Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
« » червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього рівня)

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

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Розробка моделі оцінки захищеності інформаційнних систем»

Виконавець: студентка IV курсу, групи КБ-41

_____ **Черняк Олександра Олегівна**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Браіловський М.М.	

Нормоконтроль	Даков С.Ю.	

Київ 2021

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-41** **Черняк Олександрі Олегівні**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Розробка моделі оцінки захищеності інформаційних систем

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Стандарти в сфері ІБ, оцінка захищеності ІС, оцінка ризиків.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися із відомими стандартами в сфері ІТ і ІБ, методикою їх роботи і впровадження, оцінити типові ризики для ІС організації, проаналізувати їх, проаналізувати процеси COBIT 5 з боку ІБ, скласти схему, за якою можна провести оцінювання ІБ ІС організації.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації з оцінки захищеності ІС організації

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:12 жовтня 2020 року

Завдання видав	_____	М.М, Браіловський
	(підпис)	(ініціали, прізвище)
Завдання прийняла до виконання	_____	О.О. Черняк
	(підпис)	(ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 22.01.2020	*виконано*
2	Аналіз літератури	29.01.2020 – 11.02.2020	*виконано*
3	Обґрунтування вибору стандартів	12.02.2020 – 15.02.2020	*виконано*
4	Аналіз вразливостей і ризиків	16.02.2020 – 04.03.2020	*виконано*
5	Аналіз вразливостей інформаційних систем	05.03.2020 – 21.03.2020	*виконано*
6	Аналіз ризиків	22.03.2020 – 08.04.2020	*виконано*
7	Формування моделі оцінки захищенності на основі стандартів	09.04.2020 – 10.05.2020	*виконано*
8	Оформлення пояснювальної записки	18.05.2020 – 08.06.2021	*виконано*
9	Підготовка до захисту дипломної роботи	09.05.2020 – 21.06.2021	*виконано*

Завдання видав	_____	М.М. Браіловський
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання	_____	О.О. Черняк
	(підпис)	(ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 58 сторінок основного тексту, 15 таблиць та 3 рисунка. Список використаних джерел містить 42 найменування і займає 4 сторінки.

Метою даної роботи є розробка моделі оцінки стану захищеності інформаційних систем.

У роботі проаналізована існуюча література з використання стандартів для оцінки ІБ, виконано аналіз стандартів, структуризація, вивчення та узагальнення вітчизняної і зарубіжної практики з теми оцінки захищеності інформаційних систем, розроблено модель оцінки захищеності інформаційної системи і приклад її реалізації.

Розроблено файл з блок схемою, що ілюструє суть моделі, і створено реалізацію в файлі Excel.

Розроблені в моделі рекомендації призначені для недержавних підприємств, бо деякі використані частини стандартів конфліктують із законодавством України у цій області.

Ключові слова: оцінка захищеності, ISO/IEC 27001, COBIT 5, ITIL, зрілість процесів.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІБ	–	Інформаційна безпека
COBIT	–	Control Objectives for Information and Related Technologies
ITIL	–	IT Infrastructure Library
SLA	–	Service Level Agreement
OLA	–	Operational Level Agreement
BCM	–	Business Continuity Management
IaaS	–	Infrastructure as a service
IT	–	Information Technology
PaaS	–	Platform as a service
BC	–	Business Continuity
DR	–	Disaster Recovery
BIA	–	Business Improvement Area
APT	–	Advanced Persistent Threat
ІС	–	Інформаційна система
СУІБ		Система управління інформаційною безпекою

ЗМІСТ

ВСТУП

Актуальність питання безпеки інформаційних систем завжди є актуальним і перед керівництвом організацій завджди стоїть завдання провести оцінку захищеності у межах своєї установи і більшість методик не дає досконалого результату при використанні лише одного стандарту.

