МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ **ЕФЕКТИВНІСТЬ КОРПОРАТИВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УКРАЇНІ**”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олександр ПОРОХНИЦЬКИЙ

(Підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Олександр ПОРОХНИЦЬКИЙ

Керівник:
к.т.н. Юрій ЩАВІНСЬКИЙ

Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ

Завідувач кафедрою УІКБ
_____ Світлана ЛЕГОМІНОВА
"____" _____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Порохницькому Олександру Андрійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Ефективність корпоративного управління інформаційною безпекою в Україні"

керівник кваліфікаційної роботи Юрій ЩАВІНСЬКИЙ, к.т.н.
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи "18" грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби управління інформаційною безпекою, нормативні документи, стандарти, міжнародні стандарти.*

4. Перелік питань, які потрібно розробити:
   1. Здійснити теоретичний аналіз основних понять і визначень міжнародних стандартів та методів оцінки ефективності корпоративного управління інформаційною безпекою.
   2. Проаналізувати стан корпоративного управління інформаційної безпеки в Україні.
   3. Розробити пропозиції та рекомендації щодо покращення корпоративного управління інформаційною безпекою
   4. Перелік ілюстративного матеріалу: *презентація*

5. Дата видачі завдання "02" жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: ”02” жовтня 2023 р..

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури.	15.10.2023	
3.	Аналіз понять та принципів корпоративного управління інформаційною безпекою	25.10.2023	
4.	Огляд стану корпоративного управління інформаційною безпекою в Україні	11.11.2023	
5.	Формування загального результату тенденцій та проблем в корпоративному управлінні інформаційної безпеки.	15.11.2023	
6.	Формулювання висновків за результатами проведеного дослідження.	22.11.2023	
7.	Оформлення роботи.	04.12.2023	
8.	Оформлення презентації.	14.12.2023	
9.	Отримання рецензії на роботу.	18.12.2023	
10.	Захист в ДЕК.	16.01.2024	

Здобувач вищої освіти _____ Олександр ПОРОХНИЦЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Порохницький О.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "Ефективність корпоративного управління інформаційною безпекою в Україні"
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **ПОРОХНИЦЬКИЙ Олександр** у кваліфікаційній роботі дослідив сучасний стан корпоративного управління інформаційною безпекою в Україні, визначив основні проблеми та розробив пропозиції і рекомендації керівникам структурних підрозділів кібербезпеки щодо підвищення ефективності корпоративного управління інформаційною безпекою організацій (підприємств). **ПОРОХНИЦЬКИЙ Олександр** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на трьох науково-практичних конференціях.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувача **ПОРОХНИЦЬКОГО Олександра** на оцінку "відмінно" та присвоїти йому кваліфікацію "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2024 року

Висновок кафедри про кваліфікаційну роботу

Завідувач кафедрою
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Порохницький Олександр Андрійович
на тему "ЕФЕКТИВНІСТЬ КОРПОРАТИВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УКРАЇНІ"

Актуальність

Корпоративне управління інформаційною безпекою має досить вагомий вплив на увесь робочий процес в компанії або ж організації. У зв'язку із складністю та недостатньою визначеністю нормативно-правової бази, сьогодні більшість компаній різних рівнів по своєму підходять до створення власної стратегії корпоративного управління. Це потребує проведення наукових досліджень як у галузі права так і в галузі інформаційної та кібербезпеки.

Позитивні сторони

Зроблений аналіз сучасного стану корпоративної інформаційної безпеки в Україні, дозволив визначити основні фактори та виклики що впливають на ефективність корпоративного управління. Визначені основні питання, на які слід звертати увагу при побудові тактики і стратегії корпоративного управління інформаційною безпекою, розроблені доцільні пропозиції та рекомендації щодо покращення корпоративного управління інформаційною безпекою за рахунок комплексного застосування систем моніторингу та протидії інформаційній та кібербезпеці, що розроблені вітчизняними та зарубіжними компаніями, що складає удосконалену методику дослідження. Застосування визначених рекомендацій дадуть змогу побудувати модульну систему ефективного корпоративного управління інформаційною безпекою в Україні

Недоліки

Потребують покращення якості рисунки у другому розділі. Недостатньо враховані в роботі поправки стандарту ISO/IEC 27002:2013. Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки «відмінно» а її автор Порохницький Олександр Андрійович - присвоєння кваліфікації «Магістр кібербезпеки» за освітньо-професійною програмою «Управління інформаційною безпекою».

Рецензент: завідувач кафедри
Інформаційної та кібернетичної
безпеки,
д.т.н., професор _____ Галина ГАЙДУР

підпис *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 88 стор., 17 рис., 1 табл., 62 джерел.

Метою роботи Метою даної науково-дослідної практики є визначення ефективності корпоративного управління інформаційною безпекою в Україні та розробка рекомендацій для покращення цього процесу в організаціях.

Об'єктом дослідження – управління інформаційною безпекою.

Предмет дослідження – ефективність корпоративного управління інформаційною безпекою.

Методи дослідження. Для вирішення поставленого наукового завдання в роботі були застосовано метод системного аналізу, теорія інформаційної безпеки та метод порівняння та теоретичного узагальнення, аналізу та синтезу.

Короткий зміст роботи. У роботі було проведено аналіз ефективності корпоративної інформаційної безпеки в Україні, визначені основні поняття та принципи, проаналізовані закони та стандарти, розглянутий актуальний стан в Україні, визначені основні фактори та виклики що впливають на ефективність корпоративного управління ІБ та відповідні показники які вказують на результат; в останньому розділі було визначено основні тенденції та проблеми в дані темі, та наведено основні нюанси на які слід звертати при побудові корпоративного управління інформаційної безпеки, визначені доцільні пропозиції та рекомендації щодо покращення корпоративного управління інформаційною безпекою за рахунок комплексного застосування систем моніторингу та протидії інформаційній та кібербезпеці, що розроблені вітчизняними та зарубіжними компаніями.

Галузь застосування. Розглянуті стандарти та закони, розроблений базисні пункти та метод побудови корпоративної системи управління інформаційною безпекою можуть бути використанні на початковому етапі створення СУІБ в компаніях середнього та малого сегменту, або відповідно покращення вже наявного стану в контексті захисту та оптимізації роботи відділу безпеки.

КЛЮЧОВІ СЛОВА : ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, КОРПОРАТИВНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, СТАНДАРТИ, ЗАКОНИ .

ABSTRACT

The text part of the qualification work for the degree of Master's Degree: 88 pages, 17 figures, 1 tables, 62 sources.

The purpose of the work is to study the effectiveness of corporate information security management in Ukraine.

Object of research is the corporate information security management.

Subject of research is the effectiveness of corporate information security management.

Research methods To solve the scientific task, the method of system analysis, the theory of information security and the method of comparison and theoretical generalization, analysis and synthesis were used.

Brief content of research. The paper analyses the effectiveness of corporate information security in Ukraine, defines basic concepts and principles, analyses laws and standards, considers the current situation in Ukraine, identifies the main factors and challenges that affect the effectiveness of corporate governance of information security and the relevant indicators that indicate the result; the last section identifies the main trends and problems in this area and provides the main nuances that should be taken into account when building corporate information security management, identifies appropriate proposals and recommendations for improving corporate information security management through the integrated use of information and cybersecurity monitoring and counteraction systems developed by domestic and foreign companies.

Field of research. The considered standards and laws, the developed basic points and the method of building a corporate information security management system can be used at the initial stage of creating an ISMS in medium and small companies, or, accordingly, to improve the existing state in the context of protecting and optimizing the work of the security department.

KEYWORDS:. ENTERPRISE INFORMATION SECURITY, THREAT TO INFORMATION SECURITY, CORPORATE INFORMATION SECURITY MANAGEMENT, STANDARDS, LAWS.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CIA (Confidential Integrity Availability) - Конфіденційність, цілісність та доступність.

DoS/ DDoS – Відмова в обслуговувані/ Розподілена атака на відмову в обслуговуванні.

ISO/IEC (International Organization for Standardization /International Electrotechnical Commission) – Міжнародна організація із стандартизації/ Міжнародна електротехнічна комісія.

NIST (National Institute of Standards and Technology) – Національний інститут стандартів і технології.

GDPR (General Data Protection Regulation) – Загальний регламент захисту даних.

BS (British Standards) – Британські стандарти

PCI DSS (Payment Card Industry Data Security Standard) - стандарт безпеки даних індустрії платіжних карток.

HIPAA (Health Insurance Portability and Accountability Act) - є актом про мобільність та підзвітність медичного страхування.

СУІБ - системи управління інформаційною безпекою

FISMA (Federal Information Security Management Act) - Федеральний закон про безпеку інформаційних систем.

ІБ – інформаційна безпека

BYOD (Bring your own device) – Принесіть свій власний пристрій (Мається на увазі використання в роботі власних ноутбуків або смартфонів).

AI (Artificial intelligence) – штучний інтелект.

SOC (Security operation center) – Операційний центр безпеки.

DMZ (Demilitarization Zone) – ДМЗ (Демілітаризована зона)

LAN (Local Area Network) – Локальна комп’ютерна мережа

NGFW (Next generation firewall) – фаервол наступного покоління

EDR (end-point detection and response) – система реагування на кінцевих пристроях

SIEM (Security information and event management) Управління подіями та інформаційною безпекою.

XDR – Розширене виявлення та реагування

ВСТУП

Актуальність теми. Корпоративне управління інформаційною безпекою, являє собою досить актуальне питання, особливо в Україні. Слід розуміти що даний процес має досить вагомий вплив на увесь робочий процес в компанії або ж організації, і сам пособі це комплекс поєднань різних процесів, методів, алгоритмів, людей та законів.

Через свою складність на сьогодні більшість компаній різних рівнів по своєму підходять до створення власної актуальної та дієвої системи. Особливо в цьому виділяється нормативно-правова та система стандартів що розробляють як країні так і певні організації.

Крім цього кількість загроз та факторів що націлені на зловмисні дії з кожним днем лише збільшуються, через це досить актуальним стає питання як створити корпоративну СУІБ та відповідно покращення вже наявної.

З огляду на зазначене тема кваліфікаційної робити є актуальною, а її результати дозволять компаніям малого сегменту розробити свою робочу систему управління ІБ в той час як організаціям вже з наявною системою дозволить покращити та підняти її ще на вищий рівень.

Мета роботи полягає у дослідженні основних аспектів інформаційної безпеки та відповідно покращити їх

Об'єкт дослідження - управління інформаційною безпекою.

Предмет дослідження – ефективність управління інформаційною безпекою.

Для досягнення цієї мети в роботі необхідно виконати наступні *завдання:*

1. Провести літературний огляд, аналіз існуючих підходів до корпоративного управління ІБ в Україні та світі.

2. Проаналізувати поточний стан корпоративного управління ІБ в Україні.

3. Розробити власні рекомендації для покращення корпоративного управління ІБ.

Методи дослідження. Для вирішення поставленого наукового завдання в

роботі були застосовано метод системного аналізу, теорія інформаційної безпеки та метод порівняння та теоретичного узагальнення, аналізу та синтезу.

Наукова новизна одержаних результатів. Визначений новий підхід до створення СУІБ, який полягає у комплексному застосуванні кадрових, технічних, та програмних рішень націлених на автоматизацію та покращення процесів. Удосконалено застосування критеріїв для оцінювання ефективності застосованих засобів та алгоритму удосконалення корпоративного управління інформаційної безпеки.

Практичне значення одержаних результатів. Застосування визначених рекомендацій дадуть змогу побудувати модульну систему ефективного корпоративного управління інформаційною безпекою в Україні, та значно підвищити ефективність організаційного процесу з точки зору менеджменту та інформаційної безпеки. За допомогою наведених методів та матеріалів компанія що раніше не працювала з ІБ зможе добитися початкового рівня захищеності з перспективним майбутнім.

Апробація результатів кваліфікаційної роботи було оприлюднено на науково-практичних конференціях:

Шуліпа Н., Порохницький О. Застосування етичних норм світових стандартів в корпоративному управління інформаційною безпекою. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу* : ВСЕУКР. НАУКОВО-ПРАКТ. КОНФ., м. Київ, 23 лют. 2023 р. Київ, 2023. С. 127–128.

Щавінський Ю. В., Кудін І. В., Порохницький О. А. Етичні методи та засоби управління інформаційними інцидентами і ризиками. *Актуальні проблеми кібербезпеки* : ВСЕУКР. НАУКОВО-ПРАКТ. КОНФ., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 369–372.

Порохницький О. А. Вплив на інформаційну стабільність колективу. *Актуальні проблеми кібербезпеки* : ВСЕУКР. НАУКОВО-ПРАКТ. КОНФ., м. Київ, 27 жовт. 2022 р. Київ, 2022. С. 98–99.

Розділ 1
ТЕОРЕТИЧНІ ОСНОВИ КОРПОРАТИВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

1.1 Поняття та принципи корпоративного управління інформаційною безпекою

Розглядаючи поняття та принципи управління інформаційною безпекою слід зазначити що це комплекс заходів і практик які спрямовані на захист інформації від загроз та на забезпечення її конфіденційності, цілісності і відповідно доступності. Тобто згадуючи тріаду Confidential Integrity Availability (рис. 1.1). Вона повністю оточує інформацію а також підв’язує до неї ще три поняття як комунікація, технічне та програмне забезпечення і вже останні три кола продукти (Фізична безпека), люди (Безпека персоналу) та процеси (Безпека організації). Ці принципи дозволяють правильно визначити потреби організації та її межі що описують основні цілі та загрози на які слід звернути для підвищення захищеності організації [1-3].

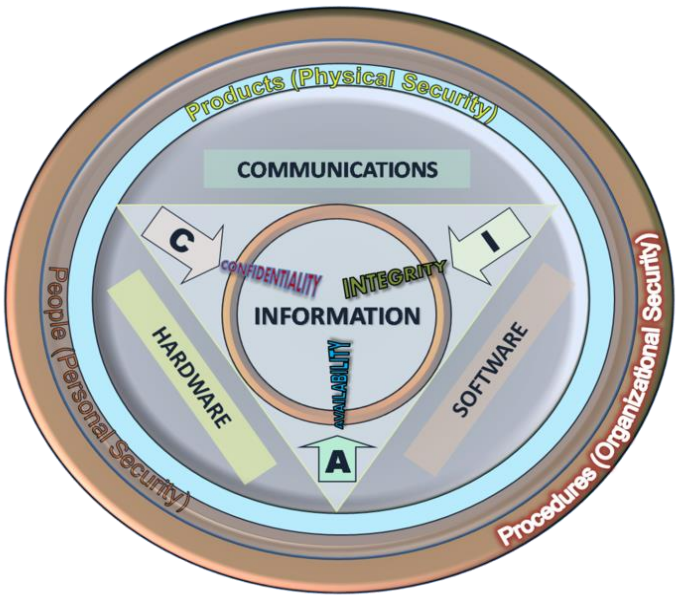

Рис. 1.1. Тріада CIA[1-3]

Дана тріада надає базу для будь-якої компанії та організації, та вказує на основні потреби для правильного рівномірного росту інформаційної безпеки.

Коли йде розмова по мережеву безпеку то дана основа одна із найважливіших моделей успіху що була розроблена що б проводити правильну компанію з управління інформаційною безпекою як в середині компанії так і запобігти витік її на за периметр організації [1-3].

Конфіденційність – даний параметр означає що лише уповноважені особи/системи можуть переглядати конфіденційну або засекречену інформацію. Дані, що передаються мережею, не повинні бути доступними для неавторизованих осіб. Зловмисник може спробувати перехопити дані за допомогою різних інструментів, доступних в Інтернеті, і отримати доступ до вашої інформації. Основний спосіб уникнути цього - використовувати методи шифрування для захисту ваших даних, щоб навіть якщо зловмисник отримає доступ до них, він не зміг їх розшифрувати. Стандартним шифруванням є AES (Advanced Encryption Standard) і DES (Data Encryption Standard). Ще один спосіб захистити ваші дані - це використання VPN-тунелю. VPN розшифровується як Virtual Private Network (віртуальна приватна мережа) і допомагає безпечно передавати дані через мережу(рис. 1.2) [1-3].

Рис. 1.2. Шифрування

Наступне, про що варто поговорити - це цілісність. Ідея полягає в тому, щоб переконатися, що дані не були змінені. Пошкодження даних - це нездатність підтримувати цілісність даних. Щоб перевірити, чи були наші дані змінені, ми використовуємо хеш-функцію.

Існує два основних типи хешування: SHA (Secure Hash Algorithm) і MD5 (Message Direct 5). MD5 - це 128-бітний хеш, а SHA - 160-бітний хеш, якщо ми використовуємо SHA-1. Існують також інші методи SHA, які ми можемо використовувати, такі як SHA-0, SHA-2 і SHA-3. (рис. 1.3) [1-3].

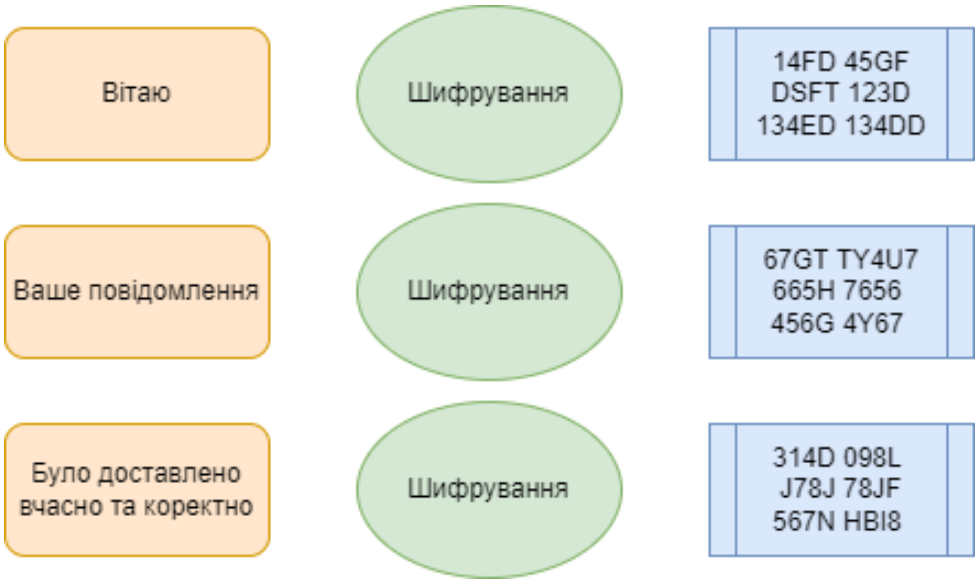

Рис. 1.3. Цілісність інформації

Доступність – це означає, що мережа повинна бути легкодоступною для користувачів. Це стосується як систем, так і даних. Щоб забезпечити доступність, мережевий адміністратор повинен підтримувати апаратне забезпечення, регулярно оновлювати його, мати план обходу відмов і запобігати виникненню вузьких місць у мережі. Такі атаки, як DoS або DDoS, можуть зробити мережу недоступною, оскільки ресурси мережі вичерпуються. Вплив може бути значним для компаній та користувачів, які покладаються на мережу як на бізнес-інструмент. Таким чином, слід вжити належних заходів для запобігання таким атакам. (рис. 1.4) [1-3].

