для спільної роботи над проєктами та обміну файлами з клієнтами (Google Drive).

Облікова система (хмарне рішення).

CRM-система для управління відносинами з клієнтами (хмарне рішення).

Мобільні пристрої співробітників, що використовуються для доступу до корпоративної пошти та хмарних сервісів (BYOD - Bring Your Own Device).

Вебсайт компанії, розміщений на зовнішньому хостингу.

Типи даних, що обробляються:

- Персональні дані клієнтів (ПІБ, контактна інформація, паспортні дані для договорів).
- Фінансова інформація (банківські реквізити клієнтів та підрядників, дані про платежі, бухгалтерська звітність).
- Проєктна документація (архітектурні проєкти, інженерні розрахунки, кошториси) – є інтелектуальною власністю.
- Внутрішня корпоративна інформація (договори з підрядниками, дані співробітників).

Поточний стан кібербезпеки (самооцінка підприємства):

- Встановлено базовий антивірус на більшості робочих станцій (не централізовано).
- Оновлення ПЗ відбувається нерегулярно, часто залежить від ініціативи користувача.
- Використовуються Wi-Fi мережі із захистом WPA2, але зі стандартними паролями для адміністративного доступу до роутера.
- Резервне копіювання даних з файлового сервера здійснюється на зовнішній жорсткий диск раз на тиждень (диск зберігається в офісі). Резервне копіювання даних з хмарних сервісів залежить від політик самих провайдерів.
- Немає чітких політик щодо паролів, доступу до інформації, використання особистих пристроїв.
- Навчання персоналу з кібербезпеки не проводилося, обізнаність низька.
- Немає формалізованого плану реагування на інциденти.
- Відсутнє централізоване управління обліковими записами та правами доступу, особливо для хмарних сервісів.
- Керівництво усвідомлює необхідність покращення безпеки через зростання кількості кіберзагроз та обробку чутливих даних клієнтів, але не знає, з чого почати.

Бізнес-цілі, пов'язані з IT/Кібербезпекою:

- Захист даних клієнтів та проєктної документації.
- Забезпечення безперервності бізнес-процесів у разі інциденту.
- Підвищення довіри з боку клієнтів та партнерів шляхом демонстрації відповідального ставлення до безпеки.
- Дотримання базових вимог законодавства щодо захисту персональних даних (наприклад, GDPR, якщо працюють з клієнтами з ЄС, або національних аналогів).
- Зменшення ризику фінансових втрат від кібератак.

Цей опис "ЕкоДім Буд" послужить відправною точкою для наступних кроків: оцінки їхнього поточного стану кібербезпеки відповідно до NIST CSF 2.0 (поточний профіль) та розробки цільового профілю – бажаного стану безпеки, який вони прагнуть досягти.

3.2. Аналіз поточного стану: оцінка ризиків та вразливостей

Після опису уявного малого підприємства "ЕкоДім Буд" та його IT-середовища, наступним логічним кроком у процесі впровадження цільового профілю безпеки за NIST CSF 2.0 є глибокий аналіз поточного стану кібербезпеки. Цей аналіз включає ідентифікацію активів (що було покладено в основу опису підприємства), виявлення вразливостей та оцінку ризиків, пов'язаних із цими вразливостями та потенційними загрозами.

Важливість аналізу поточного стану та оцінки ризиків:

У контексті NIST CSF 2.0, аналіз поточного стану та оцінка ризиків є ключовими компонентами функції Identify (Ідентифікація) та тісно пов'язані з функцією Govern (Управління). Розуміння поточних ризиків є необхідною передумовою для прийняття обґрунтованих рішень щодо того, що потрібно захищати, як це робити та які ресурси виділяти. Для МСП з обмеженими ресурсами пріоритизація зусиль на основі оцінки ризиків є життєво важливою для забезпечення максимальної ефективності інвестицій у безпеку.

Виявлення вразливостей та оцінка ризиків для "ЕкоДім Буд":

Виходячи з опису ІТ-інфраструктури, типів даних та поточного стану кібербезпеки "ЕкоДім Буд", можна ідентифікувати низку потенційних вразливостей та пов'язаних з ними ризиків:

1. Вразливість: Нерегулярне оновлення програмного забезпечення та відсутність централізованого патч-менеджменту.

1.1. Ризик: Експлуатація відомих уразливостей зловмисниками (наприклад, через шкідливе ПЗ, що використовує "дірки" в старому ПЗ), що може призвести до компрометації систем, витоку даних або зараження програмами-вимагачами.

2. Вразливість: Відсутність чітких політик щодо паролів та, ймовірно, використання слабких або однакових паролів співробітниками.

2.1. Ризик: Компрометація облікових записів через підбір паролів або використання викрадених облікових даних. Це може надати зловмисникам доступ до внутрішніх систем та даних, включаючи хмарні сервіси.

3. Вразливість: Використання особистих мобільних пристроїв (BYOD) без належного контролю та політик безпеки.

3.1. Ризик: Втрата або крадіжка пристрою з доступом до корпоративної пошти та даних, зараження шкідливим ПЗ на особистому пристрої, яке потім може поширитися на корпоративні ресурси.

4. Вразливість: Обмежене резервне копіювання даних (раз на тиждень, диск зберігається в офісі) та залежність від політик хмарних провайдерів.

4.1. Ризик: Втрата значного обсягу даних (до тижня роботи) у разі збою обладнання, пожежі, крадіжки або атаки програм-вимагачів, якщо резервні копії також будуть скомпрометовані або недоступні.

5. Вразливість: Низька обізнаність співробітників з кібербезпеки та відсутність навчання.

5.1. Ризик: Успішні фішингові атаки, соціальна інженерія, перехід за шкідливими посиланнями, завантаження та запуск шкідливих файлів. Це є однією з найбільш значущих вразливостей для будь-якого бізнесу.

6. Вразливість: Відсутність централізованого управління обліковими записами та правами доступу.

6.1. Ризик: Надмірні права доступу у співробітників, що підвищує ризик випадкової або навмисної компрометації даних. Складність відкликання доступу для звільнених співробітників.

7. Вразливість: Стандартні паролі адміністративного доступу до мережевого обладнання.

7.1. Ризик: Несанкціонований доступ до мережевих налаштувань, перехоплення трафіку, зміна налаштувань безпеки мережі.

8. Вразливість: Залежність від безпеки хмарних провайдерів без належної оцінки та налаштування безпекових параметрів з боку "ЕкоДім Буд".

8.1. Ризик: Компрометація даних, що зберігаються у хмарі, через слабкі налаштування безпеки з боку користувача або вразливості у взаємодії з хмарним сервісом.

Нижче представлено таблицю, що візуалізує Базовий Профіль "ЕкоДім Буд" за відповідними Підкатегоріями NIST CSF 2.0. Це по суті є "зрізом" їхнього поточного стану за тими областями, які ми визначили як важливі для їхнього Цільового Профілю.

Таблиця 3.1

Базовий профіль "ЕкоДім Буд"

Функція CSF	Категорія CSF	NIST CSF 2.0 Підкатегорія	Поточний Стан ("ЕкоДім Буд")
Govern	Risk Management Strategy	GV.RM-01: Політика управління ризиками кібербезпеки визначена та доведена до відома.	Відсутня формалізована політика.
Govern	Organizational Structure	GV.OR-01: Ролі та відповідальність за управління кіберризиками визначені та доведені до відома.	Ролі не чітко визначені, відповідальність не формалізована.
Identify	Asset Management	ID.AM-01: Фізичні пристрої інвентаризовані.	Є базовий, ймовірно, неповний список.
Identify	Asset Management	ID.AM-02: Програмне забезпечення інвентаризоване.	Немає системної інвентаризації ПЗ.
Identify	Asset Management	ID.AM-05: Інформаційні активи ідентифіковані та класифіковані.	Немає класифікації даних.