Інформація є критично важливим ресурсом для всіх підприємств. На всіх етапах свого життєвого циклу інформація критичним чином залежить від спеціалізованих технологій. Інформація та інформаційні технології, що перебувають ц динамічному розвивитку, є життєво важливими для сучасних підприємств: як громадських, так і державних, і комерційних.

Інформаційна система (ІС) - система, призначена для зберігання, пошуку та обробки інформації, і відповідні організаційні ресурси (людські, технічні, фінансові і т.д.), які забезпечують і поширюють інформацію[1]. І, як будь-який цінний ресурс, інформація, що циркулює в інформаційній системі та є критично важливою для діяльності компанії, має бути надійно захищеною.

Тому сьогодні, найбільше, ніж будь-коли, підприємства та їхні керівники зобов'язані:

Підтримувати високу якість інформації для прийняття управлінських рішень.

- Створювати цінність для бізнесу, реалізуючи інвестиції, пов'язані з ІТ, тобто досягати стратегічних цілей і отримувати вигоду шляхом ефективного та інноваційного використання ІТ.
- Удосконалювати операційну модель, надійно і раціонально застосовуючи технології.
- Забезпечувати прийнятний рівень ІТ-ризиків.
- Оптимізувати витрати на ІТ-послуги та технології.
- Підвищувати ступінь дотримання законів, норм, договірних зобов'язань і політик, пов'язаних із застосуванням інформаційних технологій.

Тому *метою роботи* є розробка моделі оцінки захищеності на основі відомих світових практик в сфері інформаційної безпеки.

Для досягнення поставленої мети необхідно вирішити такі *завдання*:

- Розглянути відомі міднародні стандарти в сфері інформаційної безпеки;
- Проаналізувати відомі вразливості, пов’язані з ними ризики;
- Проаналізувати структуру COBIT 5 з точки зору інформаційної безпеки.

Об'єктом дослідження в даній роботі є явище захищеності інформаційної системи.

Предметом дослідження в даній роботі є модель оцінки захищеності інформаційних систем.

Методи дослідження дипломної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння;
- вивчення та узагальнення вітчизняної і зарубіжної практики.

РОЗДІЛ 1
АНАЛІЗ ВІДОМИХ ПРАКТИК У СФЕРІ IT ТА ІБ

1.1 COBIT 5

Ряд позитивних прикладів важливості ефективного керівництва, так само як і деякі труднощі бізнесу всесвітнього масштабу, що відбулися за останні десятиліття, змусили підприємства приділяти значно більше уваги поняттю «керівництво».

Підприємства, які досягли успіху, змогли визнати, що рада директорів і виконавчі директори повинні ставитися до IT, як до будь-якої іншої значної частини бізнесу. Рада директорів і управлінці - як в бізнесі, так і в IT - повинні спільно працювати над тим, щоб IT були частиною загального підходу до керівництва та управління підприємством. На додаток до цього, необхідність ефективного керівництва диктується ще й сучасними законодавчими та іншими регулюючими вимогами.

COBIT 5 пропонує цілісну методологію[2], яка покликана допомогти у вирішенні завдання керівництва та управління IT на підприємстві. Простіше кажучи, COBIT 5 допомагає підприємствам досягти оптимальної цінності від IT, підтримуючи баланс між отриманням вигоди і оптимізацією ризиків і ресурсів. COBIT 5 дає можливість керувати і управляти IT в масштабах всього підприємства, як в областях функціональної відповідальності IT, так і бізнесу, а також дозволяє враховувати потреби в IT внутрішніх і зовнішніх зацікавлених сторін. Методологія COBIT 5 універсальна і буде корисна підприємствам будь-якого масштабу і сфери діяльності: комерційним, громадським і державним.