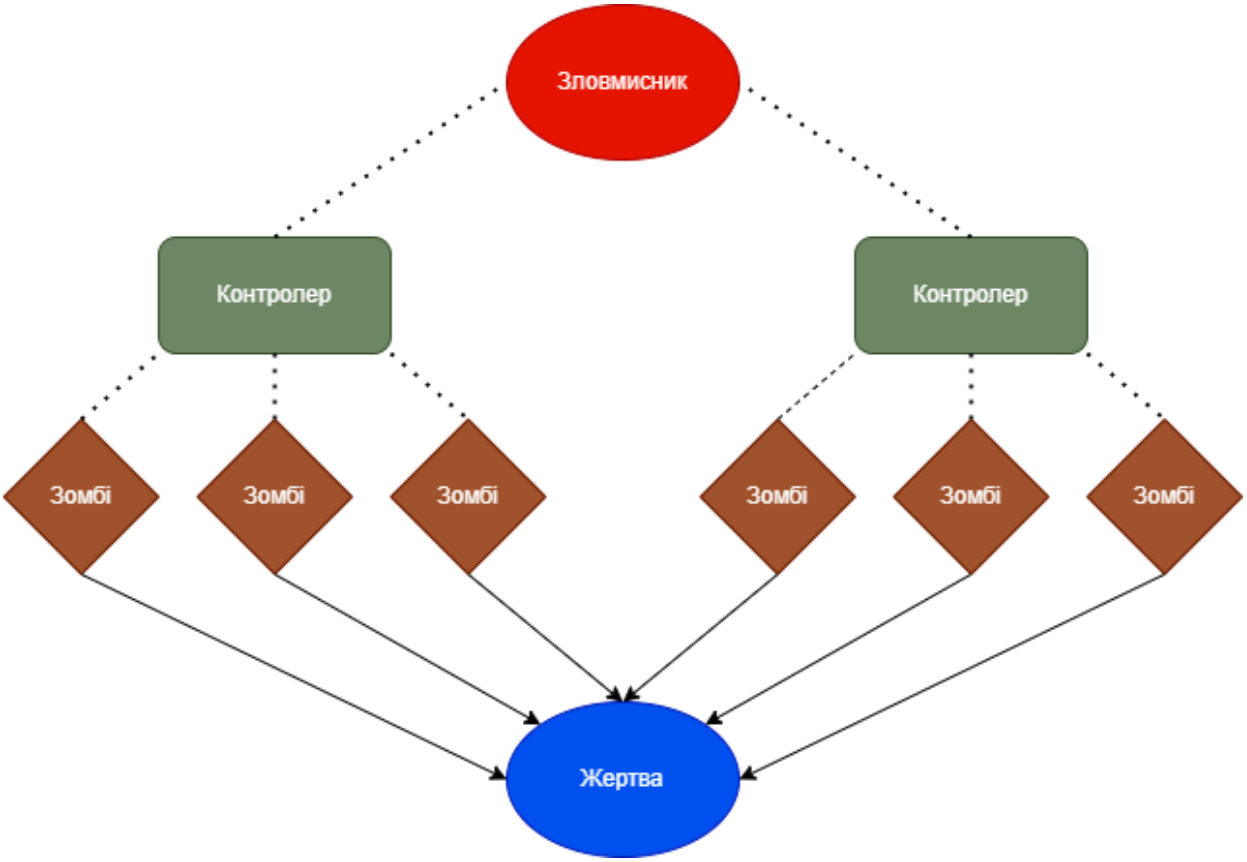

Рис. 1.4. DdoS атака

Розглядаючи корпоративне управління інформаційною безпекою слід зазначити що вони охоплюють різні підходи та методики для забезпечення відповідного рівня інформаційної безпеки в організації. Як приклад можна визначити стандарти та певні рамкові моделі, в основному вони засновані на міжнародних стандартах ISO/IEC 27001 та ISO/IEC 27002 що базуються на великій кількості досліджень та практичного спостереження та протидії негативному впливу на інформаційну безпеку організацій. Що до рамкових моделей та певної готової системи можна розглянути NIST Cybersecurity Framework. Даний фреймворк несе в собі набір кращих та вже готових до використання практик та рекомендацій розроблений в США Національним інститутом стандартів та технологій [4].

Управління ризиками це підхід заснований на оцінці ризиків що дає змогу організаціям визначати вразливості та загрози, оцінювати потенційні збитки та розроблювати стратегії по їх зниженню.

Дотримання вимог різних стандартів та нормативних, є запорукою успіху і основою усіх підходів до управління інформаційною безпекою. Краще скористатися вже готовими вимогами або рекомендаціями що надають досвід інших організацій стосовно забезпечення відповідного рівня захищеності. Три наглядних приклади даних стандартів та нормативів входить GDPR, HIPAA, або PCI DSS. Це дозволить бути повністю відповідним до вимог законодавства певної країни або нормам безпеки.

З точки зору технічного підходу слід визначити три окремих:

Перше це розділене керування доступом та автентифікація, даний підхід фокусується на розмежуванні та контролю доступу до інформації та налаштування автентифікації включно з багатьма іншими факторами, що гарантує що всі користувачі мережі будуть авторизовані та матимуть доступ до даних які їм відведені.

Друге це моніторинг та фіксація інцидентів, організація зможе за допомогою даних систем збирати, аналізувати та безперервно контролювати власні системи та мережі, вчасно реагувати на аномалії та інциденти в реальному часі.

Третє, сегментація мережі та захист даних. Даний підхід буде націлений та шифрування даних, регулярні резервні копії та контроль, в свою чергу для користувача це дасть можливість не загубити данні через технічні збої або ж відсутність світла на об’єкті обробки даних або ж офісі. До даного нюансу слід додати і запасні джерела електроживлення та провайдерів. Сегментацією ж мережі відбувається розділення її на сегменти щоб працівники не могли отримати доступ до інформації іншого відділу без дозволу. Прикладом може слугувати розділення мережі комунікації відділу кадрів та розробок. Тож чутлива інформація буде обмежена в доступі і це зменшить ризики поширення атаки з одного відділу до іншого [5].

Не слід забувати що персонал це найголовніший актив і один з можливих чинників що може стати загрозою для організації то ж їх обізнаність, освіта та мотивація грає не останню роль у підвищені безпеки та конфіденційності

інформації в компанії. Проводячи постійні тренінги та практикуми що не заважають роботі та не забирають вільний час у співробітників збільшить лояльність працівників та репутації організації загалом. Думка співробітника та його мислення має бути позитивним про компанію мінімум 70% це дозволить тримати їх в оптимальному стані та зменшить втрату цінних кадрів.

Розглядаючи в загальному роботу компанії слід приймати до уваги те що їй майже завжди знадобиться працювати з постачальниками та підрядниками або ж з сторонніми контрагентами. Слід завжди зважувати їх репутацію, послуги та товари які вони надають [5].

Останнє але не менш важливе це бізнес-спрямоване управління інформаційною безпекою, даний підхід націлений на більш стабільний та пряму стратегію інформаційною безпекою з урахуванням усіх процесів та проблем пов'язаними з етапами розробок політик та заходів безпеки.

До вище зазначених підходів можна додати ще пункт стосовно особистих якостей керівника це його лідерство та підтримка в процесі виконання поставлених задач, виділенні ресурсів та саму участь у розробці. Постійне поліпшення та оцінка актуальних ризиків для бізнес-процесів та ринку. Також слід приймати відповідальність в разі виникнення проблем з продуктом та бути відкритим по відношенню до клієнта.

Розглядаючи дані принципи та поняття слід ще додати концептуальні методи розробки моделі безпеки [5]:

Підхід «знизу вгору». Модель безпеки компанії яку застосовують системні адміністратори або працівники, у сфері мережевої та кібер безпеки. Основна концепція цього підходу полягає в тому, щоб люди, які працюють у галузі інформаційних систем, використовували свої знання та досвід у сфері кібербезпеки, щоб гарантувати розробку високо захищеної моделі інформаційної безпеки [5].

- **Ключові переваги –** технічний досвід працівника у відповідній галузі дозволяє бути впевненим, що кожна вразливість системи буде

ліквідована або буде знайдене рішення проблеми в найкоротші терміни, через це модель безпеки зможе протистояти будь-яким потенційним загрозам.

- **Недоліки –** через відсутність співпраці між вищими керівниками та відповідними директивами, це часто не відповідає вимогам і стратегіям організації.

Підхід «зверху вниз». Цей тип підходу зініціюється власне самими керівниками організації та регламентується згідно їх проблем [5].

- Оформлення політик та процедур.
- Визначення пріоритетів проекту та очікувані результати.
- Визначення відповідальних за кожний етап, дію та процеси.

Переваги та недоліки впровадження зверху вниз:

Цей підхід розглядає дані кожного відділу та досліджує, як вони пов’язані між собою за для досягнення цілей крім цього, щоб знайти вразливі місця. Менеджери мають повні повноваження в цілях видання інструкцій для всієї компанії, дозволяючи кожній особі відігравати невід’ємну роль у збереженні даних у безпеці. Порівняно з підходом до окремої особи чи відділу, підхід, що базується на управлінні, включає більше доступних ресурсів і більш чіткий огляд активів і проблем компанії [5].

Розглядаючи даний підхід слід зазначити що він має більше силу та ефективність в порівнянні з «знизу вгору», оскільки робиться в пріоритеті захист даних для усієї компанії, а не являє собою перекладання всієї відповідальності на окрему команду або особу. Вразливість даних існує у всіх офісах та відділів, але в незалежності від ситуації та схожості кожна ситуація буде унікальна та буде мати досить маленькі але критично важливі відмінності. Єдиний спосіб що може дозволити запрацювати програмі інформаційної безпеки це погодження з кожним керівником, відділом та співробітником з планом, стратегією та регламентом даного напрямку (рис. 1.5) [5].

Слід зазначити що досить важливим нюансом є впровадження багаторівневого підходу до інформаційної безпеки. Тобто кібербезпека та інформаційна безпека маю одну з найголовніших ролей в усіх типах та розмірах

компаній і відповідно залежить не тільки від технічного забезпечення а і від кожного працівника бо не слід забувати що кожний працівник це актив компанії (рис. 1.5) [5].

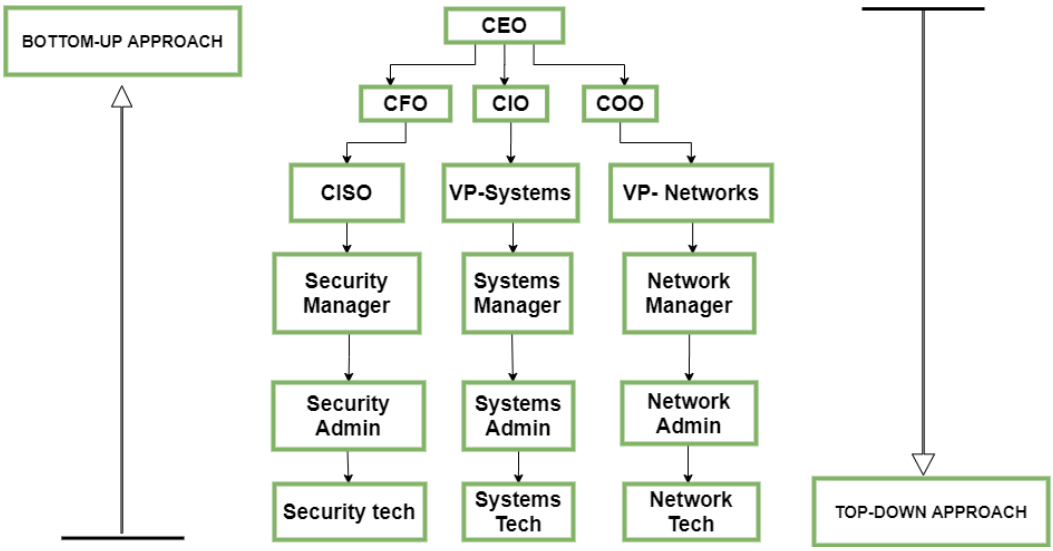

Рис. 1.5. Схема підходу до керування ІБ [5]

Порушення безпеки даних і мережі може мати руйнівні наслідки від яких компанія може не оговтатись певний період або взагалі зруйнуватись. Через це слід розглядати кожну атаку як окрему частинку головоломки, просте пінгування портів або фізична спроба проникнути в будівлю організації вже стає показником того що хтось зацікавлений у спробі зашкодити організації. Такі інциденти слід об'єднувати в певну мапу або навіть схему з усією інформацією що відома на той час і проводити розслідування для виявлення та передбачування майбутніх загроз [5].

Атаки бувають різних форм, соціальна інженерія, несанкціоноване проникнення до фізичних місць, трояни, програми шифрувальники і тд. Даний атаки та методи можуть обмежуватись лиш фантазією зловмисника. Також потрібно зазначити що жодна система не захищена на всі сто відсотків і має дуже багато вразливостей через це багаторівневий є досить непоганим методом для впровадження захисту у відділах [5].

Розглядаючи InfoSec слід вказати що її багатошаровість забезпечує захист даних разом з іншими аспектами, що включає у себе веб, мережу пристрої та додатки, програмне забезпечення та фізичну безпеку. Так в ньому наявний план аварійного відновлення та резервного копіювання даних [5].

Рівневий захист розбиває великі проблеми на більш малі і тд., це дозволяє розбити проблеми та задачі між підрозділами та розподілити навантаження рівномірно для вирішення проблеми у короткий період часу. За допомогою цього ми можемо налаштувати систему та рівень захисту в залежності від конкретних проблем, потреб відділу але філіалу, пристрою або ж від важливості даних що зберігаються на накопичувачах.

У кожного бізнеса та організації є свої потреби, банки залежні від фінансового відділу який контролює розрахунки та транзакції, медичний від бази даних своїх клієнтів в якій зберігається інформація про кожного.

Окремо слід розглядати безпеку інтернету та мережі що в свою чергу охоплює створення політик і захист усіх браузерів, приватних мереж, спільних мереж і облікових записів онлайн-користувачів, таких як [5]:

- Чітко призначені ролі користувачів для кожної особи з доступом, включаючи керівництво, співробітників, сторонніх підрядників і партнерів;
- різні методи шифрування для співробітників і підрядників на місці і за його межами;
- безпека IP-мережі для всього мережевого трафіку;
- брандмауери, системи захисту від вірусів і зловмисного програмного забезпечення, попередження про вторгнення та програмне забезпечення для захисту;
- безпека для всієї веб-пошти, включно з вкладенням та можливим фішингом;
- використання безпечного сучасного веб-браузера з індивідуальним обліковим записом контрольованого доступу співробітника;
- безпека мобільних пристроїв для корпоративних телефонів, планшетів і смарт-пристроїв;

- сегментація мережі, коли це можливо;
- запобігання втраті даних для файлів і повідомлень.

Відповідна безпека пристроїв і програм що поширюється на всі комп'ютери, планшети, корпоративні телефони, смарт-пристрої, програми, програмне забезпечення користувача, комп'ютерні програми та облікові записи в Інтернеті. Запобіжні заходи включають:

- Підтримка всіх додатків та програмного забезпечення та їх подальшої безпеки в актуальному стані;
- необхідність в унікальному паролі та облікових даних для входу кожного користувача, які регулярно змінюються;
- реалізація регулярних періодів обслуговування пристрою та системи протягом місяця;
- ведення ретельних, актуальних записів для всіх пристроїв і програм, включаючи можливі, виявлені або окремі загрози;
- надання кожному користувачеві пристрою та обліковому запису системи виявлення вторгнень;
- видалення з непотрібних програм, програмного забезпечення, облікових записів користувачів і пристроїв;
- впровадження керування виправленнями, щоб усе було актуальним і автоматично виправлялося, коли виходять нові виправлення.

Найбільша вірогідність успіху буде при дотриманні даної стратегії - це зазвичай забезпечує потужну підтримку з боку вищого керівництва шляхом виділення ресурсів, послідовного механізму підготовки та виконання та можливостей впливу на корпоративну культуру [5].

1.2 Аналіз міжнародних стандартів та рамок управління інформаційною безпекою.

Розглядаючи стандарти інформаційної безпеки слід зазначити, що вони намагаються захистити кібернетичне середовище усіма доступними способами та досвідом отриманим протягом часу. Зазначимо що дане середовище включає в себе користувачів, мережі, пристрої, програмне забезпечення, обробка та зберігання інформації, служби, системи та процеси.

Через це їх основною метою і стає зниження ризиків та попередження або зменшення впливу від атак на об’єкти.

Міжнародні стандарти інформаційної безпеки це набір норм і рекомендацій що були розроблені міжнародними організаціями та експертами з ціллю як краще забезпечити єдині, уніфіковані принципи і практики у сфері захисту інформації. Ці стандарти надають допомогу організаціям і державам створювати надійніші системи інформаційної безпеки та дотримуватися встановлених норм. Нижче перераховані досить відомі міжнародні стандарти інформаційної безпеки [6]:

ISO/IEC 27000: словник та визначення [7].

ISO/IEC 27001 та ISO/IEC 27002: ISO/IEC 27001 визначає вимоги для системи управління інформаційною безпекою (СУІБ), тоді як ISO/IEC 27002 надає рекомендації та практичні вказівки щодо реалізації заходів безпеки [8].

ISO/IEC 27005: Цей стандарт описує процес управління ризиками в галузі інформаційної безпеки та надає методику для оцінки ризиків.

ISO/IEC 27006:2015 Вимоги для організацій що проводять аудити та сертифікацій підприємств на відповідний рівень ІБ [7].

ISO/IEC 27019:2017 – Інформаційні технології для енергетичних підприємств та організацій пов’язаних з ними [7].

ISO/IEC 27018: Відповідає за керівництво захисту даних у хмарних сервісах та надає відповідні рекомендації з його покращення [7].

ISO/IEC 27701: Керівництво з управління захистом даних також має розширену версію як доповнення для стандартів типу 27001 та 27002 [7].

ISO/IEC 27032: Стандарт присвячений міжнародній кібербезпеці та містить рекомендації з управління кібер ризиками та інцидентами.

ISO/IEC 27011 – Керівництво з управління інформаційною безпекою в телекомунікаційному секторі [7].

ISO 22301: Цей стандарт визначає вимоги до систем управління неперервністю бізнесом , включно з аспектами інформаційної безпеки.

BS 7799-1: 2005 — Британський стандарт BS 7799 перша частина. Кодекс практики управління інформаційною безпекою та описує 127 механізмів контролю, необхідних для побудови системи управління інформаційною безпекою (СУІБ) організації [6].

BS 7799-2: 2005 — Британський стандарт BS 7799 друга частина стандарту. Управління інформаційною безпекою — специфікація систем управління інформаційною безпекою, дана частина відноситься ближче до сертифікації самої організації [6].

BS 7799-3: 2006 — Британський стандарт BS 7799 третя частина стандарту. Новий стандарт в області управління ризиками інформаційної безпеки [6].

ISO/IEC 17799: 2005 — «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Міжнародний стандарт, базувався на BS 7799-1: 2005 [6].

NIST SP 800-53: Цей стандарт, розроблений Національним інститутом стандартів і технології (NIST) США, містить каталог безпеки інформації та контрольних заходів для федеральних інформаційних систем [9].

GDPR (Загальний регламент із захисту даних): Цей регламент Європейського союзу регулює обробку персональних даних і містить норми, пов'язані із забезпеченням безпеки цих даних [10].

HIPAA (Закон про портативну медичну страховку та акаунти засобів охорони здоров'я): Цей закон у США встановлює стандарти для безпеки та конфіденційності медичної інформації [11].

PCI DSS (Стандарт безпеки даних в індустрії платіжних карток): Цей стандарт розробляється Радою зі стандартів безпеки платіжних карток (PCI SSC) і встановлює вимоги для захисту даних, пов'язаних із платіжними картками [12].

FISMA (Федеральний закон про безпеку інформаційних систем): Даний закон у США визначає вимоги до безпеки інформаційних систем у федеральних органах і підрозділах уряду [13].

Ці стандарти відіграють критичну роль у забезпеченні ІБ на світовому рівні, і вони часто використовуються організаціями для розроблення власних політик і процедур. Вибір стандартів в основному залежить від характеру діяльності організації та її потреб у сфері безпеки інформації. В більшості випадків компанії не великих розмірів можуть брати застарілі або користуються законами та державними стандартами.

Сертифікація один з важливих нюансів роботи будь-якої компанії. Сертифікат відповідності стандарту ISO/IEC це показник для будь-якого клієнта що якість послуг та продукції, інформаційної безпеки, систем керування та дотримання вимог різних країн та високого рівня відповідальності дасть впевненість клієнта у роботі саме з даною компанією.

В свою чергу сертифікація за стандартом ISO 27001, вимагає певної бази, підготовки та зусиль організації. Проте організація отримує можливість надати документи сертифікації. Цим вона повністю відповідає вимогам інформаційної безпеки та вживає усі заходи згідно стандартів і має конкурентну перевагу.

ISO/IEC 27001 є міжнародним стандартом та основоположником СУІБ як системи що націлена на збільшення захисту та відповідно безпеки організації. Цей стандарт встановлює вимоги для створення, реалізації, підтримання та безперервного поліпшення системи управління інформаційною безпекою (СУІБ) в організації. Цей стандарт розроблено Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Ось ключові аспекти ISO/IEC 27001 [14]:

Основною метою ISO/IEC 27001 є забезпечення ефективного управління інформаційною безпекою в організації шляхом визначення та реалізації

відповідних політик, процедур і практик. Сам стандарт заснований на процесному підході до управління інформаційною безпекою. Він передбачає, що організація повинна систематично і циклічно планувати, впроваджувати, перевіряти і покращувати заходи щодо забезпечення інформаційної безпеки [14].

Одним з приємних плюсів ISO/IEC 27001 слід вважати оцінку ризиків. Організації повинні ідентифікувати загрози та вразливості, а також визначити рівень ризику, пов'язаний з їхньою інформацією. Потім необхідно розробити та реалізувати відповідні контрольні заходи для управління ризиками.

Згідно цього стандарту організація повинна розробити політики та процедури, що визначають, як забезпечуватиметься інформаційна безпека. Ці документи мають відповідати вимогам стандарту [14].

ISO/IEC 27001 вимагає постійного поліпшення системи управління інформаційною безпекою. Організації повинні регулярно аналізувати результати та процеси, вносити зміни та коригування, якщо необхідно [14].

Після завершення процесу впровадження та підтримки системи управління інформаційною безпекою, організації можуть пройти процедуру сертифікації відповідно до ISO/IEC 27001. Це дає стороннім сторонам упевненість у тому, що організація дійсно дотримується стандарту [14].