продовження таблиці 3.1

Identify	Risk Assessment	ID.RA-01: Уразливості активів ідентифіковані та задокументовані.	Уразливості відомі на інтуїтивному рівні (старе ПЗ).
Identify	Risk Assessment	ID.RA-02: Загрози ідентифіковані та задокументовані.	Базове розуміння загроз (фішинг).
Protect	Identity and Access Management	PR.AC-01: Фізичний та логічний доступ до активів управляється.	Немає формалізованих правил доступу.
Protect	Identity and Access Management	PR.AC-03: Багатофакторна автентифікація (MFA) використовується.	Не використовується.
Protect	Awareness Training	PR.AT-01: Співробітники проінформовані та навчені.	Низька обізнаність, навчання не проводяться.
Protect	Data Security	PR.DS-01: Чутлива інформація захищена під час зберігання.	Захист залежить від індивідуальних дій користувача.
Protect	Data Security	PR.DS-02: Чутлива інформація захищена під час передачі.	Захист залежить від індивідуальних дій користувача.
Protect	Platform Security	PR.PS-02: Оновлення програмного забезпечення управляються.	Нерегулярно, нецентралізовано.
Protect	Platform Security	PR.PS-03: Конфігурації безпеки встановлені та підтримуються.	Базові, ймовірно, стандартні налаштування на мережевому обладнанні.
Detect	Monitoring	DE.CM-01: Системні логи моніторяться для виявлення аномальної активності.	Моніторинг відсутній або мінімальний.
Respond	Response Planning	RS.RP-01: Процедури реагування на інциденти розроблені та підтримуються.	Відсутні.
Recover	Recovery Planning	RC.RP-01: Процедури відновлення розроблені та підтримуються.	Відсутні формалізовані процедури.
Recover	Data Recovery	RC.RT-01: Резервні копії підтримуються та тестуються.	Регулярність низька, тестування не проводиться.
Recover	Data Recovery	RC.RE-02: Відновлення системи тестується.	Не тестується.

3.3. Розробка цільового профілю за NIST CSF 2.0

Після проведення аналізу поточного стану кібербезпеки та оцінки ризиків для "ЕкоДім Буд", наступним кроком є розробка Цільового Профілю (Target Profile) відповідно до NIST Cybersecurity Framework 2.0. Цільовий Профіль описує бажані результати кібербезпеки, яких організація прагне досягти для управління своїми кіберризиками відповідно до бізнес-цілей.

Приклад Цільового Профілю для "ЕкоДім Буд" (за NIST CSF 2.0)

Цей Цільовий Профіль включає вибрані Підкатегорії з Ядра Фреймворку, які є пріоритетними для "ЕкоДім Буд" для досягнення більш зрілого стану управління кіберризиками.

Функція: Govern (Управління)

Ця функція фокусується на загальному управлінні кібербезпекою в організації. Вона охоплює процеси прийняття рішень, встановлення політик та розподілу відповідальності для забезпечення ефективного функціонування системи безпеки.

Категорія: Risk Management Strategy (Стратегія управління ризиками)

У цій категорії визначаються підходи та принципи, за якими організація управляє своїми кіберризиками.

- GV.RM-01: Політика управління ризиками кібербезпеки визначена та доведена до відома.

Опис: Організація має чітко сформульований документ, який описує її підхід до управління кіберризиками, включаючи цілі, принципи, ролі та відповідальність. Ця політика має бути доступною для всіх співробітників, щоб вони розуміли її зміст.

Обґрунтування для "ЕкоДім Буд": Наявність базової політики є першим і найважливішим кроком до систематичного управління ризиками. Вона демонструє, що керівництво "ЕкоДім Буд" відповідально ставиться до безпеки інформаційних активів і готове інвестувати у її забезпечення. Це є критичною бізнес-ціллю для будь-якої компанії.

Категорія: Organizational Structure (Організаційна структура)

Ця категорія стосується визначення та розподілу ролей і обов'язків у сфері кібербезпеки всередині організації.

- GV.OR-01: Ролі та відповідальність за управління кіберризиками визначені та доведені до відома.

Опис: В організації чітко розподілено, хто за що відповідає в контексті кібербезпеки. Це можуть бути як окремі посади, так і додаткові обов'язки для існуючих працівників. Важливо, щоб кожен співробітник розумів свою роль у забезпеченні кібербезпеки.

Обґрунтування для "ЕкоДім Буд": Для малого та середнього підприємства (МСП) "ЕкоДім Буд" особливо важливо чітко розподілити обов'язки, навіть якщо вони поєднуються з іншими функціями. Це дозволяє знизити ризик невизначеності та гарантує, що всі аспекти кібербезпеки будуть охоплені.

Функція: Identify (Ідентифікація)

Функція "Ідентифікація" спрямована на розуміння та каталогізацію всіх активів організації, а також на виявлення та оцінку потенційних ризиків для них.

Категорія: Asset Management (Управління активами)

Ця категорія включає процеси інвентаризації та класифікації всіх інформаційних активів, що належать організації.

- ID.AM-01: Фізичні пристрої інвентаризовані.

Опис: Створено та підтримується актуальний список усіх фізичних пристроїв, які використовуються в організації (наприклад, комп'ютери, сервери, мережеве обладнання, мобільні пристрої).

Обґрунтування: Основа ефективної безпеки – це знати, що у вас є. Актуальна інвентаризація фізичних пристроїв дозволяє контролювати їхнє використання та забезпечувати належний захист.

- ID.AM-02: Програмне забезпечення інвентаризовано.

Опис: Ведеться облік всього програмного забезпечення, що використовується в організації, включаючи операційні системи, офісні програми, спеціалізоване програмне забезпечення тощо.

Обґрунтування: Важливо знати, яке програмне забезпечення використовується для ефективного управління ліцензіями та, що не менш важливо, для контролю версій та своєчасного встановлення оновлень (що пов'язано з патч-менеджментом).

- ID.AM-05: Інформаційні активи ідентифіковані та класифіковані відповідно до їхньої критичності та чутливості.

Опис: Крім фізичних пристроїв та програмного забезпечення, ідентифіковані та класифіковані дані та інформація (наприклад, дані клієнтів, фінансова інформація, проєктна документація) за ступенем їхньої критичності для бізнесу та чутливості.

Обґрунтування: Ця класифікація дозволяє пріоритизувати зусилля із захисту. Наприклад, дані клієнтів та проєктна документація "ЕкоДім Буд" є високо критичними та чутливими й потребують особливого захисту.

Категорія: Risk Assessment (Оцінка ризиків)

Ця категорія охоплює процеси виявлення та аналізу вразливостей і загроз для активів організації.

- ID.RA-01: Уразливості активів ідентифіковані та задокументовані.

Опис: Регулярно проводиться аналіз систем та програмного забезпечення на наявність відомих вразливостей (слабких місць, які можуть бути використані зловмисниками) та ведеться їхній облік.

Обґрунтування: Систематичне виявлення та облік слабких місць є ключовим для подальшого планування заходів захисту та їх усунення.

- ID.RA-02: Загрози ідентифіковані та задокументовані.

Опис: Визначаються потенційні загрози для інформаційних активів організації, такі як фішинг, шкідливе програмне забезпечення (ransomware), кібератаки тощо.

Обґрунтування: Розуміння того, від яких саме загроз потрібно захищатися, дозволяє "ЕкоДім Буд" розробляти цілеспрямовані заходи безпеки, наприклад, тренінги з протидії фішингу.

Функція: Protect (Захист)

Функція "Захист" містить реалізацію заходів безпеки для обмеження або запобігання впливу кіберінцидентів.

Категорія: Identity and Access Management (Управління ідентифікацією та доступом)

Ця категорія стосується управління доступом користувачів до інформаційних систем та даних.

- PR.AC-01: Фізичний та логічний доступ до активів управляється відповідно до авторизації.

Опис: Забезпечується, що доступ до фізичних об'єктів (наприклад, серверні кімнати) та логічних систем (комп'ютери, мережі, програми) надається лише тим співробітникам, яким це дозволено і необхідно для виконання їхніх обов'язків.

Обґрунтування: Це забезпечує, що доступ мають лише ті, кому він потрібен, що значно знижує ризик несанкціонованого доступу до важливих даних.

- PR.AC-03: Багатофакторна автентифікація (MFA) використовується для доступу до критично важливих систем.

Опис: Для доступу до найбільш важливих систем (наприклад, поштові сервери, фінансові системи, хмарні сховища) вимагається не лише пароль, а й додатковий фактор підтвердження особи (наприклад, код з SMS, додаток-автентифікатор).

Обґрунтування: MFA є одним з найефективніших способів запобігти несанкціонованому доступу та знижує ризик компрометації облікових записів працівників.

Категорія: Awareness Training (Навчання з обізнаності)

Ця категорія стосується навчання співробітників основам кібербезпеки.

- PR.AT-01: Співробітники проінформовані та навчені щодо політик та процедур кібербезпеки та своїх ролей у програмі кібербезпеки організації.

Опис: Проводяться регулярні тренінги та інформування співробітників щодо актуальних загроз, правил безпечної поведінки в інтернеті, використання паролів, розпізнавання фішингу тощо.