COBIT 5 є новим поколінням рекомендацій ISACA[3] по керівництву підприємством і менеджменту IT. COBIT 5 заснований на більш ніж 15-річному досвіді практичного використання і застосування COBIT багатьма підприємствами і спільнотами фахівців в області бізнесу, IT, управління ризиками та безпекою, також

контролю якості. Головними рушійними силами розвитку COBIT 5 є потреби в рекомендаціях з наступних питань[4]:

Отримання інформації від більш широкого кола зацікавлених сторін про їхні очікування від інформаційних і пов'язаних технологій (вигоди, прийнятний рівень ризику і ціни) і про їх пріоритети в забезпеченні впевненості в отриманні очікуваної цінності. Одні зацікавлені особи хочуть отримати віддачу в короткостроковому періоді, іншим цікава довгострокова стабільність. Одні готові до високого ступеня ризику, а інші ні. Цими сподіваннями, які відрізняються і, можливо, конфліктуючими, потрібно ефективно управляти. Більш того, зацікавлені сторони не тільки хочуть брати участь в ухваленні рішень, але і вимагають прозорості - як виконуваних робіт, так і результатів.

Управління зростаючої залежністю успішності підприємств від зовнішніх контрагентів бізнесу та IT, таких як аутсорсингові компанії, постачальники, консультанти, клієнти, постачальники хмарних і інших послуг, а також від різноманітності внутрішніх способів і механізмів формування очікуваної цінності. Управління істотно збільшеним об'ємом інформації. Як підприємства вибирають потрібну і надійну інформацію, на підставі якої повинні прийматися результативні та ефективні бізнес-рішення? Інформацією слід результативно управляти, а цьому сприятиме результативна інформаційна модель.

Управління інформаційними технологіями, які стають все більш інтегрованими в бізнес. Уже недостатньо незалежного управління IT, хай навіть скоординованого з бізнесом. Необхідно, щоб IT стали невід'ємною частиною бізнес-проектів, організаційних структур, управління ризиками, політик, навичок, процесів і так далі. Роль CIO (Chief Information Officer) і роль IT-функції розвиваються. IT та бізнес повинні все більше інтегруватися.

Подальший розвиток технологій і інновацій. Це питання, пов'язані з творчістю, винахідництвом, розробкою нових продуктів - всім, що робить існуючі пропозиції більш привабливими для клієнтів і допомагає залучати нові категорії клієнтів. Інновації також припускають раціоналізацію і прискорення процесів

розробки, виробництва і ланцюжки поставок з тим, щоб доставляти продукти на ринок більш ефективно, швидко і якісно.

Повні і наскрізні описи функціональних обов'язків бізнесу та IT і опис всіх аспектів результативного керівництва та управління IT підприємства, таких як організаційні структури, політики, культура і, звичайно, процеси.

Удосконалення контролю над зростаючим числом IT-рішень, що створюються і керованих користувачами.

Забезпечення на рівні підприємства:

- формування цінності шляхом результативного та інноваційного використання IT на підприємстві;
- задоволеності бізнес-користувачів послугами та роботою IT;
- відповідності IT законодавству, правилам, контрактними зобов'язаннями і внутрішнім політикам;
- вдосконалення зв'язків між потребами бізнесу і цілями IT.

Розуміння і, в разі потреби, застосування рекомендацій найбільших методологій і стандартів індустрії, таких як Information Technology Infrastructure Library (ITIL), The Open Group Architecture Framework (TOGAF), Project Management Body of Knowledge (PMBOK), PRojects IN Controlled Environments 2 (PRINCE2), Committee of Sponsoring Organizations of the Treadway Commission (COSO), а також стандартів International Organization for Standardization (ISO). Це допоможе зацікавленим сторонам зрозуміти зв'язку між методологіями і можливості їх спільного використання. Інтеграція всіх основних методологій і наборів рекомендацій ISACA, головними з яких є COBIT, Val IT і Risk IT, а крім того Business Model for Information Security (BMIS), IT Assurance Framework (ITAF), Board Briefing on IT Governance і ініціативи Taking Governance Forward (TGF). Методологія COBIT 5 створює основу для інтеграції інших методологій, стандартів і практик.