Стандарт ISO/IEC 27001 може бути застосований до організацій усіх розмірів і типів, включно з комерційними підприємствами, державними установами, некомерційними організаціями тощо. Одним з великих позитивних сторін ISO/IEC 27001 це те що можна його комбінувати з іншими стандартами, такими як ISO/IEC 27002, для більш конкретних реалізацій і рішень у сфері інформаційної безпеки [14].

ISO/IEC 27001 є потужним інструментом для забезпечення інформаційної безпеки та управління ризиками, пов'язаними з інформацією. Він допомагає організаціям створити систему, яка відповідає міжнародним стандартам і вимогам, а також забезпечує надійний захист конфіденційності, цілісності та доступності інформації [14].

Стандарт забезпечення захисту звичайно містять опис послідовності оцінок, які необхідно виконати, щоб вважати дану характеристику безпеки підтвердженою з точки зору атестації захисту або множину характеристик безпеки, які повинна забезпечити система захисту, щоб її можна було використовувати в даному конкретному режимі забезпечення безпеки або у відповідності до загальної стратегії захисту [14].

Порівняння ISO 27001 та ISO 27032

ISO 27032 не є стандартом, який можна сертифікувати; можливо, це одна з найважливіших відмінностей від ISO 27001, який дозволяє сертифікувати систему управління інформаційною безпекою (СУІБ) [15].

Обидва стандарти мають різні цілі, але при цьому тісно між собою пов’язані. ISO 27032 націлений на забезпечення керівництва з кібербезпеки за допомогою рекомендацій, в той час як ISO 27001 визначає вимоги до створення СУІБ. Тож можна узагальнити що 27001 націлений на організацію, а 27032 більше сфокусований на кіберпросторі і він основний для співпраці та вирішення питання що зосереджені на різних напрямках кібербезпеки.

Слід провести більш детальне порівняння між даними стандартами для визначення їх відмінностей [15].

Кожен ризик можна розрахувати на основі певних параметрів, активів, загроз та вразливостей [15].

Розглядаючи версію стандарту ISO 27001:2013 не вказано, що для вирахування рівня ризику потрібно врахувати активи, вразливості та загрози з якими можна зіштовхнутися в майбутньому, це і робить з нього більш гнучким в порівнянні з попередньою версією [15].

В свою чергу ISO 27032:2012 визначає різні типи активів і не включає в себе списку загроз і вразливостей як в ISO 27005. Але даний стандарт ISO наводить приклади, що можна застосувати в кіберпросторі і його загрози в основному поділялись на вплив на актив-особу та актив-організація [15].

Слід зазначити що жоден з цих стандартів не розкриває як правильно керувати ризиками, а просто посилаються на інші стандарти такі як ISO 27005

(управління ризиками інформаційної безпеки) або ж ISO 31000 (для будь-якого іншого типу ризику) які в свою чергу є кращими практиками в даному напрямку. Проте ISO 27001 встановлює різні вимоги які повинна охоплювати розроблена методологія(даний тип параметрів в основному залежав від власника організації та його рівень прийняття ризиків) [15].

ISO 27001:2013 містить 114 засобів контролів, не всі з яких пов'язані з технологіями. Багато з них пов'язані з управлінням постачальниками, управлінням людськими ресурсами тощо. Однак елементи управління, які можна знайти в ISO 27032:2012, є більш специфічними для кібербезпеки тобто застосування рівнів управління, захист сервера, кінцевого користувача, управління атаками соціальної інженерії і т.д [15].

Зі свого боку, ISO 27001:2013 містить лише короткий опис кожного елемента управління, і жоден з них не стосується безпосередньо кібербезпеки. Детальний опис кожного елемента управління та керівництво з його впровадження можна знайти в ISO 27002, тоді як в ISO 27032:2012 ви можете ознайомитися з детальним довідковим посібником. Таким чином, ISO 27001:2013 є більш широким і глобальним, в той час як ISO 27032:2012 є більш конкретним і специфічним для кібербезпеки [15].

Інший важливий компонент, який ви можете знайти в ISO 27032:2012, - це рамки для координації та обміну інформацією, що особливо цікаво при управлінні інцидентами, пов'язаними з кібербезпекою, які можуть статися. Стандарт ISO 27001:2013 також містить засоби управління інцидентами в додатку, але вони стосуються лише інцидентів, пов'язаних з інформаційною безпекою [15].

Технічні засоби контролю, визначені в цьому міжнародному стандарті, покладаються на те, що організації мають належну практику кібербезпеки та використовують існуючі засоби контролю інформаційної безпеки ISO/IEC 27001 в організації. Процес впровадження технічних засобів контролю кібербезпеки спрощується, якщо організація дотримується стандарту ISO 27001. Стандарт ISO

27032 містить технічні засоби контролю кібербезпеки для захисту від кіберзагроз [15]:

- Атаки за допомогою соціальної інженерії;
- злом системи;
- шкідливе програмне забезпечення ;
- шпигунські програми;
- інше небажане програмне забезпечення;

Слід зазначити що технічна частина займає не мало важливу роль в цьому процесі та включає в себе такі засоби контролю [15]:

- Захищене кодування: Для того що б захистити інформацію, що була зібрана продуктами в кіберпросторі слід застосувати засоби для контролю захищеності кодування в середині системи;
- постійний моніторинг та миттєве реагування: Слід провести впровадження засобів контролю для забезпечення надійності, доступності та особливо безпечності усіх видів послуг в тому числі й мережевих. Робота в кіберпросторі не повинна ставити під загрозу якість, безпеку та доступність;
- серверний контроль: В даному випадку слід проводити контроль на рівні серверу що б впроваджені засоби для контролю були відповідні та гарантували забезпечення захищеного доступу до серверів з мережі та захищеність від несанкціонованих доступі з обох сторін;
- рівень додатків: Впровадити засоби контролю для захисту від несанкціонованого перегляду, редагування або ж видалення даних; проводити реєстрації усі наявних транзакцій та обробку помилок;
- endpoint control або контроль кінцевих користувачів: З даним сегментом за звичай достатньо складно через людський фактор тож основною вимогою є впровадження засобів контролю без зайвих проблем для кінцевих користувачів організації від вже відомих на даний момент вразливостей та атак;

Підсумовуючи усе вище вказане слід зазначити що ці обидва стандарти слід розглядати та впроваджувати разом та паралельно, а не окремо та в різний

проміжок часу. Також їх можна по повному доповнити засобами контролю іншими стандартами ISO і це в свою чергу дозволить збільшити рівень захисту бізнесу в кіберпросторі [15].

1.3. Аналіз існуючих методів оцінки ефективності корпоративного управління інформаційною безпекою.

Оцінка ефективності корпоративного управління інформаційною безпекою може включати в себе різноманітні методи та підходи. Важливо зазначити, що – це динамічний процес, і оцінка повинна враховувати не тільки поточний стан, а й спроможність в майбутньому адаптуватися до змін в технічних умовах та різних загроз через непередбачуваність. Базовими методами оцінки можна визначити даний перелік методів:

Аудит інформаційної безпеки: Регулярний аудит інформаційної безпеки що в свою чергу дозволяє оцінити відповідність систем та процесів які були визначені за вимогами стандартів, політик та нормативних актів [16-18].

Тобто, усі сучасні організації та компанії стикаються із зростаючими кіберзагрозами, через що і вдаються до аудиту інформаційної безпеки. Даний аспект розглядається як комплекс заходів, що в свою чергу дозволяє оцінити рівень захищеності інформаційних систем та перевірити, чи належно вони відповідають усім стандартам безпеки – таким як ISO 27001, ISO 27002, а також рекомендації загального регламенту захисту даних GDPR. Кажучи іншими словами то Аудит Інформаційної Безпеки (ІБ) – це спосіб яким можна виявити потенційні загрози та вразливості в організації або компанії [16-18].

Проводячи даний аудит можна розглянути як частину загальної комплексної стратегії системи управління інформаційної безпеки. Ця стратегія дозволяє поглянути на систему з іншої сторони та вимагає пошук, навчання працівників до рівня спеціаліста з даного профілю а також закупівля,

впровадження, налаштування та підтримки технічного та програмного аспекту що буде відповідати за стан інформаційної безпеки в середині організації.

В основному аудит поділяється на два види аудиту зовнішній та внутрішній в плані цінності обидва займають досить високу роль і ось чому [16-18]:

Внутрішній аудит проводиться на постійній основі силами самої компанії та вимог що визначені в середині організації. Даний аспект аудита дозволяє без застосування зовнішніх сил проводити його досить часто, всього лиш маючи в організації відповідальних працівників які постійно проводять аудити, використовуючи лише стандарти, вимоги і нормативи якими володіє компанія. Це дозволяє в свою чергу зменшити навантаження на фінансову частину компанії, але при цьому збільшує навантаження на актив у вигляді працівників які виділені для даного завдання [16-18].

Зовнішній аудит проводиться незалежними експертами або ж компаніями, які виконують роботу відповідно до встановленого договору що був укладений між ними та компанією та технічного завдання що було визначено раніше. В даному випадку цей процес вимагатиме залучення фінансових ресурсів та на вибір керівництва повідомляти персоналу чи ні. Якщо ж все проводиться без оповіщення персоналу, це дозволяє отримати більш об’єктивну оцінку та вказати на проблеми та їх вирішення [16-18].

Якщо це підсумовувати то зовнішній аудит дозволить отримати більш об’єктивну та реальну оцінку стану інформаційної безпеки в той час як внутрішній аудит дозволяє проводити кореляцію проблем та визначення дотримання відповідного рівня безпеки.

При визначені аудиторської компанії слід дізнаватись про їх ліцензії та сертифікати і чи здатні вони самі надавати сертифікати відповідності рівня інформаційної безпеки відповідно стандартам та нормативно правовим законам.

Процес проведення внутрішнього аудиту інформаційної безпеки зазвичай в першу чергу обговорюється з керівництвом та створюється договір та технічне

завдання в якому розписується усі завдання та умови і від яких аудитор не може відійти. Це і є представляє собою підготовчий етап перед аудитом [16-18].

Першим етапом йде призначення відповідальних за аудит інформаційної безпеки співробітники служби безпеки та відповідних відділів. В разі зовнішнього аудиту компанія до якої звернулися за даною послугою сама виділяє відповідальних працівників [16-18].

Другий етап схожий в обох випадках, визначені відповідальні працівники проводять перевірку усіх бізнес процесів, технічного забезпечення та працівників. Ціль – виявити усі вразливі сегменти в організації.

Фінальним етапом проводиться повний аналіз отриманих результатів, документація та підбиття підсумків, в даному випадку позитивно може себе проявити детальна презентація з схемами та графіками, проблеми та її вирішення [16-18].

Кожен з етапів може змінюватись за вимогою організацій але в основному всі корективи документуються та вказуються на проблеми. Тож аудит інформаційної безпеки - це процес, що допомагає організаціям та компаніям дізнатися про їх проблеми та вразливості що присутні на різних їх рівнях. Сам процес аудиту починається з усвідомлення компанією її можливих вразливостей, бажанням покращити репутацію та збільшити кількість клієнтів. Завдяки цьому організація може розробити власний план та підхід до поліпшення даного становища та розробити власні протоколи та правила для подальшого дотримання відповідного рівня захищеності та довіри [16-18].

Оцінка ризиків: Визначення потенційних ризиків, їх вплив та збитків які може понести організація завдяки цьому можна визначити пріоритет для заходів які слід зробити для запобігання або ж зменшенню впливу наслідків в майбутньому. З його допомогою визначаються вразливості та потенційні наслідки інцидентів для розроблення стратегії їх мінімізації ризиків в даному секторі.

Проведення пентестів: Тестування на проникнення дає можливість оцінити стійкість систем та мереж до реальних кібератак [19].

Це дозволяє виявляти слабкі місця в інфраструктурі та програмному забезпеченню, перевірка ефективності виявлення та реагування на інциденти, оцінки впливу атак на робоче середовище. Освіченість персоналу та їх доброчесності це теж потребує певного оцінювання для виявлення якості знань персоналу. Це можна досить просто провести шляхом тренінгів, інструкцій, та внутрішніх тестів. Результати ж в свою чергу покажуть рівень знань кожного співробітника [19].

Аналіз ефективності технічних засобів безпеки: Повна оцінка ефективності технічних рішень що застосовуються в організації. Визначення вразливих місць та вирішення основних потреб компанії.

Стрес-тести: Даний етап включає в себе проведення стрес-тестів над персоналом так і технічною частиною як експеримент для виявлення готовності як з сторони персоналу так і зі сторони фізичного та технічного забезпечення безпеки у разі виникнення непередбачуваних ситуацій, хакерських атак або ж спроб проникнення на територію організації без дозволу.

Оцінка ефективності політик та процедур безпеки: Перевірка правильності та ефективності впроваджених політик та процедур що пов’язані з безпекою. Даний етап аналізує стан політик та процедур як саме вони впроваджені та їх актуальність, повна ревізія документів, перегляд усіх стандартів та оновлення до останніх версій. Оцінка ефективності використання політик безпеки на підприємстві і визначення їх слабких місць.

Міжнародні стандарти та компанії: В даному випадку приділяється висока увага що до відповідного дотримання міжнародним стандартам у відповідній сфері та вимогам типу GDPR або інших [20].

В даному аспекті важливо постійно проводити оцінки та оновлення як технічної частини так і стратегій інформаційної безпеки, постійне оновлення документації, протоколів та інструкцій безпеки.

Висновок до першого розділу.

В цьому розділі було проаналізовано основні поняття та принципи корпоративного управління інформаційною безпекою. Розглянуті такі терміни як триада CIA це – конфіденційність, цілісність та доступність, та те що вона являє собою базис безпеки для усіх сучасних компаній. Крім цього окремо було розглянуто два підходи до побудови інформаційної безпеки в організації «знизу в гору» та «згори до низу», розглянуті їх переваги та недоліки на які слід звертати увагу при побудові систем захисту. Окремо ще було розглянута безпека Інтернету та мережі і захист кінцевих пристроїв.

Окремо був проведений аналіз міжнародних стандартів та рамок управління інформаційною безпекою. На даному розглядалися стандарти ISO 27XXX – серії, ISO 22301 – вимоги до систем управління неперервністю бізнесом з аспектами безпеки, стандарт NIST SP 800-53, британські стандарти серії BS 7799-1,2,3. Крім стандартів були розглянуті закони та регламенту GDPR, HIPAA, PCI DSS та FISMA. В даному підрозділі окремо був проведений аналіз ISO 27001 який на пряму пов’язаний з СУІБ, його основна мета та підхід до забезпечення інформаційної системи.

Та під кінець проведено порівняння ISO 27001 та ISO 27032.Ці стандарти хоч і мають різні цілі але тісно пов’язані між собою. В той час як 27001 націлений на вимоги для створення СУІБ то 27032 за допомогою рекомендацій направляє керівництво з кібербезпеки. Це дозволило визначити для чого саме краще підходить кожен з цих стандартів.

В останньому підрозділі були розглянуті та проаналізовані існуючі методи оцінки ефективності корпоративного управління інформаційною безпекою такі як: Аудит інформаційної безпеки, оцінка ризиків, проведення пентесту різних рівнів складності та інші.

Розділ 2
СТАН КОРПОРАТИВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УКРАЇНІ

2.1. Аналіз сучасного стану корпоративного управління інформаційною безпекою в Україні

В Україні процеси формування нормативно-правового регулювання корпоративного управління починали своє утворення ще з 90-х років. Хоч це і дозволило прийняти нормативну базу що розширила певні можливості але від цього стало не менше проблем. З інформаційною безпекою в певному сенсі все залишається на середньому рівні.

Дана проблема по різному виглядає в компаніях та організаціях. В державних – ця проблема в основному страждає від нестачі бюджету, незацікавленості якоїсь із сторін, бюрократичній тяганині або недосвідченості працівників що працюють там. В свою чергу в приватних компаніях теж є певна проблема з бюджетом, але в даному випадку там більш гнучкіше вирішується дане питання, бюрократичне питання спрощене та не потребує велику кількість паперової роботи та звітності за кожний крок, а стосовно досвідченості працівників це залежить в людини що займається рекрутингом та тренінгами. В даних організаціях більше зацікавлені в отриманні та збереженні цінних кадрів через їх ефективність та досвід [20].

Якщо розглядати стан корпоративного управління ІБ в Україні треба одразу розділяти корпоративний та державний сектори. Бо вони мають різні цілі та зацікавленості у своїй сфері. Не слід стверджувати що в державних все настільки погано і з них треба тікати, існують певні підрозділи та організації в яких керівник знає як правильно розпорядитися усіма наявними ресурсами та має хист до привернення «позитивної уваги» та правильному підході до керування персоналом саме як активом, а не людьми або колегами.

В приватному секторі існує трохи інший аспект хоч і в державних таке теж як не кваліфікований керівник, в державних структурах є певного роду фільтр, керуючи бухгалтерією в відділ управління інформаційної безпеки перейти буде не реально, без наявності диплому, сертифікатів та досвіду. В корпоративному секторі дана проблема зустрічається рідко і тільки в не спеціалізованих компаніях. Ще слід зазначити що по факту в обох типах організацій завжди існує загальна схожість активі, але кожна компанія підлаштовує її під свої потреби та завдання (рис. 2.1) [20].

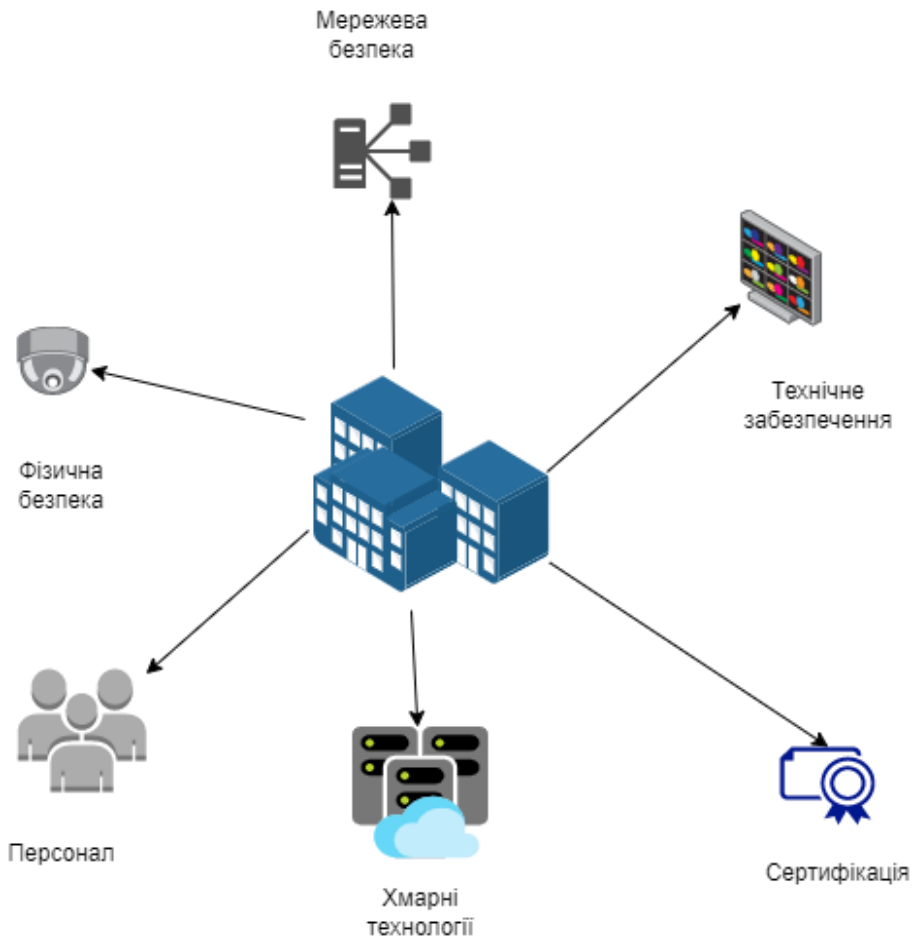

Рис. 2.1. Активи компанії

В компаніях що пов’язані з інформаційною та кібербезпекою або компанії розробники програмного забезпечення проходять жорсткий відбір під час співбесіди та тести на перевірку знань. Даний хід дозволяє відсіяти ще на етапі відбору і вже далі формувати даний актив під певні процеси або задачі. В

неспеціалізованих компаніях для яких інформаційна безпека не пріоритеті, в певному роді відбувається хаос і вони не пройдуть жодну сертифікацію з будь-якого стандарту, але для більшості це може взагалі не грати ролі.

Звісно в державних спец структурах даний аспект знаходиться на досить високому рівні через їх рівень фінансування та особлива увага у відборі кадрів, як керівного складу так і звичайних працівників, через це їх показник контролю інформаційної безпеки знаходить на найвищому рівні на відміну від інших компаній в приватному секторі та державних [20].

Слід зазначити що в Україні досить високий рівень досвідчених спеціалістів з інформаційної та кібербезпеки як в цивільному, державному та військовому секторі. Завдяки хорошим закладеним базам під час навчання в університеті, допомоги в саморозвитку в напрямку якому зацікавлений студент та навчально-матеріальній базі та молодим викладачам які націлені на актуальні технології в даній сфері. Це стає хорошою основою та мотивацією та інколи створює нелінійне мислення при виконанні певних завдань.