Обґрунтування: Це безпосередньо відповідає проблемі низької обізнаності персоналу та ризику фішингу, які є поширеними у МСП. Ефективне навчання знижує ризик людської помилки, яка часто є причиною інцидентів безпеки.

Категорія: Data Security (Безпека даних)

Ця категорія охоплює заходи, спрямовані на захист конфіденційності, цілісності та доступності даних.

• PR.DS-01: Чутлива інформація захищена під час зберігання.

Опис: Впроваджуються заходи для захисту чутливих даних (наприклад, шифрування, обмеження доступу) на всіх носіях, де вони зберігаються.

Обґрунтування: Це забезпечує захист даних клієнтів та проєктної документації, що є життєво важливим для "ЕкоДім Буд" і відповідає як бізнес-цілям, так і вимогам законодавства.

• PR.DS-02: Чутлива інформація захищена під час передачі.

Опис: Використовуються захищені канали зв'язку та протоколи для передачі чутливої інформації як всередині організації, так і за її межами (наприклад, використання VPN, HTTPS).

Обґрунтування: Це гарантує захист даних під час обміну з клієнтами та партнерами, запобігаючи перехопленню та витоку конфіденційної інформації.

Категорія: Platform Security (Безпека платформ)

Ця категорія фокусується на безпеці операційних систем, програмного забезпечення та мережевого обладнання.

• PR.PS-02: Оновлення програмного забезпечення управляються.

Опис: Встановлено процеси для регулярного та своєчасного оновлення операційних систем, програмного забезпечення та прошивок пристроїв.

Обґрунтування: Систематичний патч-менеджмент є критично важливим для усунення відомих вразливостей, які можуть бути використані зловмисниками.

• PR.PS-03: Конфігурації безпеки встановлені та підтримуються для апаратного, програмного забезпечення та сервісів.

Опис: Впроваджені стандартизовані та безпечні конфігурації для всіх систем, програм та сервісів. Це означає вимкнення непотрібних функцій, зміна стандартних паролів, налаштування фаєрволів тощо.

Обґрунтування: Це забезпечує базову безпечну конфігурацію всіх систем та мережевого обладнання, зменшуючи поверхню атаки.

Функція: Detect (Виявлення)

Функція "Виявлення" передбачає моніторинг систем та мереж для ідентифікації можливих інцидентів кібербезпеки.

Категорія: Monitoring (Моніторинг)

Ця категорія стосується збору та аналізу даних для виявлення аномальної активності.

• DE.CM-01: Системні логи моніторяться для виявлення аномальної активності.

Опис: Ведеться збір та аналіз системних журналів (логів) з комп'ютерів, серверів, мережевого обладнання для пошуку ознак незвичайної або підозрілої активності, яка може вказувати на інцидент безпеки.

Обґрунтування: Навіть базовий моніторинг журналів допомагає виявити підозрілу активність на ранній стадії, дозволяючи швидко реагувати на потенційні загрози.

Функція: Respond (Реагування)

Функція "Реагування" охоплює дії, що виконуються після виявлення кіберінциденту, з метою мінімізації його наслідків.

Категорія: Response Planning (Планування реагування)

Ця категорія стосується розробки та підтримки процедур реагування на інциденти.

• RS.RP-01: Процедури реагування на інциденти розроблені та підтримуються.

Опис: Створено чіткий план дій, який визначає кроки, які потрібно виконати у випадку виникнення кіберінциденту (наприклад, зараження вірусом, витік даних, хакерська атака).

Обґрунтування: Наявність простого плану реагування на інциденти (IR-плану) дозволяє "ЕкоДім Буд" здійснювати організовані та ефективні дії під час інциденту, зменшуючи його негативний вплив.

Функція: Recover (Відновлення)

Функція "Відновлення" фокусується на відновленні нормальної роботи після кіберінциденту та забезпеченні безперервності бізнес-процесів.

Категорія: Recovery Planning (Планування відновлення)

Ця категорія стосується розробки та підтримки процедур відновлення бізнес-операцій.

• RC.RP-01: Процедури відновлення розроблені та підтримуються.

Опис: Розроблено та підтримуються в актуальному стані плани щодо відновлення нормальної роботи інформаційних систем та бізнес-процесів після збоїв або інцидентів безпеки.

Обґрунтування: Це забезпечує можливість відновлення бізнес-операцій "ЕкоДім Буд" після збоїв або кібератак, що є ключовою бізнес-ціллю безперервності.

Категорія: Data Recovery (Відновлення даних)

Ця категорія стосується процесів резервного копіювання та відновлення даних.

• RC.RE-01: Резервні копії інформації підтримуються та тестуються.

Опис: Регулярно створюються резервні копії важливої інформації, і ці копії перевіряються на працездатність.

Обґрунтування: Критично важливо для відновлення після втрати даних (наприклад, внаслідок технічного збою) або атаки програм-вимагачів (ransomware).

• RC.RE-02: Відновлення системи тестується.

Опис: Періодично проводяться тестові відновлення систем з резервних копій, щоб переконатися, що процес відновлення працює належним чином.

Обґрунтування: Це перевіряє, що з резервних копій дійсно можна відновитися, гарантуючи ефективність плану відновлення.

Нижче представлено таблицю, що візуалізує Цільовий Профіль "ЕкоДім Буд" за відповідними Підкатегоріями NIST CSF 2.0.

Таблиця 3.2

Базовий профіль "ЕкоДім Буд"

Функція CSF	Категорія CSF	NIST CSF 2.0 Підкатегорія	Цільовий Стан
Govern	Risk Management Strategy	GV.RM-01: Політика управління ризиками кібербезпеки визначена та доведена до відома.	Обрано
Govern	Organizational Structure	GV.OR-01: Ролі та відповідальність за управління кіберризиками визначені та доведені до відома.	Обрано
Identify	Asset Management	ID.AM-01: Фізичні пристрої інвентаризовані.	Обрано
Identify	Asset Management	ID.AM-02: Програмне забезпечення інвентаризовано.	Обрано

продовження таблиці 3.2

Identify	Asset Management	ID.AM-05: Інформаційні активи ідентифіковані та класифіковані.	Обрано
Identify	Risk Assessment	ID.RA-01: Уразливості активів ідентифіковані та задокументовані.	Обрано
Identify	Risk Assessment	ID.RA-02: Загрози ідентифіковані та задокументовані.	Обрано
Protect	Identity and Access Management	PR.AC-01: Фізичний та логічний доступ до активів управляється відповідно до авторизації.	Обрано
Protect	Identity and Access Management	PR.AC-03: Багатофакторна автентифікація (MFA) використовується для доступу до критично важливих систем.	Обрано
Protect	Awareness Training	PR.AT-01: Співробітники проінформовані та навчені щодо політик та процедур кібербезпеки та своєї ролі у програмі кібербезпеки організації.	Обрано
Protect	Data Security	PR.DS-01: Чутлива інформація захищена під час зберігання.	Обрано
Protect	Data Security	PR.DS-02: Чутлива інформація захищена під час передачі.	Обрано
Protect	Platform Security	PR.PS-02: Оновлення програмного забезпечення управляються.	Обрано
Protect	Platform Security	PR.PS-03: Конфігурації безпеки встановлені та підтримуються для апаратного, програмного забезпечення та сервісів.	Обрано
Detect	Monitoring	DE.CM-01: Системні логи моніторяться для виявлення аномальної активності.	Обрано
Respond	Response Planning	RS.RP-01: Процедури реагування на інциденти розроблені та підтримуються.	Обрано
Recover	Recovery Planning	RC.RP-01: Процедури відновлення розроблені та підтримуються.	Обрано
Recover	Data Recovery	RC.RE-01: Резервні копії підтримуються та тестуються.	Обрано
Recover	Data Recovery	RC.RE-02: Відновлення системи тестується.	Обрано

Цей Цільовий Профіль представляє реалістичний набір результатів, які "ЕкоДім Буд" може прагнути досягти протягом певного періоду (наприклад, 1-2 роки). Він не включає всі можливі Підкатегорії CSF 2.0, але зосереджений на тих, що є найбільш важливими для захисту ключових активів, зниження найбільш значущих ризиків та підтримки бізнес-цілей. Порівняння цього Цільового Профілю з Поточним Профілем (поточним станом за цими ж Підкатегоріями) виявить конкретні "розриви", які

необхідно усунути. Наприклад, якщо в Поточному Профілі для PR.AC-03 (MFA) стан "Partial" (не використовується), а в Цільовому Профілі ми її вибрали, то "розривом" є відсутність MFA, і її впровадження стане завданням у плані дій.