1.1.1 Принципи COBIT 5

Принцип 1. Відповідність потребам зацікавлених сторін

Підприємства існують для того, щоб створювати цінність для зацікавлених сторін[5]. Отже, для кожного підприємства, комерційного або некомерційного, метою керівництва є створення цінності. Створення цінності означає отримання вигод при оптимізації ризиків і використання ресурсів. Вигоди можуть бути різними, наприклад, для комерційного підприємства важлива фінансова вигода, а для державного - якість послуг, що надаються населенню.

У підприємстві зазвичай зацікавлене безліч сторін, і розуміння «цінності» для кожної з них може бути різним, а часом і конфліктувати з трактуваннями інших. Керівництво полягає в тому, щоб шляхом переговорів знайти розумний компроміс між інтересами всіх сторін. Отже, оцінюючи вигоди, ризики та ресурси, система керівництва повинна враховувати інтереси всіх сторін. Перед тим, як прийняти управлінське рішення, потрібно відповісти на питання: Для кого отримується вигода? Які ризики і кого вони стосуються? Які потрібні ресурси?

Принцип 2: Комплексний погляд на підприємство.

COBIT 5 вбудовує керівництво IT в керівництво підприємством в цілому, тобто:

- Розглядає всі функції і процеси підприємства. COBIT 5 націлений не тільки на реалізацію «IT-функції», але розглядає інформацію та пов'язані з нею технології як активи підприємства, якими слід керувати, як і будь-якими іншими активами.
- Виходить із того, що фактори впливу керівництва та управління, пов'язані з IT, працюють на всьому підприємстві і по всій ланцюжка створення цінності, і включають в себе всі внутрішні і зовнішні аспекти і ролі, які мають відношення до керівництва та управління IT.

Принцип 3: Застосування єдиної інтегрованої методології.

Існує безліч пов'язаних з IT склепінь знань і стандартів, присвячених окремим аспектам IT-діяльності. У COBIT 5 реалізовано відповідність цим зовнішнім

склепіння і стандартам. Таким чином, методологія COBIT 5 забезпечує інтеграційний підхід для організації керівництва та управління IT на підприємстві.

Принцип 4: Забезпечення цілісності підходу.

Ефективне і раціональне керівництво та управління IT на підприємстві вимагає цілісного підходу, з урахуванням багатьох взаємопов'язаних компонентів.

У COBIT 5 описаний набір факторів впливу[6], які забезпечують впровадження системи керівництва та управління IT на підприємстві. Фактори впливу - це сутності, які сприяють вирішенню завдань підприємства. Методологія COBIT 5 описує сім видів факторів впливу:

- Принципи, політики і підходи
- Процеси
- Організаційна структура
- Культура, етика і поведінку
- Інформація
- Послуги, інфраструктура і додатки
- Персонал, навички та компетенції

Принцип 5: Поділ керівництва та управління.

Методологія COBIT 5 проводить чітку межу між керівництвом і управлінням. Ці дві дисципліни включають в себе різні види діяльності, вимагають різних організаційних структур і служать різним цілям.

1.1.2 Каскад цілей COBIT 5

Кожне підприємство працює в своєму контексті. Цей контекст визначається зовнішніми факторами (ринок, галузь економіки, геополітика і т.д.) і внутрішніми факторами (культура, організаційна структура, схильність до ризику і т.д.), тому системи керівництва та управління повинні бути налаштовані з урахуванням факторів, актуальних для даного підприємства. Потреби зацікавлених сторін повинні бути трансформовані в придатну на практиці стратегію. Каскад цілей COBIT 5 - це механізм перекладу потреб зацікавлених сторін в конкретні, практичні

і настроювані цілі підприємства, IT-цілі і цілі факторів впливу. Цей переклад дозволяє встановлювати і вибирати конкретні цілі на кожному рівні і в кожній області керівництва, з тим, щоб підтримувати спільні цілі і потреби зацікавлених сторін і таким чином ефективно підтримувати відповідність IT-рішень і послуг цілям підприємства.