В даний момент Україна на межі вступу у Європейський союз і це хороший знак бо в найближчий час усі від усіх компаній вимагатимуть повне дотримання GDPR. До цього моменту за звичай вимагали дане дотримання для компаній які займалися аутсорсингом і розташовувалися на території Європейського союзу. Як приклад можемо взяти компанію що розташовувалася в Україні але при цьому мала офіс який займався рекламою в Гамбургу, Німеччина, даний підрозділ цілком підпадав під цей закон, та від нього вже вимагалося дотримання усіх норм [21-22].

Через певні фактори нестабільності на даний момент організації в Україні в основному спираються на актуальні міжнародні стандарти та закони нашої країни. Хоча більшість віддає пріоритет міжнародним стандартам бо це є певною конкурентною перевагою маючи повну сертифікацію з певного стандарту можна виходити на зовнішній ринок та проводити вже там власні бізнес процеси та інші рухи.

Але не слід виключати державні органи, хоч в основному вони і прив’язані до законодавства України, але після досягнення відповідного рівня вони починають все більше спиратися на міжнародні стандарти та потроху готувати усю технічну, програмну та документаційну частину до роботи з GDPR та інших Європейських законів пов’язаних з інформаційною безпекою [21-22].

Як недавній приклад кібератака на мережу Київстар яка почалась з ранку. Це дозволило повністю вимкнути доступ абонентам до системи зв’язку на довгий проміжок часу. Але крім цього було проведені атаки на інших операторів мобільного зв’язку таких як Vodafone та інтернет банку Mono. Двоє останніх встигли відреагувати на даний інцидент та зменшити його вплив на увесь процес роботи, але не без наслідків. У випадку з Київстаром почались збої з терміналами для поповнення мобільних рахунків які обслуговував оператор та деякі проблеми у роботі терміналів ПриватБанку.

Слід зауважити що даний стан в загалом залежить від бажання та цілей кожної окремої компанії та організації, а от у випадку державних організацій такого бути не може по причині зобов’язань у дотриманні нормативно-правових вимог законодавства.

2.2. Аналіз впливу основних факторів та викликів на ефективність управління інформаційною безпекою у країні.

Перше що слід зазначити Інформаційна безпека це досить динамічна галузь, як спеціалісти що займаються її розвитком вкладають всі сили в розробку нових технологій так і зловмисники не сплять та знаходять різні способи для проникнення в захищений периметр організації, створюючи нові загрози та виклики для захисників [24-25]. То ж слід визначити які саме фактори та виклики можуть створити вплив.

Різке зростання кількості та якості кіберзагроз: В даному випадку загрози кібербезпеки ростуть пропорційно до рівня технологій які розвиваються.

Зловмисники постійно вдосконалюють власні навички та програмне забезпечення, створюють нові методи, покращують минулі, змінюють та переосмислюють підходи до певних аспектів та сучасного захисту.

Хмарні технології: Більшість сучасних процесів переведені в хмарні технології, що само по собі спрощує технічну сторону для клієнта і дає можливість отримати данні з будь-якої частини світу або ж запустити тестовий сервер. Зі сторони компанії це прибуток за рахунок неймовірного об'єму як накопичувальних так і обробляючих ресурсів які здаються в оренду [24].

Штучний інтелект, боти та нейромережі: Даний аспект дозволяє нам в деяких моментах покращити, а інколи взагалі автоматизувати обробку даних або процес. Але на даний момент штучний інтелект не настільки розвинутий що б взагалі замінити людину в процесах типу управління інформаційної безпеки або самої кібербезпеки. Хоча слід зазначити що ШІ та нейромережі зараз активно використовують для підробки даних, відео та фото контенту, це може викликати серйозні проблеми в майбутньому коли вона навчиться створювати ідеальні підробки. Боти в свою чергу використовуються для соціальної інженерії, оптимізації певних процесів та різного роду соціальних активностей.

Нормативне регулювання та контроль: З певної точки зору даний процес іде тільки на користь компаніям та організаціям, посилюючи рівень захисту та безпечності користування. Але слід звернути увагу на закон CLOUD який в разі потреби вимагає передати усі данні стосовно певної людини, її особисту переписку та інші данні [24].

Людський фактор: Знання та досвід працівників, враховує усю його цінність, та можливі ризик зі сторони соціальної інженерії та фішингу [25].

Державні агенти: В більшості випадків одні з найсильніших хакерів які можуть створити загрозу контролюються державою. Вони досить гострий інструмент, який можна використовувати як проти сусідніх держав так і проти певних компаній. Їх спектр кібератак та ресурсів майже не обмежений і їх дії можуть починатись від розвідки та шпигунства до виведення з ладу цілих атомних станцій.

Захист персональних даних: в даному випадку це вже вимагає сам користувач, та посилення даних вимог зі сторони законів, для забезпечення усіх процесів згідно тріади CIA [1-3].

IRaaS або ж Incident Response as a Service: це послуга від сторонніх компаній що дозволяє зменшити навантаження та час реагування на інциденти кібербезпеки. Вона дозволяє мінімізувати загрози, та як найшвидше відновитися від даних зловмисних дій [26].

Економіка: стабільність та фінансова доступність ресурсів є тим самим впливом на розвиток усієї організації та особливо відділу управління інформаційної та кібер безпеки.

Керівний склад: Це досить чутлива тема та виклик водночас, в багатьох випадках на керівні посади можуть потрапляти колишні працівники які довше всіх протрималися в організації та стоять на доброму рахунку у керівництва. Але з цього і виникає проблема що в них самих нема ані лідерських здібносте ані досвіду взагалі керування. Також слід зазначити що існують різні типи людей одні здатні гарно керувати інші ж виконувати якісь одні цільові завдання [25,27].

В цьому і стає виклик для організації в досвідченості, відповідальності та розумових здібностей даного прошарку з ієрархії управління організації. Даний виклик слід розглядати окремо через причину що хоч вони і працівники, але займають набагато вищу ланку і несуть відповідальність не тільки за свою роботу, а і за процеси та завдання які виникають у його підлеглих.

Політика компанії: Це певний набір документів, лозунгів та технічних рішень які застосовуються в компанії для рішення ти чи інших завдань, не правильне написання документа, не правильне його трактування або ж рішення можуть призвести до наслідків які можуть принести збитки [25].

Технічне забезпечення: В даному аспекті високі вимоги до технічних рішень та наявного невеликого та слабкого ресурсу можуть призвести до великої кількості проблем та витрат в основному фінансовому. Слід розглядати це питання з точки зору 1 до 3 тобто: якщо 1 це задача яка має бути виконана наприклад встановити сервер на якому буде йти обробка баз даних або робота

веб серверу то 3 це значить що ресурсу має бути, як при навантажені для трьох таких процесів для збільшення швидкості реагування та ресурсу на випадок непередбачуваних ситуацій. Цю формулу можна форматувати під різні задачі та процеси.

Захищеність будівлі: Офіс, серверна, точка обробки даних або ж інша будь-яка фізична будівля яка пов’язана з організацію. Якщо вона буде недостатньо захищена будь-який несанкціоноване вторгнення може створити загрозу із середини такі як заражені флеш накопичувачі, прослуховуючі системи або ж просте викрадення власності компанії. Організація повинна дотримуватись даного параметру бо фізичне проникнення може загрожувати великими проблемами.

Конкуренти та партнери: В даному випадку йдеться про те що конкуренти можуть стати досить серйозною проблемою, через можливу не добросовісну конкуренцію та можливе корпоративне шпигунство. Партнери в свою чергу можуть через власну недбалість принести шкоду та збитки вашій організації.

Внутрішня безпека: Внутрішня безпека це загальний виклик для кожної організації її дотримання кожним із співробітників є досить складною задачею, але цілком під власною та виконавчою.

BYOD: Використання особистих пристроїв (Bring Your Own Device - BYOD) і популярність споживчих технологій у робочому середовищі створюють додаткові точки входу для потенційних загроз.

Спираючись на зростання популярності особистих мобільних пристроїв і планшетів у робочому середовищі це може стати точкою входу для кіберзлочинців, які можуть використовувати незахищені пристрої для доступу до корпоративних ресурсів.

Як варіант рішення даної проблеми це розробка стратегій BYOD, включаючи використання технологій контейнеризації, аутентифікації двома факторами, та регулярного аудиту пристроїв для виявлення можливих загроз.

Зростання обсягу та складності мереж:

Розширення обсягу мережі та складності архітектури підприємств вносить додаткові виклики в області моніторингу та захисту.

Через розширення мережі організації, включаючи хмарні та розподілені середовища, вимагає ефективного моніторингу, захисту трафіку та виявлення аномалій. Можна застосувати до цього використання рішень з моніторингу та аналізу мережевого трафіку, сегментація мережі, та впровадження заходів для захисту хмарних ресурсів.

Віртуалізація та контейнеризація:

Використання технологій віртуалізації та контейнеризації робить важливим відповідне забезпечення та захист віртуальних середовищ.

В даному випадку віртуалізація та контейнеризація змінюють архітектуру та динаміку інфраструктури, що може створити нові вектори атак. Через це застосування безпекових практик для віртуальних та контейнеризованих середовищ, включаючи використання ізольованих контейнерів та регулярне оновлення віртуальних образів [28-29].

Нові технології:

Використання нових технологій, таких як Інтернет речей (IoT), штучний інтелект (AI), блокчейн тощо, вносить нові можливості, але також створює нові вектори атак. В даному випадку використання нових технологій, таких як Інтернет речей (IoT) та штучний інтелект (AI), може вимагати нових методів захисту та виявлення загроз.

Відповідно працівники повинні проводити активне вивчення та впровадження безпекових стандартів для нових технологій, моніторинг великих обсягів даних, та використання аналітики для виявлення аномалій.

Великі дані та аналітика:

Обробка великих обсягів даних вимагає високого рівня безпеки для захисту від несанкціонованого доступу та зловживань.

При збільшення обсягів даних вимагає ефективного забезпечення їх конфіденційності, цілісності та доступності. Слід використати рішення для

шифрування даних, контролю доступу, та розвиток стратегій аналітики для виявлення патернів та аномалій.

Брак стандартизації в галузі кібербезпеки:

Відсутність стандартів та єдиної системи стандартів у галузі кібербезпеки створює труднощі в уніфікації підходів та обміні інформацією між організаціями. При відсутності єдиної системи стандартів у галузі кібербезпеки може ускладнись обмін інформацією та співпрацю між організаціями.

Через це слід зайнятися впровадженням внутрішніх стандартів, використання відкритих стандартів, та участь у спільнотах для розробки стандартів.

Зменшення часу на реагування:

Умови для оперативного реагування на інциденти безпеки постійно скорочуються, що вимагає вдосконалення процесів виявлення та відновлення.

Через це виникає досить сильна вимога до швидкого виявлення, аналізу та відновлення після інцидентів збільшує тиск на команди забезпечення безпеки.

Впровадження автоматизованих систем виявлення, реагування та тренування персоналу для ефективного реагування, та постійне вдосконалення процесів відновлення може покращити дану ситуацію в компанії.

Аутсорсинг та постачальницький ланцюг:

Включення сторонніх партнерів у ділові процеси створює нові точки атак та підвищує важливість безпеки в постачальницькому ланцюзі.

При залученні сторонніх постачальників можуть створитись нові точки атак і збільшити ризик для конфіденційності та цілісності даних.

Постійне проведенні аудит інформаційної та кібер безпеки постачальницьких ланцюгів, встановлення стандартів безпеки для постачальників та управління ризиками взаємодії з постачальниками допоможуть у зменшенні та запобіганню базових проблем які вони можуть принести в компанію.

Нерівномірний розвиток області кібербезпеки:

Різниця у рівнях технічної зрілості та кіберзахищеності організацій створює різницю в рівні загроз та вразливостей в екосистемі. В даному випадку вирішенням цієї проблеми може стати співпраця з іншими організаціями, обмін інформацією про загрози, та активна участь у спільнотах для підвищення загальної кібербезпеки.

Все це є базовими факторами та викликами які впливають на саме управління інформаційною безпекою в країні. Звісно вони можуть доповнюватись та змінюватись. Через це і стоїть пріоритет на постійне оновлення стратегій та підходів за для зменшення впливу даних факторів.

2.3. Ключові показники ефективності корпоративного управління.

Після перелічених вище факторів кожна відповідальна компанія потребує розуміння того, чи дійсно всі виконані процеси були правильні та мають відповідний ефект. Через це і було наведено перелік певних факторів які мають вплив на організацію. Дані показники можуть змінюватись та підлаштовуватись під певні вимоги організації та корелюватися відповідно до їх потреб. Розглядаючи кожний з них окремо слід пам’ятати що вони лише частина всього впливу які вони привносять в організаційні процеси. Комплексний огляд даних показників, це одна з основних задач після того як все було налаштовано та встановлено, але слід пам’ятати що для більш об’єктивної та правильної оцінки даних результатів слід що б пройшов певний час та отримати відгуки від кожного працівника, керівника та клієнтів організації. Але треба розуміти те що деякі з наведеного переліку можуть з’явитись через певний проміжок часу.

Починаючи з початку то одним з найголовніших показників є правильно побудована мережа з усім розмежуваннями, як фізично так і логічно це дозволяє оптимізувати з максимальною силою усі ваші процеси обміну інформацією, безпекою та саме навантаження на мережу [30-32].

Розглянемо більш детально даний показник. При закладанні організації ми окремо розробляємо концепцію мережі та безпеки. В деяких випадках нею нехтують та вже пізніше проводять її закладку по факту наявних ресурсів, приміщень та працівників. Це не правильний підхід, але в деяких випадка відсутня серйозна потреба в цьому або ж матеріально фінансове забезпечення на даний захід [30-32].

Тож почнемо з початкової стадії, виникла потреба у побудуванні правильної мережі та відповідно її безпечності для використання в компанії. В першу чергу визначається чи потрібні послуги аутсорсингу, тобто просто орендуємо сервер та послуги хмарної платформи та оплачуємо її. Це досить простий крок у для організації та користуванні, але може сильно бити по фінансовій стороні [30-32].

Початок побудови системи іде з формування концепції, вимог та наявних ресурсів в подальшому переходить до опису усього у паперовому виді з майбутнім переходом у фізичний стан.

Що ж нам дає правильне побудування мережі логічно – в першу чергу це розмежування різних відділів, бухгалтерія не може отримати доступ в технічний відділ і навпаки. Тобто прописуються правила користування нею не на словах, а технічно. Даний крок дає змогу розділити та керувати даними відділами та процесами окремо і в разі атаки на один з них зменшити вплив на усю систему та певні важливі сегменти [30-32].

Таким чином ми можемо отримати окремі сектори які можна контролювати та налаштовувати не привносячи радикальні зміни в усю систему та не впливаючи на процеси в середині (рис. 2.2) [30-32].

Крім цього як необхідне доповнення ми повинні зробити Демілітаризовану зону (ДМЗ) тобто це дозволить нам підвищити безпеку, надаючи проміжний фільтр та активну систему захисту між інтернетом та внутрішньою мережею (рис. 2.2).

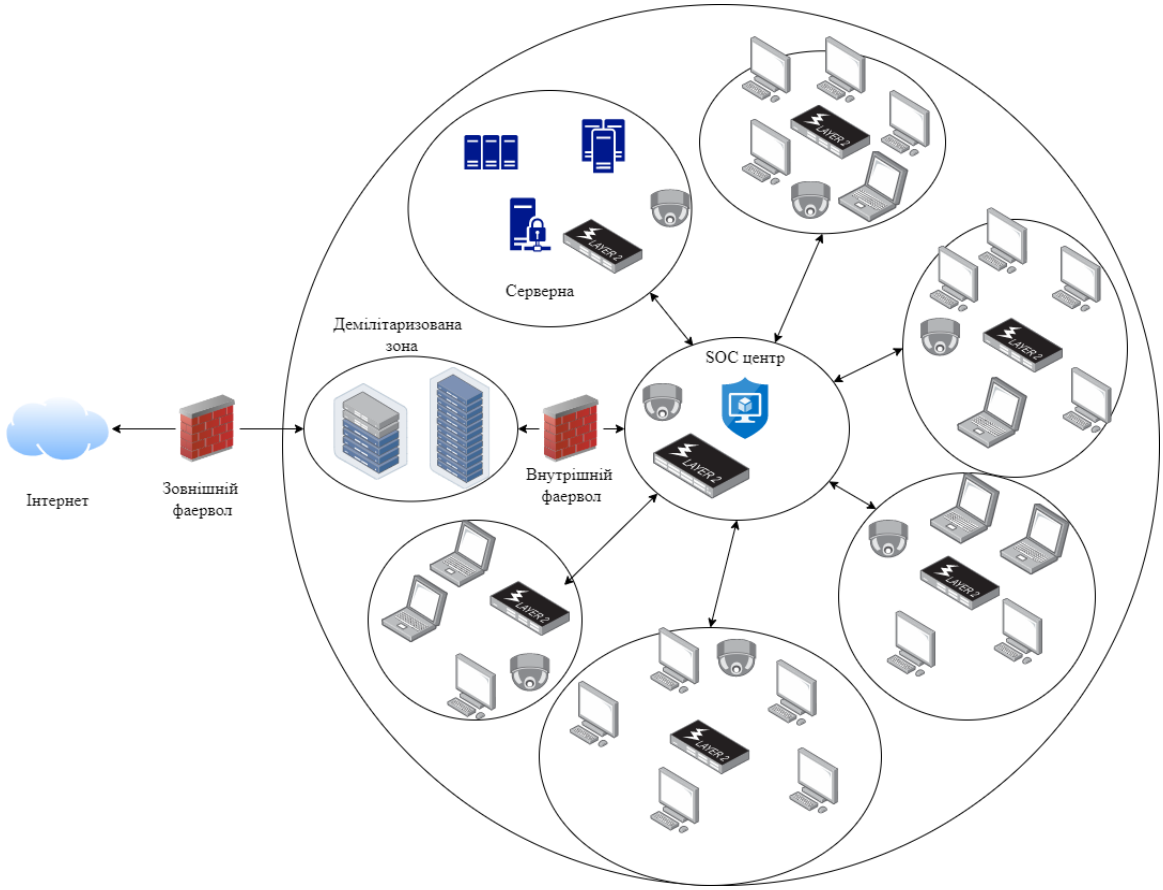

Рис. 2.2. Розмежування мережі

Це в свою чергу ускладнить можливість проникнення в неї та дасть час на реагування центру SOC на даний інцидент та прийняти дії по його запобіганню та зменшення впливу. Крім даного функціоналу це дозволить збільшити продуктивність мережі шляхом переміщення певних служб, як веб сервер на територію ДМЗ і зменшить навантаження внутрішньої мережі та відповідно покращить загальну мережеву продуктивність.

Крім усього наведеного почтові сервери, віддалений доступ та веб-сервери можуть використовуватись в ній. Та бути під постійним контролем задля безпеки внутрішньої корпоративної мережі [30-32].

Але слід взяти до уваги окремо побудову внутрішньої мережі на рівні кожного відділу. Спочатку слід визначити тип передачі сигналу та його актуальність в даному відділі, якщо це відділ графічних розробок і тд., приміщення в якому допустиме використання BYOD і відсутня обробка конфіденційної або корпоративної таємниці допустимо використовувати

WLAN(Бездротова локальна мережа). Але в даному випадку слід обмежити його зону дії та розмежувати від інших мереж. У випадку якщо це конференц зал можна використовувати гостьову бездротову мережу, але її головною особливістю повинна буди відсутність контакту з основною. Дротову мережу LAN слід проводити у вигляді розеток і розраховувати на кількість робочих місць та їх розташування в кабінеті та додавати запас у кількості 3-6 штук. Це дозволить у будь-який момент встановити ще кілька робочих місць та не створювати відповідно проблем для інших працівників [30,33-34].

Наступний етап це більше технічна частина проведення налаштувань та побудови VLAN(Віртуальна локальна комп'ютерна мережа) для технічного обмеження доступу в разі проникнення зловмисника із середини. Крім цього слід підготувати резервне електропостачання та мережі Інтернет. В даному випадку можна скористатися оптоволоконним терміналом та компактним джерелом живлення [33-34].

Позитивні відгуки клієнтів, даний аспект є запорукою конкуренто здатності компанії. Кожний клієнт це крок до успіху компанії та її популярності їх відгуки та рекомендації іншим людям допомагають скласти позитивну думку стосовно товарів та послуг і це в свою чергу зіграє на зацікавленості з боку інших організацій до вашого статусу та конкуренції яку ви можете їм скласти. Один клієнт приведе двох і так далі. Але слід зауважити що потрібно збирати усі відгуки як позитивні так і негативні. Це дасть більш реальну картину того як відбуваються певні окремі процеси, їх позитивні та негативні сторони і дозволити покращити або ж прорекламувати як особливу сторону організації.