Таблиця 3.3

Порівняння Цільового Профілю з Поточним Профілем (поточним станом за цими ж Підкатегоріями)

Функція CSF	Категорія CSF	NIST CSF 2.0 Підкатегорія	Поточний Стан ('ЕкоДім Буд')	Цільовий Стан	Прогалина / Статус
Govern	Risk Management Strategy	GV.RM-01: Політика управління ризиками кібербезпеки визначена та доведена до відома.	Відсутня формалізована політика.	Обрано	Немає формалізованої політики управління ризиками.
Govern	Organizational Structure	GV.OR-01: Ролі та відповідальність за управління кіберризиками визначені та доведені до відома.	Ролі не чітко визначені, відповідальність не формалізована.	Обрано	Відсутнє чітке визначення ролей та відповідальності за кіберризики.
Identify	Asset Management	ID.AM-01: Фізичні пристрої інвентаризовані.	Є базовий, ймовірно, неповний список.	Обрано	Інвентаризація фізичних активів неповна або неактуальна.
Identify	Asset Management	ID.AM-02: Програмне забезпечення інвентаризовано.	Немає системної інвентаризації ПЗ.	Обрано	Відсутня системна інвентаризація програмного забезпечення.

продовження таблиці 3.3

Identify	Asset Management	ID.AM-05: Інформаційні активи ідентифіковані та класифіковані.	Немає класифікації даних.	Обрано	Не проведена ідентифікація та класифікація інформаційних активів.
Identify	Risk Assessment	ID.RA-01: Уразливості активів ідентифіковані та задокументовані.	Уразливості відомі на інтуїтивному рівні (старе ПЗ).	Обрано	Відсутній формалізований процес ідентифікації та документування уразливостей.
Identify	Risk Assessment	ID.RA-02: Загрози ідентифіковані та задокументовані.	Базове розуміння загроз.	Обрано	Не проведено систематичну ідентифікацію та документування актуальних загроз.
Protect	Identity and Access Management	PR.AC-01: Фізичний та логічний доступ до активів управляється відповідно до авторизації.	Немає формалізованих правил доступу.	Обрано	Відсутні формалізовані правила та процедури управління доступом.
Protect	Identity and Access Management	PR.AC-03: Багатофакторна автентифікація (MFA) використовується для доступу до критично важливих систем.	Не використовується.	Обрано	Не впроваджено багатофакторну автентифікацію для критично важливих систем.

продовження таблиці 3.3

Protect	Awareness Training	PR.AT-01: Співробітники проінформовані та навчені щодо політик та процедур кібербезпеки та своїх ролей у програмі кібербезпеки організації.	Низька обізнаність, навчання не проводилося.	Обрано	Не проведено навчання персоналу з обізнаності з кібербезпеки.
Protect	Data Security	PR.DS-01: Чутлива інформація захищена під час зберігання.	Захист залежить від індивідуальних дій користувачів.	Обрано	Немає системного захисту чутливої інформації при зберіганні.
Protect	Data Security	PR.DS-02: Чутлива інформація захищена під час передачі.	Захист залежить від індивідуальних дій користувачів.	Обрано	Немає системного захисту чутливої інформації при передачі.
Protect	Platform Security	PR.PS-02: Оновлення програмного забезпечення управляються.	Нерегулярно, нецентралізовано.	Обрано	Відсутній систематичний процес управління оновленнями ПЗ.
Protect	Platform Security	PR.PS-03: Конфігурації безпеки встановлені та підтримуються для апаратного,програмного забезпечення.	Базові, ймовірно, стандартні налаштування.	Обрано	Не встановлені та не підтримуються безпечні конфігурації.

продовження таблиці 3.3

Detect	Monitoring	DE.CM-01: Системні логи моніторяться для виявлення аномальної активності.	Моніторинг відсутній або мінімальний.	Обрано	Відсутній базовий моніторинг системних логів.
Respond	Response Planning	RS.RP-01: Процедури реагування на інциденти розроблені та підтримуються.	Відсутні.	Обрано	Відсутній план та процедури реагування на інциденти.
Recover	Recovery Planning	RC.RP-01: Процедури відновлення розроблені та підтримуються.	Відсутні формалізовані процедури.	Обрано	Відсутні формалізовані процедури планування відновлення.
Recover	Data Recovery	RC.RE-01: Резервні копії підтримуються та тестуються.	Регулярність низька, тестування не проводиться.	Обрано	Резервне копіювання нерегулярне та не тестується.
Recover	Data Recovery	RC.RE-02: Відновлення системи тестується.	Не тестується.	Обрано	Процес відновлення з резервних копій не тестується.

Ця таблиця наочно демонструє, що для всіх обраних в Цільовому Профілі Підкатегорій, поточний стан "ЕкоДім Буд" суттєво відстає від бажаного. Кожен рядок, де "Поточний Стан" не відповідає "Цільовому Стану" (який для цього прикладу завжди "Обрано"), по суті, є виявленою прогалиною. Ці прогалини є

основою для розробки завдань у плані впровадження, спрямованих на їх усунення та досягнення бажаного рівня кібербезпеки.

3.4. Реальний план дій для досягнення цільового профілю

На основі аналізу поточного стану, виявлених розривів та розробленого Цільового Профілю за NIST CSF 2.0, ми тепер можемо створити реалістичний план дій для "ЕкоДім Буд". Цей план є покроковою інструкцією, яка допоможе підприємству систематично підвищувати свій рівень кібербезпеки, рухаючись до бажаного стану. План враховує типові для МСП обмеження ресурсів і зосереджений на пріоритетних заходах.

Мета плану дій:

Систематичне усунення розривів між Поточним та Цільовим Профілями "ЕкоДім Буд" за NIST CSF 2.0 шляхом реалізації конкретних, пріоритизованих завдань у реалістичні терміни.

Принципи пріоритизації:

Завдання у плані дій пріоритизовані, виходячи з:

1. Високого ризику: Заходи, що спрямовані на зниження найбільш ймовірних загроз з високим потенційним впливом (наприклад, захист від програм-вимагачів та фішингу).
2. Бізнес-критичності: Заходи, що захищають найважливіші для бізнесу активи та процеси (наприклад, дані клієнтів, доступність систем).
3. Швидких перемог: Заходи, які можна реалізувати відносно швидко та з невеликими витратами, але які дають значний ефект для безпеки.
4. Залежностей: Виконання одних завдань може бути необхідною умовою для початку інших.

План дій (орієнтовний період: 6-12 місяців)

План дій згруповано за логічними ініціативами, які охоплюють кілька функцій CSF та пов'язані між собою.

Крок 1: Підвищення базової гігієни кібербезпеки (місяці 1-3)

Ця ініціатива зосереджена на швидких перемогах та фундаментальних заходах, які мають значний вплив на загальний рівень безпеки.

Завдання 1.1: Повна інвентаризація активів.

Цільовий Профіль (Підкатегорії): ID.AM-01 (Фізичні пристрої інвентаризовані), ID.AM-02 (Програмне забезпечення інвентаризовано).

Розрив: Відсутність повної та актуальної інвентаризації.

Ключові кроки: Скласти список усіх робочих станцій, ноутбуків, мобільних пристроїв, серверів та основного програмного забезпечення (включаючи версії). Використовувати електронну таблицю або простий інструмент.

Відповідальний: IT-менеджер.

Термін: 1 місяць.

Результат: Актуальний список усіх IT-активів.

Завдання 1.2: Впровадження базової політики паролів та MFA.

Цільовий Профіль (Підкатегорії): PR.AC-01 (Доступ управляється відповідно до авторизації), PR.AC-03 (MFA використовується для критично важливих систем).

Розрив: Слабка політика паролів, відсутність MFA.

Ключові кроки: Розробити просту політику, що вимагає сильних унікальних паролів. Впровадити MFA для доступу до Google Workspace, CRM та облікової системи. Навчити співробітників використовувати MFA.

Відповідальний: IT-менеджер.

Термін: 2 місяці.

Результат: Затверджена політика паролів, увімкнена MFA для ключових сервісів.

Завдання 1.3: Встановлення та налаштування антивірусу та автоматичних оновлень.

Цільовий Профіль (Підкатегорії): PR.PS-02 (Оновлення ПЗ управляються), ID.RA-01 (Уразливості ідентифіковані).

Розрив: Нерегулярне оновлення ПЗ, нецентралізований антивірус.

Ключові кроки: Вибрати та встановити централізоване антивірусне/антишкідливе рішення на всі пристрої. Налаштувати автоматичні оновлення для ОС та основного ПЗ.

Відповідальний: IT-менеджер.

Термін: 1.5 місяці.