Хороші стосунки та контракти з державою – це найкраще підходить для великих та середніх організацій і покаже усім що ви дійшли до високого рівня конкуренції, та готові переходити до держзамовлень, бо зазвичай там йдуть досить великі гроші, а відповідно і ризики які ви готові прийняти та понести відповідальність в разі виникнення проблем через них.

Даний аспект дуже складний по багатьом причинам:

1) дотримання міжнародних стандартів та законів країни або союзу;

2) професіоналізм співробітників;

3) навичок нести відповідальність за власні дії;

4) готовність вкластися в умови та терміни визначені державою;

5) своєчасне реагування на події та міжнародне становище;

6) постійна участь у різних конференціях та подіях на яких є можливість проводити власні доповіді;

7) бути готовим для проходження перевірок від служби безпеки країни окремих працівників або ж цілком усієї компанії.

Дотримання цього переліку відкриває перед компанією великі можливості у розвитку в середині країни, через створення конкурентоздатності та підтримки держави, то ж вони дісталися майже вершини. Цей перелік це певного роду іспити що перевіряє компанію та їй персонал на міцність та стійкість їх духу.

Автоматизована робота SOC. Це відноситься більше до технічної та програмної частини. Якщо компанія автоматизувала усі процеси та пришвидшила усі доступні процеси за допомогою певних систем це вже є причиною для гордості. Це свідчить про те що кожний у вашому відділі є професіоналом своєї справи та готовий займатися саме своєю справою без відволікання на інші повсякденні проблеми роботи системи.

Розглядаючи це в перспективі інформаційної та кіберзахисту слід зазначити шо кількість векторів атаки рівна до кількості рішень захисту. За для правильної побудови мережі слід брати NGFW (Next generation firewall) для кінцевих точок EDR (end-point detection and response) та SIEM (Security information and event management) для загального моніторингу мережі.

Маленька плинність кадрів це запорука сильної компанії, бо це значить що її колектив це одне ціле і кожен знає що слід очікувати одне від одного. Готовність підмінити когось або ж допомогти йому у складний час сильна сторона кожного працівника. Саме найголовніше що б керівництво не нехтувало потребами працівників у робочих процесах та їх особистих потреба це дозволить зайвий раз уникнути двох проблем.

Перша це незадоволений працівник який може зробити певні дії для принесення шкоди компанії. Друга - це його звільнення і тоді керівнику відділу потрібно буде шукати спеціаліста такого ж або трохи нижче рівня та заточувати під певні задачі.

Постійне інформування працівників та їх досвідченість. Навчання, тренінги та корпоративи, тобто залучення працівника та його особистості до закладання успіху компанії та формування сильного та розумного колективу буде запорукою до успіху компанії [35].

Прокачка таких навичок як Hard skill (розвиток компетентності) та Soft skill (компетенція) - це певного роду система яка націлена на працівника для розвитку його відповідальності та компетенції відповідно до його робочого положення та задач встановлених в організації (рис. 2.3). Даний процес досить складний та потребує певного часу та немалих зусиль. Цей розвиток за звичай підпадає під компетенцію відділу human resources. Компетенція включає в себе певний ряд індикаторів «що, як та чого не», але він досить відносний і залежний від різних умов в компаніях. По факту вона включає в себе п’ять складових: знання, навички, я-концепція, якості та мотиви. Як показала практика їх слід оцінювати разом, в деяких компаніях є певна пріоритетна характеристика яку керівництво хоче бачити в співробітниках то їм простіше віднайти її ніж виховувати у вже наявних співробітниках [35].

Тому слід приділити досить серйозну увагу при виборі рекрутера, який в свою чергу буде збирати, аналізувати анкети та резюме майбутніх співробітників. Після процесу обробки та тестувань він наддасть ці данні керівництву відділів та компанії від яких і буде залежати рішення.

Слід окремо розглянути модель самої компетенції, це алгоритм згідно якого в майбутньому проводиться оцінка працівників та керівників.

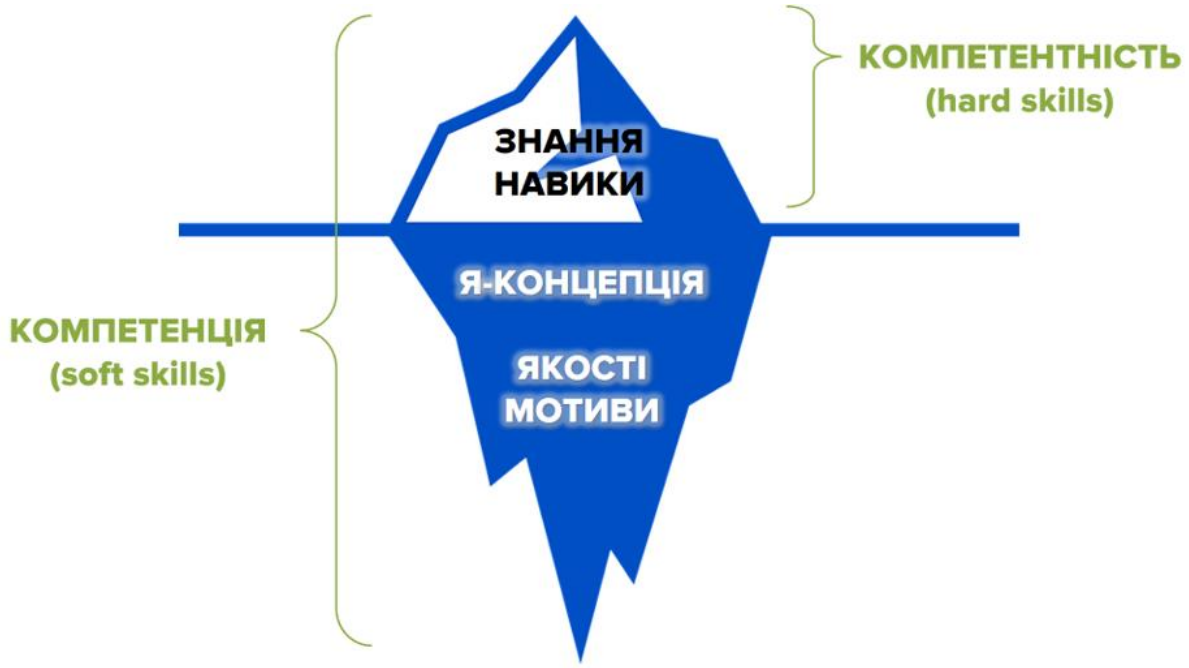

Рис. 2.3. Порівняння навичок [35]

В даному випадку її можна описати як таблицю з кількома рівнями, починаючи від -1 до 3, де в свою чергу -1 це повне нехтування своїми обов'язками та не дотримання поставлених завдань і 3 це ідеальне виконання поставленої цілі, передбачення майбутніх подій та ринку. Це спосіб дозволяє оцінити кожний процес, та правильно підготувати майбутнього спеціаліста або ж просто замінити його на більш компетентного та відповідального працівника [35].

За допомогою цієї концепції можна сформулювати майбутні вимоги від спеціаліста та підготувати для нього індивідуальний підхід та навчання згідно його знань та компетенції. Але цю модель можна використати більш широко та виставити внутрішні характеристики для кожної з посад окремо. Тобто створити картку в якій вказано декілька пунктів як наприклад [35]:

1) командна робота;
2) ефективна взаємодія;
3) саморозвиток;
4) організація робочого процесу;
5) розуміння процесів досягання цілі;

6) ухвала рішень;

7) комунікація;

8) мотивація.

Але вона все ще залишається модульним рішенням для компанії, її візуальне зображення може спростити вибір кандидата на певну посаду та дозволить зробити правильний вибір [35].

Слід зазначити потрібно ще дотримуватись етичного управління ризиками, тобто у разі виникнення інциденту, не варто звинувачувати та вести себе хамовито. В даному випадку слід підійти більш комплексно та відповідно до рівня компанії. Під цим мається на увазі що будь-яке звинувачення має бути етичним та виражати конкретне порушення з дотриманням усього професійного кодексу. Завдяки цьому можна уникнути великої плинності кадрів та непорозумінь в команді. Як приклад керівник відділу не має права звернутися до співробітника в агресивній формі якщо він виразив свою думку стосовно певної проблеми пригнічення особистості або як його ще називають булінгом не припустимо в жодній формі [36].

Мінімальний час простою серверу, тобто це наближення до найменшого можливого часу коли сервер не працює. Даний пункт за звичай не виноситься на суспільний огляд бо є досить чутливою інформацією для компанії, але його важливістю не слід нехтувати. Через дану затримку в робочому процесі ми можемо отримати великі проблеми в багатьох аспектах [37]:

1) скорочення доходів, кожен раз коли ваш сервер з CRM або Cloud-сервіси відключаються хоч на пів години, раз в місяць це вже викликає велику проблему та втрату у доході компанії, особливо це стає критично в разі відмови більше ніж на годину у пік навантаження сервісу клієнтами якщо ви торгова фірма. Через це компаніє може нести великі фінансові збитки;

2) репутаційна втрата, в даному випадку все досить просто клієнт що не може терміново замовити річ на вашому сайті через його відключення, не буде рекомендувати вас та поширювати негативні відгуки стосовно вашої компанії;

3) втрата даних, ось становить найвищу загрозу, втративши дані клієнта або дуже чутливу інформацію без можливості відновити ми отримуємо самий найбільший удар по компанії, бо це може потягнути за собою юридичні, фінансові та фізичні втрати, починаючи від співробітників закінчуючи судовими процесами.

В даному питанні слід розуміти що ризики можуть бути різні починаючи від технічної частини, закінчуючи кібератаками на об’єкти обробки інформацією та сервери вашої компанії [37].

Ідеальна відповідність міжнародним стандартам та робота з компаніями що реагують на кібератаки.

В даному випадку йдеться про відповідність стандартам типу ISO/IEC та іншим. Завдяки цьому компанія отримує окрім визнання в міжнародному IT середовище що вони дійсно дотримуються усіх вимог та використовують досвід компаній та організацій. Крім цього самі допомагають у розвитку даних стандартів та роблять власний вклад в захист та розвиток міжнародної коаліції по боротьбі із кіберзлочинністю. Передаючи самі актуальні дані про спроби вторгнення та виявленню атак типу Zero Day вони допомагають у покращенню стандартів та законів країн та союзів [38].

Як додаткова позитивна сторона це робота з командами виявлення загроз та злочинів в кібер просторі по типу CERT-UA. В даному випадку це урядова компанія з реагування на надзвичайні події з кібер випадків в Україні, яка в свою чергу функціонує в складі служби Державного спеціального зв’язку та захисту інформації України. В завдання якої входить [38]:

1) накопичення та аналіз даних про кіберінциденти та ведення державного реєстру стосовно цього;

2) надання власникам таких об’єктів практичної допомоги та консультацій у виявленні та усуненні наслідків від атак;

3) організації та проведення семінарів з питань кіберзахисту;

4) розміщують на офіційному веб-сайті рекомендації стосовно актуальних кіберзагроз та протидій ним;

5) робота з правоохоронними органами та відповідно інформування про атаки;

6) робота з іноземними організаціями з питань реагувань на такого типу інциденти та роботу з командою форуму FIRST;

7) взаємодія з українськими командами по реагуванню на кіберзлочини.

Крім зазначеного переліку дана організація має ще багато пунктів стосовно своєї роботи та пов'язану з нею нормативно-правову базу яку використовує з ціллю захисту та поширенню інформації про кіберзлочини [38].

Підсумовуючи це, слід зазначити що для кожної компанії даний перелік може змінюватись в залежності від їх потреб, завдань та цілей. Ці показники по своїй суті є базисом для розуміння чи дійсно задіяні алгоритми, процеси та заходи були успішні по відношенню до компанії, або ж певного відділу та принесли свої плоди у вигляді автоматизації, позитивних відгуків або ж активності та розвитку персоналу.

Будь-які дії будуть так або інакше впливати на увесь організм компанії як єдине ціле, одна з основних проблем з якою дійсно кожен день зіштовхуються компанії це плинність кадрів та відповідно їх компетентність ставить під сумнів навички їх керівника. Як приклад студенти які приходять працювати в компанію потребують специфічного підходу та навчання через свою юність та не досвідченість в багатьох аспектах.

Не слід забувати і про старих працівників, вони є кістяком команди яка веде компанію вперед, їх досвід та навички задіяні у всіх процесах, не слід їх перевантажувати безглуздими завдання лиш заради роботи. Але є ще один нюанс про який забувають майже усюди і це інтерес та знання працівника його роботи. Для керівника за звичай це менш критично бо вони зіштовхуються з новими завданнями кожен день, в той час як звичайний працівник вивчивши вже повністю свій алгоритм роботи буде нудьгувати на роботі та в певному сенсі відноситися до неї зверхньо. В даному випадку ми отримуємо співробітника який знає усе до автоматизму та виконує цілком успішно свою роботу, але в той же

час йому це стає не цікаво. Тож для керівника відділу випадає нове завдання вигадати нове завдання або напрямок який ще не був вивчений даним співробітником та займе його на кілька місяців для його досконального виконання.

Таким чином ми отримаємо ще один показник на який слід орієнтуватися для отримання позитивних результатів. Хоч він і тісно пов’язаний з таким пунктом я тренінги та навчання, але через те що націлений на окремих осіб він має певний характер унікальності, бо кожен з працівників різний та потребує уваги від свого керівника не тільки у постанові завдань, а і у розумінні та допомозі в розвитку професійних та власних навичок.

Висновки до другого розділу

Підсумовуючи усе вище наведене слід зазначити що сучасний стан інформаційної та кібербезпеки в Україні в різних сферах таких як державна та приватна знаходиться досить в опосередкованому стані, тобто їх рівень ще не досяг рівня європейських та американських компаній та їй ще є куди рости та розвиватися в свої напрямках.

Спираючись на наведені виклики можна зазначити що рівень технологій не стоїть на одному місці та розвивається, так і загрози і зловмисники не зупиняються у досягненні свої цілей з власних або ж інших причин. Але крім зазначених загроз ще був наведений певний перелік показників які показують ефективність та відповідний вплив на саму організацію.

Розділ 3.
ДОСЛІДЖЕННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ КОРПОРАТИВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УКРАЇНІ

3.1 Дослідження основних тенденцій та проблем в корпоративному управлінні інформаційною безпекою в Україні.

Проводячи аналіз сучасного стану корпоративного управління інформаційною безпекою в Україні слід зазначити що в даний момент можна виокремити три різні сектори: приватний, державний та корпоративний. Розвиток ІБ в кожному секторі відбувається по різному, але кожен з них націлений на конкурентоздатність та відповідно майбутній розвиток основного напряму їх роботи.

Приватний сектор в основному не настільки націлений на захист персональних даних якщо це відповідно не їх основний профіль роботи. Тобто маючи компанію малих-середніх розмірів вона в основному зацікавлена в фінансовому прибутку від свого напрямку діяльності, але все таки вона зв’язана законами держави в які вона проводить свою господарську діяльність згідно закону України №2297-VI «Про захист персональних даних» [39]. В основному вся їх діяльність стосовно інформаційної безпеки зав’язана на даному законі по причині того що їх недотримання може викликати їх до відповідальності згідно із порушення даного нормативно-правового акту. Окремо ще слід зазначити закон України «Про основні засади забезпечення кібербезпеки України» [40].

Спираючись на дані закони компанії які досить тісно пов’язані із кіберпростором зобов’язуються дотримуватись чинних законів. В даному випадку компанії малого та середнього які напряму працюють у наданні послуг пов’язаних із цим дотримуються їх та стараються поглиблювати свої знання та рівень відповідальності у рівнянні на міжнародних стандарти що би вийти на

відповідний рівень який дозволяє створити конкуренцію на ринку серед інших компаній.

Переходячи до компаній рівня корпоративного, в них виникає трохи інша ситуація, вони мають більше охоплення стосовно відповідності законам по типу GDPR та країнам в яких вони розташовуються. Рівень їх роботи знаходиться вже на міжнародному через це їм досить не вигідно втрачати репутацію через недотримання тих чи інших законів, в той час як стандарти яких вони можуть дотримуватися можуть доказати державі що вони дотримуються вищого рівня захисту, але в свою чергу більшість стандартів несуть більше рекомендаційну функцію ніж пряме зобов'язання дотримання (рис. 3.1).

В державному секторі взагалі все виходить трохи по іншому. Їх зобов'язують обов'язково дотримуватися законів держави. В більшості випадків дані закони це загальні вижимки та вимога від організацій що саме вони зобов'язані робити що б не бути притягнутим до відповідальності за порушення чинного законодавства. Через це всі державні структури повністю дотримуються їх, але для покращення тих чи інших функцій вони відповідно користуються міжнародним досвідом відповідно їх стандартами у досягненні цілей поставлених державою (рис. 3.1).

Окремо слід зазначити що корпоративний сектор що прибуває в Україну за кордону та працює на відповідно вищому рівні тож, відділи які відкриваються в нашій країні маю відповідний рівень з поправкою на вимоги законодавства. Але в більшості випадків це досить складний процес для директорського рівня, через те що відкриття може вимагати велику увагу зі сторони юридичного та відділу рекрутингу.

Переходячи на цьому етапі на проаналізовані наявні міжнародні стандарти такі як ISO/IEC, NIST, BS та відповідно законів GDPR, PCI DSS, HIPPA та інші можна визнати те що корпоративне управління інформаційної безпеки в Україні ще є куди рости, та на що саме звертати увагу фактично можна отримати вже готовий досвід через стандарти. Тож можна виділити такі основні тенденції та проблеми з якими можна зіштовхнутися

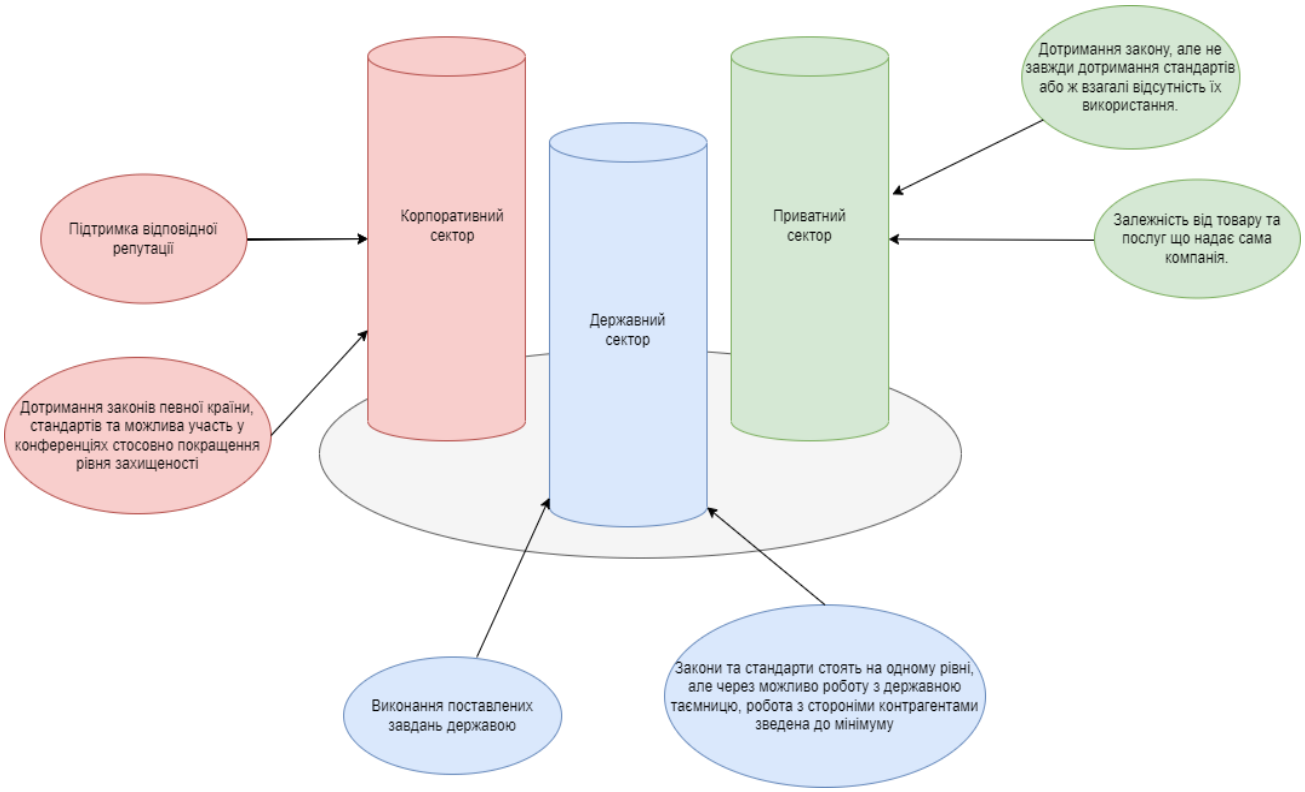

Рис. 3.1. Залежність секторів

Основні тенденції та проблеми в корпоративному управлінні інформаційною безпекою можна виділити наступним чином:

Зростання обсягу та складності загроз:

- кількість та різноманітність кібер загроз постійно та невпинно зростає з кожним роком їх кількість не зменшується, на заміну старим приходять нові та більш потужні або старі просто переформовуються або модифікуються під нові способи як соціальна інженерія.
- таким чином вони впливають на ІБ підприємства через це спеціалістам треба весь час вивчати нові способи протистояти їм та попереджати керівництво та інших працівників бути готовим до нових атак та загроз.

Загрози зі сторін інших держав:

•через своє особливе геополітичне місце Україна має як партнерів, конкурентів так і загрози видимі та ні [41];

• цілеспрямоване формування певними іноземними державами негативного іміджу України в очах міжнародних союзів або ж певних країн;

• активна критика державного керівництва України з цілю дескридитації;

• маніпулювання іншими країнами керівництвом України з ціллю отримання вигідних для них дій або рішень;

• перешкоджання розвитку в кіберпросторі так і інших напрямках Україні;

• дискредитація військово-технічного розвитку держави;

• зростання для України загроз кібернетичних атак через думку про слабкість країни та з наявними новими технічними засобами.

Дані тенденції не здаються спочатку чимось критичним для корпоративного управління ІБ але вони мають досить серйозний вплив на неї з різних сторін які простій людині не побачити і її вплив може бути дуже руйнівним і зачепити не тільки державний сектор а і інші (рис. 3.2).

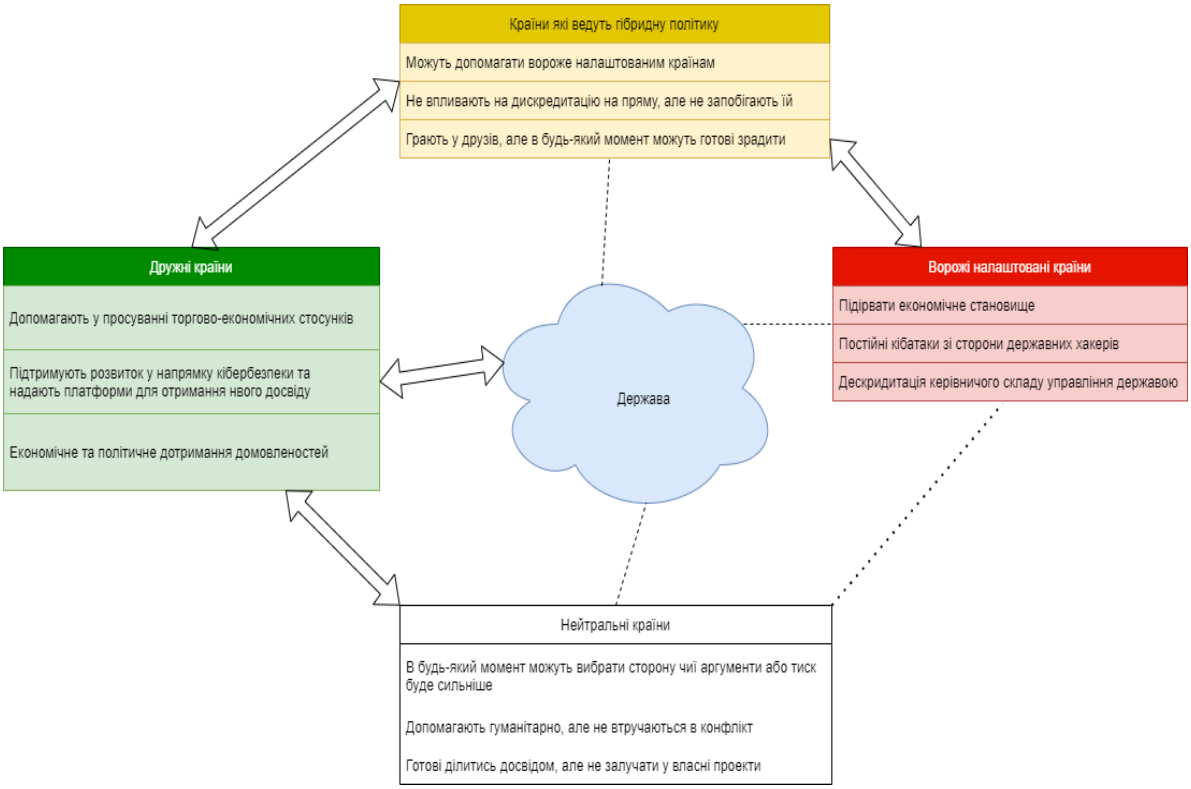

Рис. 3.2. Друзі та вороги держави

Цифрова трансформація та хмарні технології - перехід до цифрових та хмарних середовищ спрощує багато різних процесів та вимог до технічної частини, але вимагає адаптації цілої стратегії безпеки до нових методів.

Технічні рішення нового покоління - в даному випадку тенденція йде до переходу на нові види технічної та програмної частини у вигляді EDR, XDR, NGFR та інших видів. Досить велика кількість компаній віддає перевагу даному типу рішень через багаті аспекти їх використання, але проблемою сьогодення все ще стоїть те що технології рухаються швидше ніж бюджет та досвідченість працівників компаній [42].

Розвиток штучного інтелекту та аналітики - ШІ зайняв своє не останнє місце в розвитку та оптимізації багатьох процесів. Через це їх почали додавати майже усюди для підвищення ефективності роботи, в тому ж відділі безпеки це спрощує пошук аномалій та дозволяє швидше реагувати на певні інциденти.

Зміна законодавства та регуляторних вимог - через розвиток технологій та загрози з їх боку розвинуті країни почали вводити закони що б забезпечити захищеність як самої державності так і її населення. Через даний аспект вони почали вимагати від компаній на їх території дотримуватись законів які націлені на безпеку так і на те що б застрахувати державу від тероризму як приклад закон США CLOUD.

Підвищення уваги до людського фактору - в сучасній реальності майже 90% усієї інформації оброблюється людиною, але через певні можливі прогалини в знаннях або ж самої компетентності людини зникає виникають прогалини та інциденти інформаційної або ж кібербезпеки. Як продовження нестача кваліфікованого спеціаліста, через такі проблеми багацько компаній досить уважно відносяться до набору студентів на стажування та роботу [43].

Даний перелік не є остаточним на сьогоднішній день Україна знаходиться досить в скрутному становищі через величезну кількість різних факторів які впливають на неї. Через це в нас стала досить популярна тенденція до роботи на віддаленому робочому місці.

З огляду на реалії сьогоднішньої гібридної робочої сили, організаціям необхідно оцінити, наскільки добре працюють разом їхні технології управління доступом, виявлення загроз і реагування на них. Аномалії віддаленого доступу, особливо в контексті браузерів, які раніше було легше виявити, зараз набагато складніше постійно виявляти, що створює додатковий тиск як на IT-відділ, який повинен виявляти потенційні та реальні ризики, так і на самих працівників, які очікують на надання доступу для продовження своїх робочих процесів[44].

В даний момент існує кілька ключових доповнень до стратегії, які організації повинні враховувати при вирішенні проблеми гібридної робочої сили. По-перше, при роботі за принципом "найменших привілеїв" або "нульових привілеїв" ефективна обробка запитів на доступ стає критично важливою - як з точки зору продовження роботи бізнесу, так і з точки зору задоволеності співробітників (і, можливо, партнерів). Затримка із затвердженням відповідних запитів сповільнить бізнес і розчарує кінцевих користувачів. Отже, автоматизований робочий процес є ключовим у цьому відношенні. Штучний інтелект також може відігравати важливу роль у прискоренні маршрутизації запитів і навіть схвалення за дорученням [44].

Ще одним стратегічним доповненням, на яке варто звернути увагу організаціям, є впровадження політик динамічного доступу. При виявленні потенційно ризикованого облікового запису, який отримує доступ до інформації з нестандартного місця, організації повинні мати можливість динамічного коригування заходів безпеки даних, наприклад, шляхом маскування даних, щоб більш ефективно управляти ризиком в рамках певної програми або бізнес-процесу. Автоматизація цього процесу дає IT-спеціалістам і службам безпеки більше часу, щоб оцінити ризик і виробити правильну реакцію, а не реагувати на нього, не будучи повністю поінформованими [44].

У міру цього індустрія страхування розширила свої ділянки роботи і перейшла до страхування кіберінциденців через це з'являється все більше історичних даних про страхові випадки, вимоги до страхового покриття продовжують змінюватися. Це, як правило, призводить до підвищення вимог до

захисту кібербезпеки та збільшення кількості "обов'язкових умов" для придбання полісу, наприклад, multi-function authentication (MFA) та endpoint protection (EPP). З огляду на те, що галузь базується на масовому аналізі даних і виявленні кореляцій, одна вимога може не мати значного впливу (рис. 3.3) [44-45].

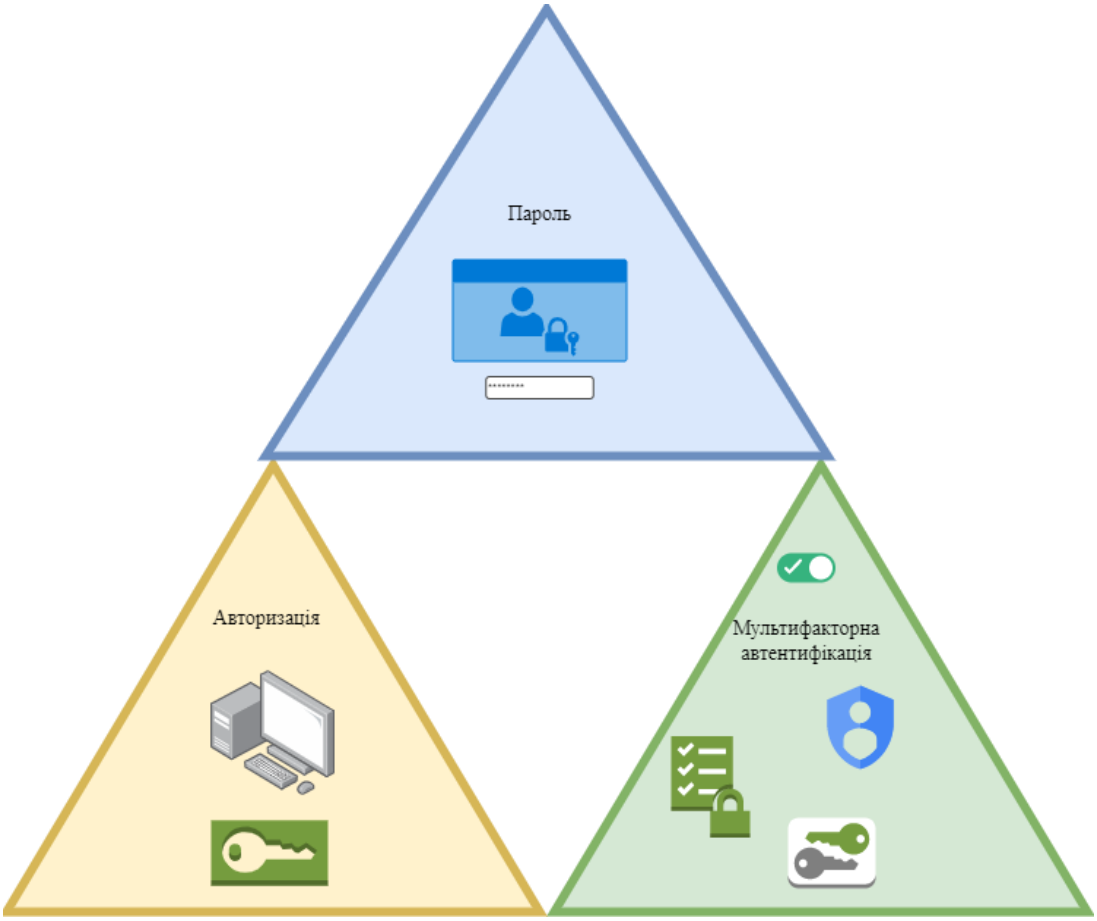

Рис. 3.3. Мульти-факторна автентифікація

Слід розуміти що до даного типу компаній з кіберстрахуванням слід ставитися, як до партнера, а не як до найкращого друга. Розвиток міцних відносин і регулярний діалог покращить як процес продовження, так і процес врегулювання збитків. Лідери безпеки повинні бути про активними і відкритими у відносинах і розповідати повну історію свого підходу до кібербезпеки, не обмежуючись заповненням заявки та анкет. Пам'ятайте: ніхто не має більше даних про ризики та збитки у сфері кібербезпеки, ніж кіберстраховики - є сенс прислухатися до їхніх порад.

На сьогодні майже всі працівники використовують мобільні девайси для роботи та обміну інформації через це і зростає великий попит у забезпеченні захисту цих кінцевих девайсів та відповідно навчанню персоналу що до їх правильного використанню. У більшості випадків мобільні пристрої представляють собою значну, некеровану поверхню атак для підприємств. Незалежно від того, чи вони належать компанії, чи є частиною стратегії BYOD, необхідність впровадження відповідних засобів контролю безпеки та навчання кінцевих користувачів щодо потенційних загроз є критично важливою (рис. 3.4) [44-45].

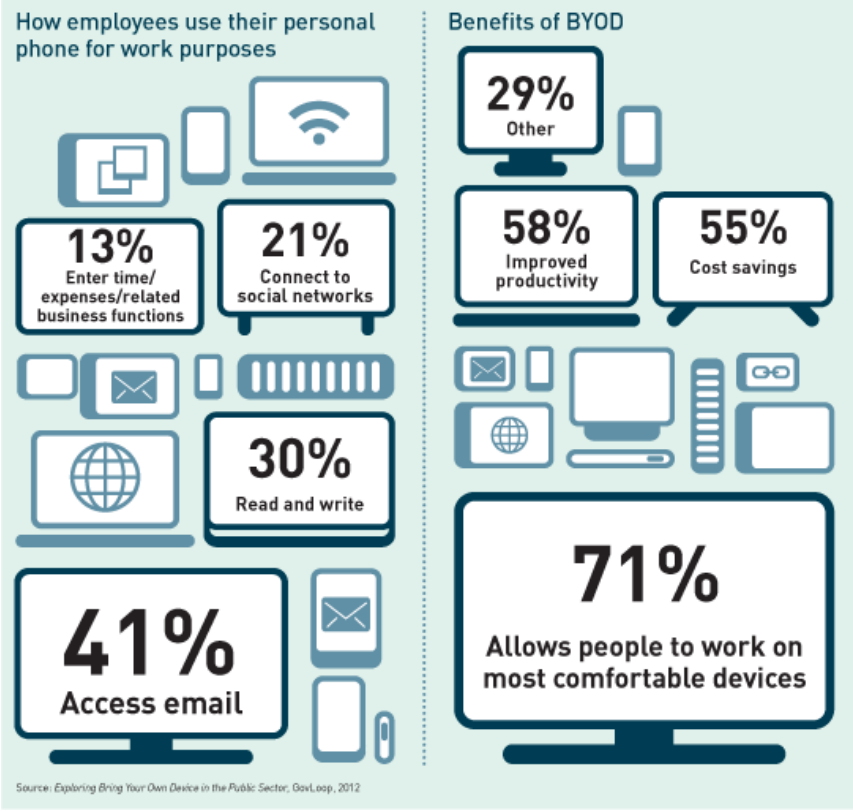

Рис. 3.4. Відсоткове відношення BYOD та інших систем [44-45]

Витоки даних один з особливих випадків Дані й надалі залишатимуться головним предметом занепокоєння для організацій в усьому світі. Незалежно від того, чи це фізична особа, чи організація, захист цифрових даних зараз є першочерговим завданням. Будь-який незначний недолік або помилка у вашому системному браузері або програмному забезпеченні є потенційною вразливістю для хакерів, які можуть отримати доступ до особистої інформації. З 25 травня

2018 року набув чинності новий суворий Загальний регламент про захист даних (GDPR), який забезпечує захист даних і конфіденційність для громадян Європейського Союзу (ЄС). Аналогічно, Каліфорнійський закон про конфіденційність споживачів (CCPA).

Слід розглянути дане питання більш детально спираючись на кілька аспектів. Перше це основна різниця між витоком даних та зламом:

Витік даних – це випадок коли третя сторона отримує неправомірний доступ до інформації, як приклад втрачена флешка або ноутбук з чутливою інформацією яку можна використати з ціллю продати, або використати в майбутній кібератаці на об’єкт. З даної точки зору виток не є сам по собі злочином, але це інцидент на який безумовно слід звернути увагу та приділити на це певний ресурс для можливого зменшення впливу [46-47].

Злам в свою чергу, це спланована, націлена на певний сегмент, або працівника атака для отримання чутливої інформації компанії чи працівника з подальшим продовженням в напрямку всієї компанії. Як приклад вразливості в ПЗ, соціальна інженерія та фізичне викрадення носії чи пристрої з конфіденційною інформацією є досить поширеним способом для отримання доступу до того що саме цікавить зловмисника.

Також слід розуміти що в кожного набору даних є певна цінність як для компанії так і злодія який націлений на протизаконні дії. Першими в даному списку йдуть ранні квартальні звіти або будь-які фінансові звіти, їх виток може призвести до позачергових змін у ринку. Другими на черзі йде операційна інформація про внутрішні зміни в організації, транзакції, накази, кількість наявних пристроїв. І останнім це виток секретної інформації, це зазвичай відбувається не досить часто, або ж взагалі даний тип інформації не оброблюється підприємством. Але це досить важливо для оборонних та аерокосмічних підприємств, через їх пряму роботу з державою. Навіть проста втрата таблиці в якій описуються які рішення та матеріали використовуються в новій моделі виробу буде критичною для організації, але дуже цікавою для інших країн або організацій [46-47].

3.2. Методика оцінки ефективності корпоративного управління інформаційною безпекою

Методика у вигляді алгоритму ASRTCU

Враховуючи все вище наведене, слід сформувати певну базову схему для правильної організації корпоративного управління інформаційною безпекою та навести певні рекомендації що дозволять покращити її та вивести на середній та вище рівень захищеності.

Тож тепер слід розглянути розроблений на основі попередніх досліджень власний алгоритм-базис ASRTCU в якому зібрана вся ця інформація, із графічним зображенням яке наддасть змогу візуально зрозуміти як проходять усі процеси:

Активи (Assets) – проводимо детальний аналіз усіх наявних ресурсів в нашій компанії, та цілі яких ми збираємось досягти та розробляємо план з уточненням усіх етапів та цілей в даному алгоритмі. З початку це дозволить нам зрозуміти що зараз є в наявності, та розподілити ці ресурси на наступні етапи з урахуванням цілі та можливістю зменшити початковий вплив на той чи інший сектор.

Таким чином ми отримуємо параметр за допомогою якого ми можемо впливати на різні частини алгоритму та віддавати пріоритет тому чи іншому в будь-якому новому циклу алгоритмах. З кожним покращенням зростає кількість та якість даного пункту що дозволяє приділити більше ресурсів на певний сектор далі.

В першу чергу слід визначити основні вимоги та активи з якими буде працювати організація це дозволить сформувати перше коло зацікавленості організації та компанії в цілому, «те за що ми боремось» або простіше кажучи наш заробіток та ключові процеси пов’язані з ним.

Як приклад можна взяти компанію по розробці програмного забезпечення. Спочатку ставиться пріоритет на сам процес розробки в який включені самі розробники та менеджери проектів. В даному випадку вони виступають активом що робить дохід компанії та відповідно їх навички та їх робочі станції за допомогою яких вони створюють програми або сайти. Їх навички, робота в колективі та особисті якості слід цінувати досить високо, та у випадку виникнення нехватки знань чи досвіду слід надати курси по підвищенню кваліфікації. Слід звертати увагу ще на забезпечення їх особистих потреб під час робочого процесу. Те саме і з проджект-менеджерами вони крім керування процесом та його побудовою ще проводять консультації з замовником. В даному аспекті критична інформація або ж корпоративна таємниця пов’язана з процесом розробки та його методами, клієнтською базою та кодом яким написано даний додаток. Отримуючи хоч якусь з цих частин зловмисник вже зможе провести певного роду цільову атаку на компанію що користується даним програмним забезпечення, а конкуренти в свою чергу зможуть розробити кращу версію свого ПЗ.

Персонал (Staff) – Один з головних рушіїв прогресу, якщо цей етап відбувається в перше то йому слід приділити увагу на обох рівнях, керівників відділів та їх підлеглих. Найкраще проводити багатоетапні співбесіди, це дозволить відсіяти «не якісні кадри», що в майбутньому зменшить появу таких ризиків як, не кваліфікований персонал та недбалі керівники. При повторному проходженні даного етапу в умовах набору нових кадрів його слід пройти повторно, а для вже наявного персоналу слід провести тренінги та корпоративи для покращення єдності та досвідченості колективу.

Після рішення о визначенні головних активів за допомогою чого та кого і відбувається фінансовий ріст компанії, слід перейти до тих хто саме займається обробкою фінансової сторони компанії. В даному випадку відділ бухгалтерії і тут вже відбуваються інші процеси та оброблюється критична інформація пов’язана на пряму з фінансовою складовою компанії. Витрати на самі базові потреби, кавоварки, заміна жорстких дисків або процесорів в ПК, може стати

корисною інформацією як для конкурентів так і зловмисників. Отримавши інформацію про заробітну плату проджект-менеджера конкурент може таргетовано проводити підривну діяльність у вигляді пропозиції про більшу заробітну плату та умови робити у себе. Тим самим переманюючи до себе досвідчених спеціалісті та дискредитуючи компанію з точки зору плинності кадрів, заробітної плати та умов праці (рис. 3.5).