Результат: Встановлений антивірус, налаштовані автоматичні оновлення.

Завдання 1.4: Безпечна конфігурація мережевого обладнання.

Цільовий Профіль (Підкатегорії): PR.PS-03 (Конфігурації безпеки встановлені).

Розрив: Стандартні адміністративні паролі на роутері.

Ключові кроки: Змінити стандартні адміністративні логіни/паролі на роутері та інших мережевих пристроях. Налаштувати WPA3 для Wi-Fi. Створити окрему гостьову Wi-Fi мережу.

Відповідальний: IT-менеджер.

Термін: 0.5 місяці.

Результат: Захищене мережеве обладнання.

Таблиця 3.4

Підвищення базової гігієни кібербезпеки

Завдання	Відповідальний	Строк (Орієнтовно)	Бюджет (Орієнтовна складова витрат)
1.1. Повна інвентаризація фізичних пристроїв та ПЗ.	IT-менеджер	1 місяць	Внутрішні ресурси (зусилля персоналу), можлива вартість інструментів інвентаризації.
1.2. Розробка та затвердження базової політики паролів.	IT-менеджер, Керівництво	0.5 місяці	Внутрішні ресурси (зусилля персоналу), можливі консультаційні послуги.

продовження таблиці 3.4

1.3. Впровадження MFA для Google Workspace та інших ключових сервісів.	IT-менеджер	1.5 місяці	Вартість MFA-рішення (ліцензії), Внутрішні ресурси (зусилля персоналу).
1.4. Безпечна конфігурація мережевого обладнання (роутер, Wi-Fi).	IT-менеджер	0.5 місяці	Внутрішні ресурси (зусилля персоналу).
1.5. Встановлення централізованого антивірусу/антишкідливого ПЗ.	IT-менеджер	1 місяць	Вартість ліцензій на ПЗ, Внутрішні ресурси (зусилля персоналу).

Крок 2: Захист даних та забезпечення відновлення (місяці 2-4)

Ця ініціатива фокусується на найцінніших активах – даних – та забезпеченні можливості відновлення після інцидентів.

Завдання 2.1: Впровадження надійного резервного копіювання.

Цільовий Профіль (Підкатегорії): RC.RE-01 (Резервні копії підтримуються та тестуються), RC.RE-02 (Відновлення системи тестується).

Розрив: Обмежене та нетестоване резервне копіювання.

Ключові кроки: Вибрати та впровадити рішення для щоденного автоматичного резервного копіювання критично важливих даних з файлового сервера та хмарних сервісів до зовнішнього хмарного сховища. Розробити просту процедуру тестування відновлення даних (наприклад, раз на місяць).

Відповідальний: IT-менеджер.

Термін: 2 місяці.

Результат: Налаштоване щоденне резервне копіювання, процедура тестування відновлення.

Завдання 2.2: Захист чутливих даних при зберіганні та передачі.

Цільовий Профіль (Підкатегорії): PR.DS-01 (Чутлива інформація захищена під час зберігання), PR.DS-02 (Чутлива інформація захищена під час передачі).

Розрив: Немає чітких правил захисту чутливих даних.

Ключові кроки: Визначити, які дані є чутливими (дані клієнтів, фінансова інформація, проєкти). Навчити співробітників безпечно зберігати та передавати ці дані (наприклад, використовувати шифровані папки, захищені канали передачі даних).

Відповідальний: IT-менеджер (за участі керівництва).

Термін: 1 місяць.

Результат: Визначені чутливі дані, розроблені та доведені до відома правила їх обробки.

Таблиця 3.5

Захист даних та забезпечення відновлення

Завдання	Відповідальний	Строк (Орієнтовно)	Бюджет (Орієнтовна складова витрат)
2.1. Впровадження надійного резервного копіювання (хмара/офсайт).	IT-менеджер	2 місяці	Вартість хмарного сховища, вартість ПЗ для резервного копіювання, Внутрішні ресурси (зусилля персоналу).
2.2. Розробка простої процедури тестування відновлення даних.	IT-менеджер	0.5 місяці	Внутрішні ресурси (зусилля персоналу).
2.3. Визначення та класифікація чутливих даних.	IT-менеджер, Керівництво	0.5 місяці	Внутрішні ресурси (зусилля персоналу).
2.4. Розробка базових правил обробки чутливих даних (зберігання, передача).	IT-менеджер, Керівництво	0.5 місяці	Внутрішні ресурси (зусилля персоналу).

Крок 3: Розвиток культури безпеки та реагування (місяці 3-6)

Ця ініціатива зосереджена на людському факторі та готовності до інцидентів.

Завдання 3.1: Проведення тренінгу з обізнаності з кібербезпеки.

Цільовий Профіль (Підкатегорії): PR.AT-01 (Співробітники проінформовані та навчені).

Розрив: Низька обізнаність персоналу.

Ключові кроки: Розробити або придбати прості навчальні матеріали (презентація, брошура). Провести інтерактивний тренінг для всіх співробітників, зосередившись на фішингу, паролях, використанні Інтернету та електронної пошти.

Відповідальний: Менеджер з персоналу (за підтримки IT-менеджера).

Термін: 1 місяць.

Результат: Співробітники пройшли базовий тренінг.

Завдання 3.2: Розробка простого плану реагування на інциденти.

Цільовий Профіль (Підкатегорії): RS.RP-01 (Процедури реагування на інциденти розроблені).

Розрив: Відсутність IR-плану.

Ключові кроки: Створити базовий документ (чек-лист) з описом перших кроків при виявленні інциденту (з ким зв'язатися, що відключити). Включити контактні дані зовнішньої IT-підтримки.

Відповідальний: IT-менеджер (за участі керівництва).

Термін: 1 місяць.

Результат: Базовий план реагування на інциденти задокументований.

Таблиця 3.6

Крок 3: Розвиток культури безпеки та реагування

Завдання	Відповідальний	Строк (Орієнтовно)	Бюджет (Орієнтовна складова витрат)
3.1. Розробка матеріалів для тренінгу з обізнаності з кібербезпеки.	Менеджер з персоналу, IT-менеджер	1 місяць	Внутрішні ресурси (зусилля персоналу), можлива вартість готових навчальних матеріалів.
3.2. Проведення початкового тренінгу з обізнаності для всіх співробітників.	Менеджер з персоналу	0.5 місяці	Внутрішні ресурси (зусилля персоналу співробітників під час тренінгу).
3.3. Розробка базового плану реагування на інциденти (чек-лист).	IT-менеджер, Керівництво	1 місяць	Внутрішні ресурси (зусилля персоналу), можливі консультаційні послуги.

продовження таблиці 3.6

3.4. Ознайомлення ключового персоналу з планом реагування на інциденти.	IT-менеджер	0.5 місяці	Внутрішні ресурси (зусилля персоналу).

Крок 4: Вдосконалення та моніторинг (місяці 6-12 та постійно)

Ця ініціатива включає заходи, що вимагають постійних зусиль та інтеграцію моніторингу.

Завдання 4.1: Впровадження базового моніторингу та аналізу логів.

Цільовий Профіль (Підкатегорії): DE.CM-01 (Системні логи моніторяться), ID.RA-01 (Уразливості ідентифіковані).

Розрив: Відсутність моніторингу та аналізу логів.

Ключові кроки: Налаштувати збір логів з критично важливих систем. Використовувати доступні інструменти для базового перегляду логів та пошуку аномалій. Проводити періодичне сканування на наявність уразливостей (можна використовувати безкоштовні сканери).

Відповідальний: IT-менеджер.

Термін: 3 місяці для налаштування, далі постійно.

Результат: Налаштований базовий моніторинг, періодична перевірка на уразливості.

Завдання 4.2: Регулярний перегляд плану дій та оцінка прогресу.

Цільовий Профіль (Підкатегорії): GV.RM-01 (Політика управління ризиками визначена).

Розрив: Необхідність підтримки процесу.

Ключові кроки: Раз на квартал проводити зустрічі за участю керівництва та IT-менеджера для оцінки виконання плану дій, перегляду виявлених ризиків та коригування плану за необхідності.

Відповідальний: Керівництво, IT-менеджер.

Термін: Постійно (щоквартально).

Результат: Регулярний перегляд, актуальний план.

Таблиця 3.7

Крок 4: Вдосконалення та моніторинг

Завдання	Відповідальний	Строк (Орієнтовно)	Бюджет (Орієнтовна складова витрат)
4.1. Налаштування базового моніторингу системних логів.	IT-менеджер	1 місяць	Вартість інструментів моніторингу (можуть бути безкоштовні), Внутрішні ресурси.
4.2. Впровадження процесу систематичного управління оновленнями ПЗ.	IT-менеджер	Постійно (настроюється впродовж 1 міс.)	Внутрішні ресурси (зусилля персоналу).
4.3. Проведення періодичного сканування на наявність уразливостей.	IT-менеджер	Постійно (настроюється впродовж 0.5 міс.)	Вартість інструментів сканування (можуть бути безкоштовні), Внутрішні ресурси (зусилля персоналу).

Постійні активності (після перших 6-12 місяців та надалі):

- Щоденне/Щотижневе резервне копіювання та періодичне тестування відновлення.
- Постійний патч-менеджмент.
- Регулярний моніторинг логів та сповіщень.
- Періодичні нагадування співробітникам про правила безпеки та, можливо, щорічні оновлюючі тренінги.
- Регулярний перегляд прав доступу співробітників.
- Актуалізація інвентаризації активів.
- Щоквартальний перегляд ризиків та плану дій.

Цей "реальний" план дій для "ЕкоДім Буд", заснований на NIST CSF 2.0, є гнучким і може бути адаптований відповідно до конкретного прогресу та мінливих умов. Він надає МСП структурований шлях для поступового, але значного підвищення рівня своєї кібербезпеки, переходячи від реактивного до більш проактивного та систематичного підходу.

Представлення плану дій шляхом надання конкретних варіантів. Доповнимо план впровадження для "ЕкоДім Буд" конкретними прикладами інструментів (як

безкоштовних, так і платних), які можуть допомогти реалізувати необхідні дії для досягнення Цільового Профілю за NIST CSF 2.0.

Важливо пам'ятати, що це лише приклади, і вибір конкретних рішень має базуватися на детальнішому аналізі потреб, бюджету та технічної експертизи "ЕкоДім Буд". Для МСП часто оптимальним є поєднання безкоштовних рішень для базових потреб та платних сервісів для більш критичних функцій.

Ось пропозиції інструментів для ключових завдань плану дій:

1. Інвентаризація активів (ID.AM-01, ID.AM-02)

Завдання: Створити повну та актуальну інвентаризацію фізичних пристроїв та програмного забезпечення.

Безкоштовні засоби:

Електронні таблиці (Google Sheets, Microsoft Excel Online): Простий ручний облік.

Spiceworks Inventory: Безкоштовний інструмент для сканування мережі та збору інформації про пристрої та ПЗ. Може бути надмірним для дуже маленьких МСП, але корисний при зростанні.

Платні засоби:

ManageEngine AssetExplorer: Платний інструмент управління IT-активами з розширеними функціями.

Lansweeper: Платне рішення для інвентаризації активів з широкими можливостями сканування.

2. Впровадження MFA (PR.AC-03)

Завдання: Впровадити MFA для критично важливих систем (Google Workspace, CRM, облікова система).

Безкоштовні засоби:

Google Authenticator, Microsoft Authenticator: Безкоштовні мобільні додатки для генерації одноразових кодів, які інтегруються з багатьма сервісами (включаючи Google Workspace).

Функції провайдерів хмарних сервісів: Багато хмарних сервісів (Google Workspace, Microsoft 365, більшість CRM) мають вбудовані безкоштовні опції MFA.

Платні засоби:

Duo Security (частина Cisco), Okta, Microsoft Azure AD Premium: Комплексні рішення для управління ідентифікацією та доступом, що включають розширені можливості MFA, єдиного входу (SSO) тощо.

3. Політика паролів та управління доступом (PR.AC-01)

Завдання: Розробити політику паролів, впровадити базові правила управління доступом.

Безкоштовні засоби:

Документ політики: Просто створити та поширити документ з вимогами до паролів (довжина, складність, термін дії) та правилами доступу.

Функції ОС та сервісів: Використання вбудованих політик паролів у Windows Server (для доменних користувачів), налаштування вимог до паролів в хмарних сервісах.

Менеджери паролів (напр., LastPass, Bitwarden мають безкоштовні персональні версії): Можуть допомогти співробітникам безпечно генерувати та зберігати унікальні паролі (хоча для бізнесу часто потрібна платна версія).

Платні засоби:

Менеджери паролів для бізнесу (LastPass Enterprise, 1Password Business): Централізоване управління паролями для всіх співробітників.

Рішення для управління ідентифікацією та доступом (Okta, Azure AD): Надають розширені можливості управління користувачами, групами та дозволами.

4. Патч-менеджмент та оновлення (PR.PS-02)

Завдання: Впровадити систематичний процес управління оновленнями ПЗ.

Безкоштовні засоби:

Функції автоматичного оновлення в ОС та додатках: Налаштувати автоматичні оновлення для Windows Update, оновлень браузерів, Adobe Reader тощо.

WSUS (Windows Server Update Services): Безкоштовний інструмент від Microsoft для централізованого управління оновленнями Windows у локальній мережі (потребує сервера).

Платні засоби:

ManageEngine Patch Manager Plus, SolarWinds Patch Manager: Комплексні рішення для автоматизації процесу патч-менеджменту на різних ОС та додатках.

5. Антивірусне та антишкідливе ПЗ (Пов'язано з PR.PS-03, PR.AT-01)

Завдання: Встановити та підтримувати актуальний антивірус на всіх пристроях.

Безкоштовні засоби:

Microsoft Defender (вбудовано в Windows): Хороший базовий рівень захисту для Windows.

Avast Free Antivirus, AVG AntiVirus Free (перевіряйте умови використання для бізнесу): Популярні безкоштовні антивіруси, але часто з обмеженнями для комерційного використання та рекламою.

Платні засоби:

ESET Endpoint Security, Kaspersky Endpoint Security, Bitdefender GravityZone Business Security: Надійні комплексні антивірусні рішення корпоративного класу з централізованим управлінням.

6. Безпечна конфігурація (PR.PS-03)

Завдання: Встановити та підтримувати безпечні конфігурації систем та обладнання.

Безкоштовні засоби:

Настанови CIS Benchmarks: Безкоштовні рекомендації щодо безпечної конфігурації для різних ОС, додатків та мережевого обладнання.

Вбудовані функції безпеки ОС: Використання групових політик у Windows, налаштування брандмауера Windows Defender.

Платні засоби:

Інструменти управління конфігурацією (напр., Microsoft Endpoint Manager): Дозволяють централізовано застосовувати та контролювати безпекові налаштування на пристроях.

Рішення для сканування відповідності стандартам (частина деяких Vulnerability Management Tools).

7. Захист даних (PR.DS-01, PR.DS-02)

Завдання: Захистити чутливі дані при зберіганні та передачі.

Безкоштовні засоби:

Шифрування дисків (BitLocker в Windows Pro/Enterprise, FileVault в macOS): Вбудовані функції для шифрування даних на локальних дисках.

Шифрування файлів/папок (вбудовано в ОС): Базове шифрування окремих файлів.

Захищені протоколи (HTTPS, SFTP): Використання захищених протоколів для передачі даних (перевіряйте, чи підтримуються вашими сервісами).

Платні засоби:

Комплексні рішення для шифрування даних (VeraCrypt - безкоштовний, але складніший; платні комерційні рішення).

Рішення для захищеного обміну файлами (Sync.com, Tresorit): Хмарні сервіси з сильним фокусом на шифруванні та безпеці.

8. Резервне копіювання та відновлення (RC.RE-01, RC.RE-02)

Завдання: Впровадити регулярне тестоване резервне копіювання та процедури відновлення.

Безкоштовні засоби:

Вбудовані засоби резервного копіювання ОС: Windows Backup and Restore, Time Machine в macOS.

Безкоштовні хмарні сховища (Google Drive, Dropbox Basic): Можна використовувати для зберігання копій критично важливих файлів (звертайте увагу на обсяг та умови).

Duplicati, Veeam Agent for Microsoft Windows (Free): Безкоштовне ПЗ для резервного копіювання.

Платні засоби:

Veeam Backup & Replication, Acronis Cyber Protect, Carbonite: Комплексні рішення для резервного копіювання та відновлення з широкими можливостями та підтримкою.

Платні хмарні сховища, спеціалізовані для резервного копіювання (Backblaze Business, Wasabi Cloud Storage).

9. Навчання з обізнаності (PR.AT-01)

Завдання: Провести тренінг з обізнаності персоналу.

Безкоштовні засоби:

Матеріали від NIST, CIS, ENISA: Багато організацій надають безкоштовні ресурси (брошури, презентації) з обізнаності з кібербезпеки.

Відеоуроки на YouTube: Численні освітні відеоролики.