Тепер ми переходимо до етапу «ті хто прокладають шлях» і це одна з проблем для персоналу може стати сам керівний склад, нерозуміння усіх робочих процесів та вимог працівників може призвести до великої плинності кадрів та недотримання термінів виконання поставлених завдань, призведуть до краху компанії. В даному випадку слід набирати та проводити кваліфікаційну перевірку відповідності вимогам та тим знанням що потребує компанія. З точки зору витоку інформації керівництво має до неї більший доступ та може бачити усю картину, через це за звичай вони і стають цілями для атак від різних зловмисників. Це може в свою чергу призвести до великих втрат як фінансових так і репутаційних (рис.3.5).

Рис. 3.5. Відділи та інформація

Досить серйозну роль грає такі поняття як інформаційна та взагалі стабільність колективу. В даному випадку це запорука росту компанії, в даному

випадку розглядається не стагнація, а розвиток зі сталим колективом або можливим його поповнення. В даному випадку до кожного працівника відділу слід відноситись як до особистості та мати свій власний підхід. Це буде один з правильних, підходів у розвитку колективу. Слід ще звертати увагу на захист та протидію впливу, зовнішніх чинників які ставлять під загрозу такі поняття як етика та стабільність[48].

Тож можна підсумувати що це потребує приділення досить великої уваги до правильного підбору персоналу та керівного складу і розуміння що та кому саме можна довірити при виконанні поставлених завдань.

Правила (Rules) – в даному секторі ми зіштовхуємося із дотриманням законів. В даному випадку все досить просто, з початку ми дотримуємось законів країни в якій розташовуємось, далі ми переходимо до союзів(як приклад GDPR у ЄС), і вже потім до стандартів. У цьому випадку дана послідовність зумовлена тим, що закони країни стоять на обов'язковому першому місці в той час як закони союзів та стандарти мають вже меншу вагу.

Наступним етапом після визначення «те за що ми боремось» ми переходимо до того «закони що нас захищають» в даний етап ми розглядаємо в першу чергу нормативно-правові акти країни в якій розташовується наш бізнес. Ми граємо по правилам країни, а не вона по нашим. Для даного аспекту треба найняти досвідченого юриста який зможе провести консультацію з тих чи інших питань та вказати на можливі нюанси в законодавстві які можуть вносити певні зміни у регламент компанії.

В даному випадку два основних закони на які будуть спиратися це «Про захист персональних даних» та «Про основні засади забезпечення кібербезпеки України» вони вказують чітко на те що саме ми повинні дотримуватись в рамках країни та відповідно зменшить можливість привернення уваги зі сторони держави та створенню негативної думки про компанію. Звісно існує велика кількість різних законів через які може виникнути колізія і викликати певні непорозуміння, тому краще завжди мати досвідчених та проінформаних про

діяльність компанії юристів, які в будь-який момент зможуть вирішити проблеми компанії.

Після цього ми зіштовхуємось із законами ЄС типу GDPR або США CLOUD, але вони застосовуються лише на території визначених країн чи союзів. Хоча слід зазначити що Україна в даний момент переходить по троху на вимоги GDPR як умова вступу в ЄС.

Існує тільки одна проблема, бюрократія, в даному випадку вона досить сильно може застопорити розвиток документації по відношенню до технологій. То ж тут ми переходимо до етапу «досвіду інших» тож їм на доповнення приходять такі поняття як стандарти, та відповідні компанії що займаються їх розвитком та прописують актуальні рекомендації по протидії, або запобіганню можливих майбутніх атак ззовні та з середини. То ж як базис для компанії слід взяти стандарти ISO 27001 та ISO 27032 та застосовувати їх паралельно, та виходячи з цього компанія починає розширення списку стандартів які будуть використовуватись на підприємстві.

Слід зазначити що їх дотримання це лише вершина айсберга і по факту без проходження сертифікації від відповідних компаній, що проводять аудити безпеки, компанія не матиме відповідної репутації. Цей етап досить фінансово та фізично затратний, але піднімає компанію на ще один етап, який в свою чергу дозволяє знаходити нових клієнтів від держави або ж інших компаній середнього та високого рівня.

Застосовуючи стандарт ISO 27001 та 27002 дозволить проводити керування безпекою активів починаючи від фізичних та інтелектуальних закінчуючи персоналом що займає досить високу роль при поєднанні з інформацією наведеною вище стосовно важливості персоналу та керівного складу (рис. 3.6) [49].

У разі використанні хмарними послугами слід звернутись до ISO 27017 це дозволить розкрити набагато краще впроваджувати певні послуги та ресурси по використанню дано типу рішень. Обов’язково слід відмітити ISO 27018. Це дозволить встановити загальні цілі стосовно кібербезпеки та впровадити

відповідні заходи щодо ідентифікації персональних даних, а це в свою чергу буде позитивно впливати на принципи конфіденційності ISO 29100 (рис. 3.6).

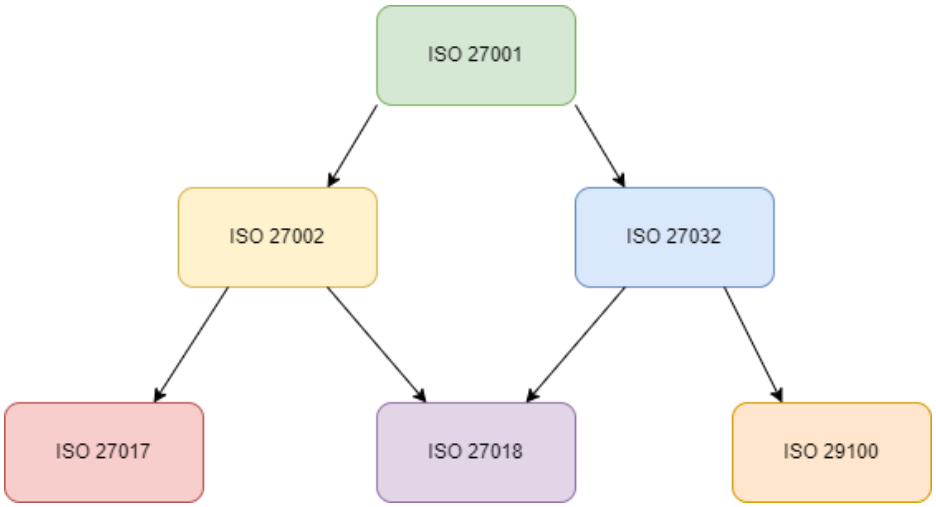

Рис. 3.6. Етапи підключення стандартів

Та під кінець один з найголовніший стандарт який покращить управління корпоративною безпеки та візьме до уваги ризики ІБ в організації. Це ISO 27799 він іде у зв'язці з ISO 27002 та вказує як правильно впровадити представлені механізми безпеки і доповнює їх (рис. 3.6) [49].

Тож в загальному можна сказати що використання усі цих стандартів у зв'язці дозволить отримати бажаний результат та покращити вже наявний стан управління інформаційною та кібербезпекою в організації.

Технічна сторона (Technical side) – тут вже досить велику частку займає активи та персонал, ресурси та рішення які виділяються на технічне та програмне забезпечення що в свою чергу дозволяє персоналу ефективніше дотримуватись поставлених цілей. Вище були наведені приклади рішень які рекомендуються до застосування на початку, з відповідним покращенням у майбутньому.

Складність цього етапу залежить від багатьох факторів в більшості випадків технічна більш простіша бо там все залежить від комп'ютерів, серверів та маршрутизаторів їх налаштування та підтримка займає певний час та ресурси. В свою чергу програмна вимагає навчених спеціалістів, які здатні реагувати та певні інциденти та проводити налаштування систем та нових баз даних.

З цього всього випливає перша проблема це виток даних та способи попередити його[50]:

1) Визначення важливих даних – відповідно застосування та приділенню максимальної уваги до збереження цих даних в таємниці, або простіше не згадувати про них взагалі. З технічної сторони краще використовувати системи DLP [50-51].

2) Захист кінцевих точок – в даному випадку це EDR або OSSIM, а через роботу у віддаленому режимі їх відсутність може принести певні проблеми[50].

3) Шифрування даних – складне шифрування за відсутності ключа може зайняти від місяця до років дешифрування, метод досить старий але його актуальність не втрачається з роками.

Слід зазначити що існує досить багато розробників програмного забезпечення, не має сенсу їх всіх перераховувати, бо в кожної компанії є обмеження по технічній частині, персоналу або ж фінансах, то ж нижче будуть представлені рішення, а вибір вендора залишається за компанією:

DLP – рішення це певного роду стратегія яка стане на захист самої важливої інформації. Слід зауважити що досить велика частина даних що оброблюється в організації не є критично важливою. Тож цю систему можна буде налаштувати та скорегувати для захисту самих критичних даних, але це все ще залежить від розуміння яка саме інформаціє є пріоритетною [51].

NGFW – це пристрій мережевої безпеки, що виходить за рамки стандартного брандмауера з контролем. В даному випадку система що включає в себе велику кількість різних інструментів що автоматизує загальний захист кіберзагроз, такі як перевірка зашифрованого трафіку TLS/SSL (Transport Layer Security/Secure Sockets Layer) та включає в себе системи захист від фішингу та блокує шкідливе посилання в листах та повідомленнях [52-53].

Для більш комплексного підходу можна взяти OSSIM Alien Vault – це досить багатофункціональна платформа що дозволяє повноцінно управляти інформаційною безпекою, спрощує та централізує усі процеси по виявленню

загроз в системі компанії. Дана SIEM з відкритим кодом дозволяє перекрити базові потреби у безпеці:

1) Контроль та виявлення активів;
2) кореляція подій;
3) виявлення вторгнень;
4) моніторинг поведінки.

Ця система має дві версії платну та безкоштовну для ознайомлення, як вказує виробник система USM Anywhere об'єднує в собі базові технології від управління активами, закінчуючи звітністю та SIEM. Досить великим плюсом від виробника це три готові варіанти використання:

1) Виявлення загроз, ідентифікація атак як ззовні так і всередині;
2) реагування тільки на інциденти;
3) дотримання стандартів та нормативно-правових норм та політик починаючи з ISO 27-серії закінчуючи GDPR, для гарантії що компанія дотримується усіх вимог.

Також дана система пропонує систему OTX (Open Threat Exchange) – це дослідження стосовно актуальних загроз які надають інші учасники з різних країни і до неї можна долучитись [54-57].

В дану систему включено HIDS (Host-based intrusion detection system), це хостова система виявлення вторгнень, вона дозволяє проводити моніторинг та збирати журнали, виявляти руткіти та контролювати цілісність файлів, але це лише частина її функціоналу. Сама по собі ця система існує в клієнтських системах та працює як служба в пам'яті, вона пов'язана з датчиком USM через порт UDP 1514 також він поширює попередньо згенерований ключ та поширює його між агентами та датчиком (рис. 3.7) [58].

EDR(Endpoint detection and response) – це виявлення та реагування на кінцевих точках тобто, комплексна система яка несе в собі певний набір технологій які призначені для моніторингу, збору інформації та відстеження дій на кінцевих пристроях.

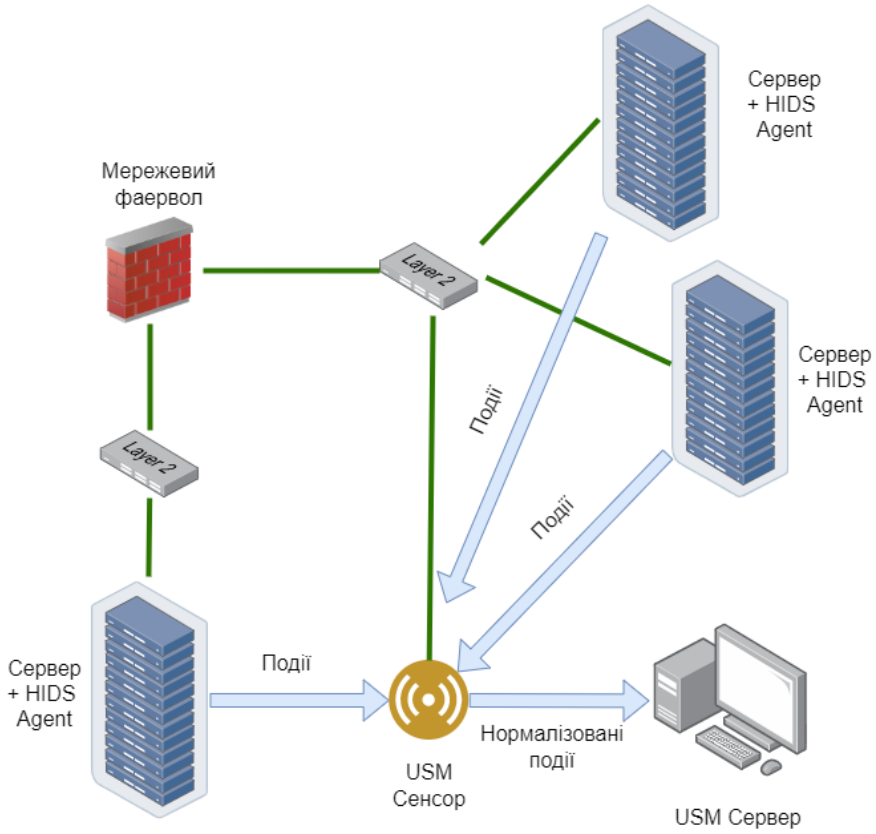

Рис. 3.7. Діаграма HIDS

Фактично це самостійне рішення яке проводить постійний аналіз усіх дій на пристроях зберігаючи повну видимість процесів та відхилень. Вона здатна автоматично виявляти приховані зловмисні дії в режимі реального часу та протидіяти їм паралельно повідомляючи працівників про даний інцидент[58-60].

На ринку існує цікавий представник даного класу від компанії Crowd Strike яку можна вважати активним мисливцем на загрози і відповідно надає команді захисту усю корисну інформацію про подію що допоможе в майбутньому у прийнятті рішень. Це дозволить розробити як загальну стратегію протидії кожному випадку так і тактику про даного типу атак. Тобто можна підсумувати що це прямий контроль кінцевих пристроїв який здатний проводити криміналістичний аналіз інциденту та надати моментальну відповідь [59-61].

Розширеним даного рішенням може бути XDR – це інструмент іде як SaaS (Програмне забезпечення як послуга) що в свою чергу забезпечить комплексний захист та включає в себе більший функціонал на відміну від EDR. В даному

випадку додатково йде використання штучного інтелекту та машинного навчання, що дасть змогу автоматично розслідувати та усунути дану проблему [62].

Аудит та покращення (або ж Check & Upgrade) – на даному етапі ми проводимо аудит всього що було виконано та порівнюємо із поставленими та запланованим завданнями. Це дозволяє отримати повну картину спроможностей компанії та в майбутньому ставити реальні цілі та терміни їх виконання.

В даному етапі цього алгоритму, після проведення усі попередніх етапів слід провести цикл PDCA (Plan, Do, Check, Act) або OODA (Observe, Orient, Decide, Act) по своїй суті вони однакові тільки перший використовується в компаніях та цивільному житті, а другий відноситься більше до військових (рис. 3.8).

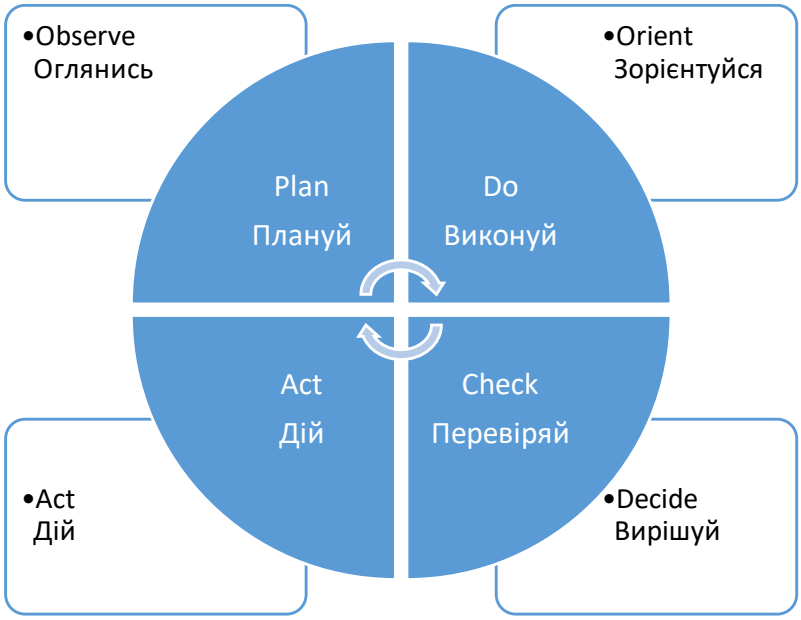

Рис. 3.8. Цикл PDCA в порівнянні з OODA

Це можна вважати основою та запорукою успіху цього алгоритму на кожному його етапі. Проведення даного циклу на постійній основі дає розуміння які дії виправдовуються та приносять результат, а які лише заважають та витрачають ресурси.

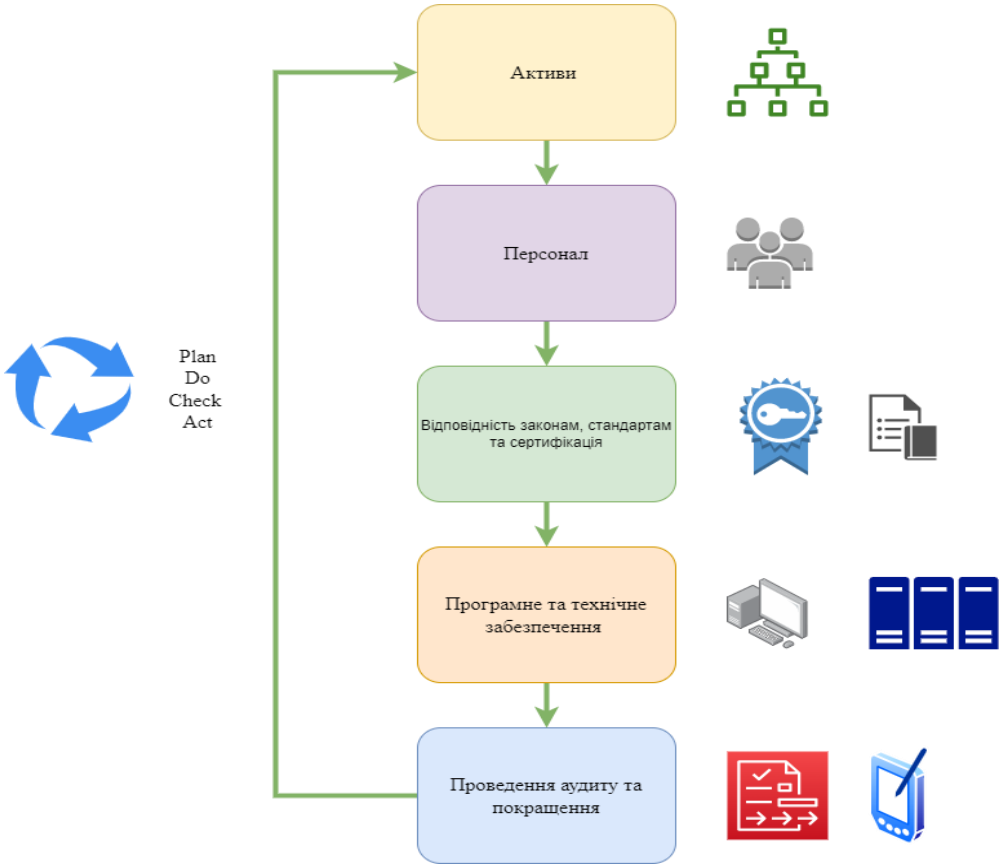

Рис. 3.9. Схема методики у вигляді алгоритму ASRTCU

Представлена методика у вигляді алгоритму потребує останнього визначення загальної ефективності усіх наведених рішень. Для цього керівнику та відповідальній комісії потрібно провести оцінку кожного з етапів від 1 до 10 (Не ефективно та відповідно дуже ефективно) – це дозволить нам об’єктивно оціни внесені зміни та побачити результати наших підходів.

Тобто в табл. 3.1 зображено кожен з етапів та відповідно оцінювання їх користі для організації по окремості в третій колонці, в четвертій в свою чергу рахуємо середнє арифметичне для кожного етапу. Таким чином ми визначаємо для кожного розділу їх позитивний чи негативний вплив на структуру. І в кінці етапу Аудит ми отримуємо загальну оцінку з наявної суми середнього арифметичного кожного розділу, в даному випадку це 28,04 балів із 40 можливих тобто рівень ефективності знаходиться на 70,1%.