Симуляції фішингу (безкоштовні пробні версії або обмежені безкоштовні інструменти).

Платні засоби:

Спеціалізовані платформи для навчання з обізнаності (KnowBe4, Proofpoint Security Awareness Training): Надають інтерактивні курси, симуляції фішингу, звітування.

10. Планування реагування на інциденти (RS.RP-01)

Завдання: Розробити базовий план реагування на інциденти.

Безкоштовні засоби:

Шаблони планів від NIST, SANS, CIS: Доступні безкоштовні шаблони, які можна адаптувати.

Простий документ/чек-лист: Створити документ у Google Docs або Word.

Платні засоби:

Консультаційні послуги: Залучення спеціалістів для допомоги у розробці плану, адаптованого до специфіки бізнесу.

11. Базовий моніторинг та аналіз логів (DE.CM-01)

Завдання: Налаштувати базовий моніторинг системних логів.

Безкоштовні засоби:

Вбудовані засоби перегляду логів в ОС (Event Viewer в Windows).

Прості скрипти: Написання скриптів для автоматичного збору та базового аналізу логів (потребує технічних навичок).

Syslog-сервер (напр., rsyslog на Linux): Для централізованого збору логів з різних пристроїв (потребує технічних навичок та сервера).

Платні засоби:

Базові SIEM-системи або Log Management інструменти (Splunk, ELK Stack - має безкоштовні компоненти, але складний; LogRhythm): Надають розширені можливості збору, аналізу та кореляції логів.

Керовані послуги моніторингу (Managed Detection and Response - MDR): Зовнішні провайдери, які здійснюють моніторинг та реагування віддалено (часто дорожче, але знімає навантаження з внутрішніх ресурсів).

12. Сканування уразливостей (ID.RA-01)

Завдання: Проводити періодичне сканування на наявність уразливостей.

Безкоштовні засоби:

OpenVAS (частина GVM): Потужний сканер уразливостей (потребує значних технічних навичок для встановлення та налаштування).

Nmap: Інструмент для сканування мережі та виявлення служб, може допомогти виявити деякі базові уразливості (потребує технічних навичок).

Онлайн-сканери: Обмежені безкоштовні онлайн-сервіси для сканування зовнішнього периметра.

Платні засоби:

Tenable Nessus, Rapid7 Nexpose, Qualys: Професійні сканери уразливостей з широкими можливостями та зручним інтерфейсом.

При виборі інструментів для "ЕкоДім Буд" слід шукати баланс між необхідним рівнем безпеки, простотою використання та вартістю. Часто варто почати з безкоштовних або найдоступніших рішень для базових завдань і поступово переходити до платних, більш функціональних інструментів в міру зростання бізнесу та підвищення рівня зрілості кібербезпеки.

3.5. Система моніторингу та оцінка успішності (KPI)

Впровадження плану дій є значним кроком до покращення кібербезпеки, але сама імплементація не є кінцевою точкою. Для "ЕкоДім Буд", як і для будь-якої іншої організації, критично важливо встановити систему моніторингу та оцінки успішності впроваджених заходів. Це дозволить зрозуміти, чи досягаються поставлені цілі, чи є

впроваджені заходи ефективними у зниженні ризиків та де є можливості для подальшого вдосконалення. Цей процес є невід'ємною частиною функцій Govern (Управління) та Detect (Виявлення), а також циклу постійного покращення в NIST CSF 2.0.

Важливість моніторингу та оцінки для МСП:

Для "ЕкоДім Буд" з їхніми обмеженими ресурсами, ефективний моніторинг та оцінка є життєво важливими для:

- Підтвердження ефективності інвестицій: Переконатися, що час та кошти, витрачені на безпеку, приносять реальну користь.
- Виявлення нових або неочікуваних ризиків: Моніторинг може допомогти виявити активність, яка свідчить про нові загрози або уразливості.
- Підтримки актуальності програми безпеки: Ландшафт загроз постійно змінюється, і система моніторингу допомагає адаптуватися до цих змін.
- Прийняття обґрунтованих рішень: Дані від моніторингу та KPI є основою для коригування плану дій та визначення пріоритетів на майбутнє.

Встановлення базової системи моніторингу та оцінки для "ЕкоДім Буд":

"ЕкоДім Буд" може створити просту, але ефективну систему моніторингу та оцінки, зосередившись на ключових показниках та регулярних перевірках.

1. Визначення ключових KPI: На основі обговорених раніше критеріїв, "ЕкоДім Буд" може зосередитися на відстеженні наступних KPI:

1.1.Час виявлення та реагування на інциденти: Навіть без складної SIEM-системи, можна фіксувати час виявлення підозрілих подій (наприклад, повідомлення співробітника про підозрілий лист, спрацювання антивірусу) та час, необхідний для їх усунення. Ведення простого журналу інцидентів (дата, час виявлення, опис, час усунення) допоможе збирати ці дані.

1.2.Кількість інцидентів: Вести облік усіх зареєстрованих інцидентів кібербезпеки, класифікуючи їх за типом (фішинг, шкідливе ПЗ тощо). Аналіз динаміки кількості та типів інцидентів може вказати на ефективність певних захисних заходів або появу нових загроз.

1.3.Рівень підготовки персоналу: Відстежувати відсоток співробітників, які пройшли навчання. Періодично проводити прості симуляції фішингу та фіксувати відсоток успішних ідентифікацій. Відстежувати кількість повідомлень співробітників про підозрілі події.

2. Відстеження прогресу виконання плану дій: Регулярно (наприклад, щомісяця або щокварталу) оцінювати, які завдання з плану дій виконано, які перебувають у процесі, а які відстають від графіка. Це показує прогрес у досягненні Цільового Профілю.

3. Моніторинг виконання ключових завдань: Для деяких критичних завдань можна відстежувати конкретні метрики:

3.1.Патч-менеджмент: Відсоток систем, на яких встановлено останні оновлення безпеки.

3.2.Резервне копіювання: Частота створення резервних копій (наприклад, щоденно), успішність тестів відновлення (так/ні).

3.3.MFA: Відсоток критично важливих облікових записів з увімкненою MFA.

3.4.Моніторинг логів: Регулярність перегляду логів (наприклад, раз на тиждень переглядати логи брандмауера та сервера).

4. Регулярні перевірки та оцінка:

4.1.Щоквартальні зустрічі керівництва та IT-менеджера: Використовувати ці зустрічі для перегляду зібраних даних (KPI, прогрес плану), обговорення виявлених проблем, аналізу нових ризиків та прийняття рішень щодо подальших дій та коригування плану.

4.2.Проведення періодичної самооцінки за NIST CSF 2.0: Раз на певний період (наприклад, щорічно) повторно оцінювати свій "Поточний Профіль" за NIST CSF 2.0, щоб побачити, як змінився їхній стан порівняно з попередньою оцінкою та наскільки вони наблизилися до свого Цільового Профілю.

Використання результатів моніторингу та оцінки:

Зібрані дані та результати оцінки повинні використовуватися для:

- Звітування керівництву: Надання чіткої інформації про стан кібербезпеки, виявлені ризики та результати впроваджених заходів.

- Визначення областей для покращення: Ідентифікація конкретних слабких місць, які потребують додаткової уваги та ресурсів.
- Оновлення оцінки ризиків: Включення інформації про інциденти та виявлені уразливості до процесу оцінки ризиків.
- Коригування плану дій: Внесення змін до плану впровадження на основі отриманого досвіду та нових пріоритетів.
- Підтримки циклу постійного покращення: Використання моніторингу та оцінки як рушійної сили для безперервного вдосконалення програми кібербезпеки.

Для "ЕкоДім Буд" важливо створити систему моніторингу та оцінки, яка є реалістичною та не вимагає надмірних ресурсів. Навіть прості ручні процеси та використання доступних інструментів можуть надати цінну інформацію для управління кіберризиками та підвищення рівня безпеки. Ключ – у послідовності та використанні отриманих даних для прийняття рішень.

Таблиця 3.8

Критерій ефективності/KPI

Критерій ефективності / KPI	Що вимірює	Як вимірювати	Частота моніторингу / збору даних
Час виявлення та реагування на інциденти	Швидкість ідентифікації та усунення інцидентів.	Фіксація часу в журналі інцидентів (від виявлення до усунення). Розрахунок середнього (якщо можливо).	Вимірювання для кожного інциденту. Узагальнення щомісячно/щоквартально.
Кількість інцидентів	Частота подій безпеки.	Підрахунок записів у журналі інцидентів за період. Класифікація за типом.	Узагальнення щомісячно/щоквартально.
Рівень підготовки персоналу	Обізнаність співробітників з питань безпеки.	Відсоток співробітників, що пройшли навчання. Результати симуляцій фішингу. Кількість повідомлень про підозри.	Відстеження після тренінгів/симуляцій. Узагальнення щоквартально/півріччя.
Виконання плану дій	Прогрес у впровадженні заходів безпеки.	Відсоток виконаних завдань плану.	Узагальнення щомісячно/щоквартально.

Продовження таблиці 3.8

Успішність тестування відновлення резервних копій	Надійність процесу резервного копіювання та відновлення.	Результат тесту (успішно/не успішно).	Після кожного тесту (напр., щомісячно).
Відсоток систем з оновленнями/MFA	Стан реалізації конкретних захисних заходів.	Підрахунок систем/користувачів, що відповідають критерію.	Періодично (напр., щоквартально).

Висновок до розділу 3

Висновок практичної частини полягає в тому, що навіть для малого підприємства з обмеженими ресурсами, систематичний та структурований підхід до кібербезпеки є можливим та надзвичайно важливим. Використання фреймворку, такого як NIST CSF 2.0, надає необхідну структуру, допомагає зосередитися на пріоритетах (на основі ризиків) та перетворити абстрактні концепції безпеки на конкретні, дієві кроки.

Цей практичний приклад демонструє, що впровадження цільового профілю безпеки – це не одноразовий проєкт, а ітеративний процес, який починається з розуміння поточного стану та ризиків, визначення бажаного стану, планування дій, їх реалізації та, найголовніше, постійного моніторингу та оцінки для забезпечення ефективності та адаптації до мінливого ландшафту загроз. Успіх досягається через послідовні, реалістичні кроки та інтеграцію безпекових практик у повсякденну діяльність підприємства.

ВИСНОВОК

У підсумку проведене дослідження демонструє, що успішна організація кібербезпеки в умовах малого та середнього бізнесу — це не просто набір «галочок» у технічних рішеннях, а цілісний, багаторівневий процес, який об’єднує стратегію, практичні заходи та безперервний зворотний зв’язок.

Перш за все, теоретичний базис (Розділ 1) заклав основу, де ми чітко розмежували «інформаційну безпеку» та «кібербезпеку», відокремили три ключові принципи CIA (конфіденційність, цілісність, доступність) і відобразили специфіку МСП як суб’єкта з обмеженими ресурсами та підвищеною вразливістю. Далі ми проаналізували основні типи загроз від фішингу до ransomware, DDoS та інсайдерських атак, і показали, чому саме людський фактор і прості технологічні недоліки найчастіше стають «точками входу» для зловмисників. Окремий огляд міжнародних стандартів (ISO/IEC 27001, COBIT, CIS Controls, NIST CSF 2.0) дав можливість порівняти підходи «згори вниз» і «знизу вгору» від комплексних систем управління безпекою до пріоритетних «швидких перемог». І, нарешті, перелік найкращих практик технологічних, організаційних і пов’язаних із людиною показав, як усі ці концепти можна втілити в прості, але ефективні кроки.

У другому розділі ми занурилися в глибший аналіз: порівняли методології за охопленням функцій (включно з новою *Govern* у NIST CSF 2.0), за вартістю та ресурсомісткістю, складністю впровадження і здатністю масштабуватися разом із розвитком МСП. Виявилося, що універсальних рецептів не існує: кожен бізнес має обирати компроміс між швидкими результатами (CIS Controls), системною побудовою (ISO 27001, COBIT) і гнучкістю (NIST CSF). Також ми окреслили додаткові підходи — процесний (PDCA), організаційно-методичний і хмарний (CSA CCM), щоб показати, як різні «логіки» можуть працювати в одному проєкті.

Нарешті, практична частина (Розділ 3) продемонструвала крок за кроком, як на прикладі уявного підприємства «ЕкоДім Буд» можна сформувати поточний та цільовий профіль безпеки за NIST CSF 2.0, візуалізувати розриви, розробити

деталізований план впровадження з термінами, бюджетом та відповідальними. І ключова ідея: жодна стратегія не працює без вимірювань саме тому ми заклали систему KPI (TTD/TTR, кількість інцидентів, рівень обізнаності персоналу тощо), яка живить цикл PDCA та дозволяє не лише закривати виявлені прогалини, а й упроваджувати постійні покращення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 20 квіт. 2025 р. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

3. Cybersecurity and Infrastructure Security Agency. Malware, phishing, and ransomware [Електронний ресурс]. – Режим доступу: https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware.

4. Rahmonbek K. 35 alarming small business cybersecurity statistics for 2025 | StrongDM. StrongDM: Your Partner in Zero Trust Privileged Access [Електронний ресурс]. – Режим доступу: https://www.strongdm.com/blog/small-business-cyber-security-statistics.

5. The 3 biggest cybersecurity threats to small businesses. Malwarebytes [Електронний ресурс].– Режим доступу: https://www.malwarebytes.com/blog/news/2025/05/the-3-biggest-cybersecurity-threats-to-small-businesses.

6. Why are SMBs most vulnerable to cyberattacks? [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/resources/cyberglossary/smb-cyberattacks.

7. ДСТУ ISO/IEC 27001:2022. Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. – [Чинний від 01.10.2022]. – К.: ДП «УкрНДНЦ», 2022.

8. ISACA. COBIT 2019 Framework: Introduction and Methodology. – ISACA, 2019.

9. CIS critical security controls version 8.1. CIS [Електронний ресурс]. – Режим доступу: https://www.cisecurity.org/controls/v8-1.

10. NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology. February 2024 [Електронний ресурс]. – Режим доступу: https://www.nist.gov/cyberframework.

11. Federal Communications Commission. Cybersecurity for Small Businesses [Електронний ресурс]. – Режим доступу: https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses.

12. Cybersecurity and Infrastructure Security Agency (CISA). Cyber Guidance for Small Businesses [Електронний ресурс]. – Режим доступу: https://www.cisa.gov/cyber-guidance-small-businesses.

13. U.S. Small Business Administration. Strengthen your cybersecurity [Електронний ресурс]. – Режим доступу: https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity.

14. Federal Trade Commission. Cybersecurity for Small Business [Електронний ресурс]. – Режим доступу: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity.

15. Fortinet. 10 Cybersecurity Tips for Small Businesses [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/resources/cyberglossary/10-cybersecurity-tips-small-business.

16. National Cyber Security Centre (NCSC). Small Business Guide: Cyber Security [Електронний ресурс]. – Режим доступу: https://www.ncsc.gov.uk/collection/small-business-guide (дата звернення: 24.05.2025).

17. Шевченко В. Л. Кращі світові практики управління інформаційною безпекою та їх вплив на економічну стабільність держави // Сучасний захист інформації. – 2015. – № 4. – С. 4–9.

18. Кібербезпека в Україні. Нормативна база, коментарі та роз’яснення. – К. : Юрінком Інтер, 2022. – 320 с.

19. Актуальні проблеми кібербезпеки : матеріали Всеукраїнської науково-практичної конференції (м. Київ, 25 жовтня 2024 року). – К. : ДУІКТ, 2024. – 251 с.

20. Програма розвитку ООН в Україні. Кращі практики управління кібербезпекою. – К. : ПРООН, 2020. – 48 с.

21. ISO/IEC 27005:2022. Information security risk management. – International Organization for Standardization, 2022.

22. ISO/IEC 27004:2022. Information security management – Monitoring, measurement, analysis and evaluation. – International Organization for Standardization, 2022.

23. Cobit 5 resources. Governance of Enterprise IT based on COBIT 5. – 2014. – P. 135–140 [Електронний ресурс]. – Режим доступу: https://doi.org/10.2307/j.ctt7zsxfv.14.

24. CIS community defense model 2.0. CIS [Електронний ресурс]. – Режим доступу: https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0.

25. Zero trust architecture / S. Rose et al. – National Institute of Standards and Technology, 2020 [Електронний ресурс]. – Режим доступу: https://doi.org/10.6028/nist.sp.800-207.

26. Parmenter D. Key performance indicators: developing, implementing, and using winning KPIs. – Wiley & Sons, Limited, John, 2019.

27. Armstrong M. Armstrong's handbook of performance management: an evidence-based guide to delivering high performance. – Kogan Page, Limited, 2017.

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

Тези наукових доповідей

Яковенко В.Ю., Лаптєв О.А. Методи впровадження стратегій кібербезпеки підприємства малого бізнесу.VIII Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-комунікаційних систем» (CPICS).