Табл. 3.1

Приклад визначення середньої оцінки кожного з етапів та відповідно загальної

Етап оцінки	Складові	Оцінка за кожен підпункт	Загальна оцінка ефективності
Активи	Бюджет Приміщення Ресурси	8 7 4	6,3
Персонал	Працівники Керівництво Бухгалтерія	9 5 8	7,3
Правила	Закони країни Закони міжнародних союзів Стандарти	10 5 8	7,7
Технічна сторона	Сервери Персональні комп’ютери Фізична безпека Технічна безпека	6 7 8 6	6,75
Аудит	Перевірка кожного з етапів на ефективність Відсоток відповідності ефективності	-	28,04/40 70,1%

Представлений алгоритм являє собою основу яку можна розвивати та при поглибленні в яку почнеться розширення та покращення ефективності усього процесу корпоративного управління безпекою особливо в Україні.

Дана табл. 3.1 дозволить правильно оцінити ефективність кожного з етапів, та визначити критично важливі аспекти які потребують негайного втручання та відповідного покращення. На сьогодні досить велика кількість працівників не

розуміють саму концепцію захисту, думаючи що це лише фізичний вплив. Тож дана методика у вигляді алгоритму та таблиці зображує наявний стан ефективності корпоративного управління інформаційною безпекою. А це в свою чергу наддасть відповідну основу для покращення або побудови міцної та робочої корпоративної структури не тільки бізнесу але і управління інформаційною безпекою в середині нього. Це дозволяє зрозуміти навіть стажеру що дана компанія націлена на підвищення ефективності та прокачування усі засобів захисту свого бізнесу (рис. 3.9).

Висновки до третього розділу

Підсумовуючи усе вище наведене слід зазначити що був проведений аналіз результатів вище та проведено визначення основних тенденцій і проблем в корпоративному управлінні інформаційною безпекою в Україні. Окремо визначено для трьох незалежних проте пов’язаних між собою секторів – це корпоративний, приватний та державний, були визначені їх основні зв’язки та залежності. Відповідно їх зав’язка на багатьох факторах ІБ як вимоги від держави та дотримання стандартів і закінчуючи загрозами з боку конкурентів та інших держав.

В другому під розділі був наведена методика у вигляді алгоритму та таблиця для будування ефективного корпоративного управління інформаційною безпекою в Україні. Для початку було розглянуто питання що таке актив та що є собою прибуток компанії, в наступну чергу був розглянутий персонал та керівництво їх ризики та проблематику яку вони можуть створити для компанії в цілому. Наступним етапом було відповідність стандартам та законам які слід дотримуватись компанії для отримання хорошої репутації серед клієнтів та держави. Наступним етапом технічну складову яку слід дотримуватись та покращувати відповідно до вимог та потреб компанії. Під кінець даного аналізу було розглянуто алгоритм який дозволяє без зупину проводити покращення роботи PDCA/OODA.

Таблиця що була наведена в кінці, зображує те що для визначення дійсно наявної ефективності, ми використовуємо суму середнього арифметичного кожного з підрозділів для визначення в загальному ефективність етапу. Відповідно додаючи інші етапи ми отримуємо загальну суму що показує нам відсоток ефективності нашої системи. Ці математичні данні в майбутньому можна порівнювати та створювати графічне порівняння усього прогресу ефективності нашої системи.

Узагальнюючи можна сказати що наведений алгоритм надає базову основу для компаній що починають та організацій що вже мають певну основу. Це дозволяє гнучко використовувати, модифікувати та покращувати ефективність усієї системи корпоративного управління ІБ згідно потреб та динаміки розвитку технологій у світі.

ВИСНОВКИ

Підсумовуючи усе вище наведене слід зазначити що у першому розділі було проаналізовано наявні поняття та принципи корпоративного управління інформаційною безпекою які в свою чергу спиралися на вимогу у вигляді тріади CIA, що спирається на основні вимоги конфіденційності, цілісності та доступності. В подальшому розглядалися питання побудови концептуальної моделі безпеки та відповідних їй два підходи, безпеки інтернету та мережі та інших. Розглянуто досить важливе питання міжнародних рамок стандартів та рамок управління ІБ, в даному розділі в основному розглядалися стандарти та закони різних країн та союзів відповідно і порівняння двох схожих за концепцією але різних за застосуванням стандартів ISO 27001 та ISO 27032. В останньому розділі розглядалися вже існуючих методів оцінки ефективності корпоративного управління ІБ, як приклад це аудити, ризики, пентести, стрес-тести та аналіз ефективності технічних засобів безпеки і тд.

В другому розділі було проаналізовано сучасний стана корпоративного управління ІБ в Україні, що в свою чергу слід зазначити знаходиться на досить посередньому рівні, що в свою чергу дозволяє йому розвиватись відповідно до сучасних потреб та реальності. Далі були розглянуті основні фактори та виклики, що саме впливають на ефективність управління ІБ в країні в загальному. З цього виплило досить багато різних нюансів, такі як різке зростання кількості та якості кіберзагроз, штучного інтелекту та хмарних технологій, нормативних регулювань та самого простого людського фактору і тд. Розглянуто велику кількість різних факторів та їх особистий вплив на різні структури ІБ, ключові показники ефективності. В даному випадку були оглянуті саме ті чинники які позитивно впливають на усю ІБ в цілому та показують що всі підходи та методи були застосовано правильно та розумно, що в свою чергу дало позитивний результат.

В останньому ж розділі наведений алгоритм що дозволяє підвищити ефективність корпоративного управління інформаційною безпекою. В даному

випадку він засновується на аналізі попередньо наведених даних та основних тенденцій розвитку та проблем в корпоративному управлінні ІБ в Україні. Заради підвищення ефективності він націлений на боротьбу не тільки з наслідками, але і з причиною, неправильним підходом до загальної організації. В цілому було виділені три сектори де саме застосовується дана функція, корпоративний, приватний та державний. Огляд у потребі дотримання стандартів, відповідно законів різних союзів та держав. В останньому підрозділі було наведено власний алгоритм який націлений на правильний підхід до організації ефективного управління ІБ.

Також була надана таблиця із прикладом вирахування ефективності корпоративного управління ІБ на основі простих математичних дій таких як, суми середнього арифметичного та простого додавання і визначення відсотка. В даному випадку можна визначити які саме підрозділі погіршують загальну оцінку етапів і покращити їх більш тонко та відповідно до їх поотреб.

Запропоновані пропозиції надають перспективи для самостійного розвитку компанії із можливістю налаштувати усі процеси під власні потреби.

Новизна дослідження ефективності корпоративного управління інформаційною безпекою, включає у себе визначення критеріїв моніторингу ІБ в середині компанії, комплексному застосуванні SIEM-систем разом із EDR, DMZ та XDR для запобігання витоку інформації та відповідно запобіганню кібер інцидентам, робота з персоналом та відповідно покращення їх навичок та компетентності.

Практична реалізація рекомендацій дозволить компаніям значно підвищити ефективність корпоративного управління інформаційною безпекою на початкових етапах створення бізнесу, або відповідно покращити наявний стан за допомогою циклічного алгоритму із залученням міжнародних стандартів та законів. Окремо слід зазначити що даний алгоритм також можна застосовувати і в державному та військовому секторі, але потрібні будуть відповідні зміни.

Підсумовуючи, можна зазначити що на даний момент в Україні через певне тяжке становище після 90-х років, та відповідно агресії зі сторони

сусідньої країни, виникла висока потреба у дотриманні стандартів та державних законів та нормативно-правових актів. Це дозволило стабілізувати та підняти рівень захищеності усіх компаній, які тісно пов’язані з КБ та ІБ на високий рівень, хоча цього все рівно поки не достатньо, але існує досить велика перспектива розвитку.

ПЕРЕЛІК ПОСИЛАНЬ

1. CIA Triad - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/the-cia-triad-in-cryptography/ (date of access: 03.10.2023).

2. Chai W. What is the CIA triad? Definition, explanation, examples | techtarget. WhatIs.URL: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA (date of access: 03.10.2023).

3. What is the CIA triad and why is it important? | fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/cia-triad (date of access: 03.10.2023).

4. Cybersecurity framework. NIST. URL: https://www.nist.gov/cyberframework (date of access: 03.10.2023).

5. Approaches to information security implementation - geeksforgeeks. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/approaches-to-information-security-implementation/ (date of access: 03.10.2023).

6. Анастасия. Міжнародні стандарти інформаціоної безпеки. *Щоденник особистих вражень у вивченні технології*. URL: https://informationsecuritypalamarchuk.blogspot.com/2021/01/blog-post_13.html (дата звернення: 04.10.2023).

7. Information security standards - an overview. *DQS | Audits und Zertifizierung | Simply leveraging Quality*. URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/standarti-informacijnoyi-bezpeki-oglyad#standards-fuer-informationssicherheit-chapter01 (date of access: 04.10.2023).

8. ISO/IEC FDIS 27001:2013(E). Information technology – Security techniques – Information security management systems – Requirements. Replaces ISO/IEC 27001:2005. Official edition. 2013. 30 p. URL: http://www.itref.ir/uploads/editor/42890b.pdf (date of access: 04.10.2023).

9. Що таке ніст 800-53? - визначення з техопедії - Безпека 2023. *Icy Science*. URL: https://uk.theastrologypage.com/nist-800-53 (дата звернення: 04.10.2023).

10. Загальний регламент про захист даних (GDPR) - gdpr-text.com. *GDPR-Text.com - GDPR Text, Translation and Commentary*. URL: https://gdpr-text.com/uk/ (дата звернення: 05.10.2023).

11. HIPAA: як захищають медичні дані пацієнтів в США?. *Everlegal*. URL: https://everlegal.ua/hipaa-yak-zakhyschayut-medychni-dani-patsientiv-v-ssha (дата звернення: 05.10.2023).

12. Pci dss. *Platon*. URL: https://platon.ua/faq/pci-dss (date of access: 05.10.2023).

13. What are FISMA Compliance Requirements? | SolarWinds. *IT Management Software and Observability Platform*. URL: https://www.solarwinds.com/public-sector/fisma-compliance-requirements (date of access: 05.10.2023).

14. Information security management system saas for ISO 27001. *ISMS.online*.URL: https://www.isms.online/information-security-management-system-isms/ (date of access: 06.10.2023).

15. ISO 27032 vs ISO 27001 | Cybersecurity standard: main differences. *27001Academy*.
URL: https://advisera.com/27001academy/blog/2015/08/25/iso-27001-vs-iso-27032-cybersecurity-standard/ (date of access: 09.10.2023).

16. Аудит - IT-Solutions, Україна. *IT-Solutions, Україна*. URL: https://it-solutions.ua/it-consulting/informaciyna-bezpeka/audit/ (дата звернення: 11.10.2023).

17. Аудит інформаційної безпеки: що це, види | Блог Colobridge. *blog.colobridge.net*. URL: https://blog.colobridge.net/uk/2023/06/information_security_audit-ua/ (дата звернення: 11.10.2023).

18. Аудит безпеки інформаційної безпеки. *ТЗІ - інформаційна безпека та захист інформації*. URL: https://tzi.com.ua/audbezib.html (дата звернення: 11.10.2023).

19. Що таке пентест – тест на проникнення? - datami. *datami*. URL: https://datami.ua/shho-take-pentest-test-na-proniknennya/ (дата звернення: 11.10.2023).

20. Чубаєвський В. І. Корпоративна інформаційна безпека. Київ : Держ. торг.-екон. ун-т, 2022. 272 с. URL: https://knute.edu.ua/file/MjIxNw==/c575744f80c383571b00fa6bb0b09cfd.pdf (дата звернення: 12.10.2023).

21. Дем'янець В. Територія застосування GDPR. Хто потрапляє під дію GDPR?. *Legal IT group*. URL: https://legalitgroup.com/teritoriya-zastosuvannya-gdpr/ (дата звернення: 12.10.2023).

22. What is GDPR? Key elements and requirements explained. *Advisera*. URL: https://advisera.com/articles/what-is-eu-gdpr/ (date of access: 24.10.2023).

23. GDPR україна. GDPR в україні. захист персональних даних в україні. *Legal IT group*. URL: https://legalitgroup.com/category/gdpr-ta-personalni-dani/gdpr-ukrayina/ (дата звернення: 12.10.2023).

24. Інформаційна безпека: види загроз і методи їх усунення - datami. *datami*. URL: https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/ (дата звернення: 12.10.2023).

25. Войціховський А. В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *The journal of eastern european law / журнал східноєвропейського права.* 2018. № 53. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/a2dd0ed8-c884-4205-8d60-df50918d943e/content (дата звернення: 14.10.2023).

26. Incident response as a service and its importance in cyber. *CYBERVIE*. URL: https://www.cybervie.com/blog/incident-response-service-importance/ (date of access: 14.10.2023).

27. Інформаційна безпека держави : навч. посіб. / В. Гур'єв та ін. Ніжин : ЧЕРНІГ. НАЦ. ТЕХНОЛ. УН-Т, 2018. URL: http://ir.stu.cn.ua/bitstream/handle/123456789/19246/Інформ.%20безпека%20держ.%20New%20booklet%201.pdf?sequence=1&isAllowed=y (дата звернення: 14.10.2023).

28. Що таке контейнеризація: основне визначення та завдання. *FoxmindEd*. URL: https://foxminded.ua/shcho-take-konteineryzatsiia/ (дата звернення: 20.10.2023).

29. Навіщо нам контейнеризація: переваги для DevOps. *IT Education Center Blog*. URL: https://blog.iteducenter.ua/articles/navishho-nam-kontejnerizaciya-perevagi-dlya-devops/ (дата звернення: 25.10.2023).

30. Локальна мережа в офісі: будуємо правильно | Nspace. *Nspace – послуги IT-аутсорсингу для бізнесу*. URL: https://nspace.ua/info/lokalna-merezha-v-ofisi-buduyemo-pravilno/ (дата звернення: 04.11.2023).

31. Побудова сучасних інтернет мереж та новітнє мережеве обладнання. *GAZIK - інтернет-магазин мережевого обладнання, вживаної комп'ютерної техніки: бу ноутбуки, бу монітори, бу ПК*. URL: https://gazik.ua/blog/tekhnologii/pobudova-suchasnykh-internet-merezh-ta-novitnye-merezheve-obladnannya/ (дата звернення: 04.11.2023).

32. Правила побудови домашньої мережі. *Макснет – Гігабітний інтернет-провайдер та оператор зв'язку для дому та бізнесу*. URL: https://maxnet.ua/blog/pravila-postroyeniya-domashney-seti/ (дата звернення: 04.11.2023).

33. Технологія VLAN. об'єднання офісів у локальну, віртуальну мережу. *westelecom.ua*. URL: https://westelecom.ua/blog/tehnologia-vlan-obedinenie-ofisov-v-lokalnuu-virtualnuu-set (дата звернення: 04.11.2023).

34. Як зберегти інтернет під час відключення світла | інтернет-провайдер вестелеком одеса. *westelecom.ua*. URL: https://westelecom.ua/blog/kak-sohranit-internet-vo-vrema-otklucenia-sveta-zapitajte-vsego-odno-ustrojstvo (дата звернення: 09.11.2023).

35. Грицак Н. Навіщо IT-спеціалістам оцінювання soft skills і як це робити. *DOU*. URL: https://dou.ua/lenta/articles/assessing-soft-skills-in-it/ (дата звернення: 14.11.2023).

36. Щавінський Ю. В., Кудін І. В., Порохницький О. А. Етичні методи та засоби управління інформаційними інцидентами і ризиками. *Актуальні*

проблеми кібербезпеки : ВСЕУКР. НАУКОВО-ПРАКТ. КОНФ., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 369–372. URL: https://duikt.edu.ua/uploads/p_2626_52007398.pdf.

37. Oteir N. Час простою сервера: що має знати кожен бізнес, щоб залишатися онлайн. *INTROSERV*. URL: https://introserv.com/ua/blog/chas-prostoyu-servera-shho-mae-znati-kozhen-biznes-shhob-zalishatisya-onlajn/ (дата звернення: 14.11.2023).

38. CERT-UA. *cert.gov.ua*. URL: https://cert.gov.ua/about-us (date of access: 14.11.2023).

39. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 17.11.2023).

40. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.11.2023).

41. Сучасні загрози інформаційній безпеці країни та шляхи їх подолання – UJCL. *UJCL*. URL: https://www.constjournal.com/pub/4-2021/suchasni-zahrozy-informatsiyniy-bezpetsi-krainy-shliakhy-ikh-podolannia/ (дата звернення: 19.11.2023).

42. Експертна думка про тенденції в кібербезпеці - Асоціація підприємств інформаційних технологій України. *Асоціація підприємств інформаційних технологій України*. URL: https://apitu.org.ua/ekspertna-dumka-pro-tendentsii-v-kiberbezpetsi/ (дата звернення: 20.11.2023).

43. Дослідження глобальних тенденцій інформаційної безпеки за 2018 рік: основні висновки. *PwC*. URL: https://www.pwc.com/ua/uk/survey/2018/strengthening-digital-society-against-cyber-shocks.html (дата звернення: 20.11.2023).

44. Security Magazine. *Security Magazine | The business magazine for security executives*. URL: https://www.securitymagazine.com/articles/100156-top-cybersecurity-trends-of-2023 (date of access: 22.11.2023).

45. Duggal N. Top 20 Cybersecurity Trends to Watch Out for in 2024. *Simplilearn.com*. URL: https://www.simplilearn.com/top-cybersecurity-trends-article#1_rise_of_automotive_hacking (date of access: 22.11.2023).

46. Витік даних чи злам – в чому різниця | 10Guards. *10Guards | Cybersecurity Services (Advisory/Ethical Hacking)*. URL: https://10guards.com/ua/articles/whats-the-difference-between-a-data-leak-and-a-data-breach/ (дата звернення: 24.11.2023).

47. Витік даних. визначення та приклади у 2023. | gridinsoft. *ТОВ "Грідінсофт"*. URL: https://gridinsoft.ua/data-breaches (дата звернення: 25.11.2023).

48. Порохницький О. А. Вплив на інформаційну стабільність колективу. *Актуальні проблеми кібербезпеки* : ВСЕУКР. НАУКОВО-ПРАКТ. КОНФ., м. Київ, 27жовт. 2022 р. Київ, 2022. С. 98–99. URL: https://duikt.edu.ua/uploads/p_2121_20358827.pdf?file=p_2121_20358827.pdf.

49. Стандарти серії ISO 27000. *https://ikmj.com*. URL: https://ikmj.com/uk/24894-2/ (дата звернення: 22.11.2023).

50. 6 порад як захистити бізнес від витоку даних. *GigaTrans - Интернет для Вашего офиса*. URL: https://gigatrans.ua/ua/news/6-sposobov-kak-zash-itit-biznes-ot-utechki-dannuh (дата звернення: 22.11.2023).

51. Що таке запобігання втраті даних (data loss prevention або DLP)? - kingston technology. *Kingston Technology Company*. URL: https://www.kingston.com/ua/blog/data-security/data-loss-prevention-dlp (дата звернення: 22.11.2023).

52. What Is a Next-Generation Firewall (NGFW)?. *Cisco*. URL: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html (date of access: 22.11.2023).

53. NGFW – у чому переваги файрволів наступного покоління?. *ESKA*. URL: https://eska.global/blog/ngfw-v-chem-preimushestva-fajrvolov-sleduyushego-pokoleniya (дата звернення: 26.11.2023).

54. AlienVault® USM Anywhere™. *Bakotech*. URL: https://bakotech.ua/ua/product/351/ (date of access: 26.11.2023).

55. AlienVault OSSIM. *AT&T Cybersecurity | Managed Security Services for Network, XDR & more*. URL: https://cybersecurity.att.com/products/ossim (date of access: 02.12.2023).

56. AlienVault OSSIM | UnifiedThreatWorks.com. *AlienVault | AT&T Cybersecurity | UnifiedThreatWorks.com*. URL: https://www.unifiedthreatworks.com/OSSIM.asp (date of access: 02.12.2023).

57. OSSIM: a careful, free and always available guardian for your network. *ACM Digital Library*. URL: https://dl.acm.org/doi/fullHtml/10.5555/2642922.2642924 (date of access: 02.12.2023).

58. About Host-based IDS (HIDS) in AlienVault USM Appliance. *AT&T Cybersecurity | Managed Security Services for Network, XDR & more*. URL: https://cutt.ly/VwHZBnyK (date of access: 12.12.2023).

59. ЗАХИСТ КІНЦЕВИХ ТОЧОК. *IITD*. URL: https://iitd.com.ua/zashchita-konechnyh-tochek/ (дата звернення: 11.12.2023).

60. What is EDR? Endpoint detection & response defined. *crowdstrike.com*. URL: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/ (date of access: 11.12.2023).

61. What is endpoint detection and response? | EDR security | trellix. *Trellix | Revolutionary Threat Detection and Response*. URL: https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-detection-and-response/ (date of access: 12.12.2023).

62. Що таке розширене виявлення й реагування (XDR)?. *Microsoft*. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-xdr.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