Крок 1. Рушійні сили зацікавлених сторін впливають на їх потреби

На потреби зацікавлених сторін впливає ряд рушійних сил, наприклад, зміни стратегії, бізнес-середовище і законодавство,що змінюються, нові технології.

Крок 2. Потреби зацікавлених сторін зв'язуються з цілями підприємства

Потреби зацікавлених сторін можна пов'язати з набором універсальних цілей підприємства. Ці цілі були розроблені на основі вимірів в системі збалансованих показників (Balanced Scorecard1) і являють собою список найбільш широко використовуваних цілей, які підприємство може визначити для себе. Хоча цей список не є вичерпним, більшість цілей, сформульованих для конкретного підприємства, можна легко перевести в терміни універсальних.

Крок 3. Цілі підприємства зв'язуються з IT-цілями

Досягнення цілей підприємства вимагає отримання ряду IT-результатів, які описуються IT-цілями. Під IT розуміються інформаційні та пов'язані з інформацією технології, а IT-цілі структуруються за вимірюваннями збалансованої карти показників IT. COBIT 5 визначає 17 IT-цілей, представлених на малюнку 6. Матриця відповідності IT-цілей цілям підприємства представлена в додатку В. У цій матриці показано, яким чином кожна мета підприємства підтримується IT-цілями.

Крок 4. IT-цілі зв'язуються з цілями факторів впливу

Досягнення IT-цілей можливо лише при успішному застосуванні факторів впливу. Поняття фактора впливу докладно розглянуто в розділі 5. Фактори впливу включають в себе процеси, організаційні структури і інформацію, а для кожного фактора впливу можна визначити набір конкретних цілей, які зв'язуються з IT-цілями. Процеси є одним з факторів впливу, і в додатку З приведена матриця зв'язку між IT-цілями і процесами COBIT 5, в якій вказані цілі процесів.

1.2 ITIL

ITIL був розроблений наприкінці 1980-х років Центральним агентством обчислювальної техніки та зв'язку (CCTA)[7], урядовим агентством Великобританії. Причиною введення в експлуатацію CCTA була недостатня якість IT-послуг, що надаються британським урядом, і потрібно було знайти метод досягнення кращої якості за менших витрат. Тож CCTA вирішив розробити рекомендації щодо ефективного та результативного надання IT-послуг. Це призвело до каталогу найкращих практик для IT-організацій, який сьогодні відомий як "ITIL".

Історично IT-організації часто орієнтувались на програмне забезпечення, апаратне забезпечення та інші технології, а не на вимоги замовника. На цьому тлі ключовою ідеєю ITIL є те, що IT-послуги повинні бути зосереджені на потребах клієнтів, і що організації чітко погоджують послуги, що надаються зі своїми клієнтами. Це повинно поєднуватися з ефективними процесами та чітко визначеними обов'язками щодо надання послуг в рамках IT-організації.

Під час своїх досліджень CCTA виявила, що вимоги різних підприємств та організацій здебільшого були подібними, незалежно від їх розміру та галузевого сектору. Таким чином, рекомендації, складені CCTA, дійсні для організацій усіх типів та розмірів.

Серія книг про ITIL видається з 1989 року Кабінетом Міністрів, адміністративним органом уряду Великобританії. На початку 2014 року торгова марка ITIL® та інтелектуальна власність належать AXELOS, спільному підприємству між Кабінетом Міністрів та Capita Plc.

У 2007 році OGC опублікував повністю переглянуту версію ITIL, відому як "ITIL Версія 3 (ITIL V3)"[8].

Публікації ITIL 2 були оновлені в 2011 році з урахуванням відгуків користувачів та навчальної спільноти ("ITIL 2011").

Життєвий цикл обслуговування ITIL: ITIL стадіює стратегію обслуговування, дизайн послуги, перехід на службу, експлуатацію послуги та постійне вдосконалення служби.

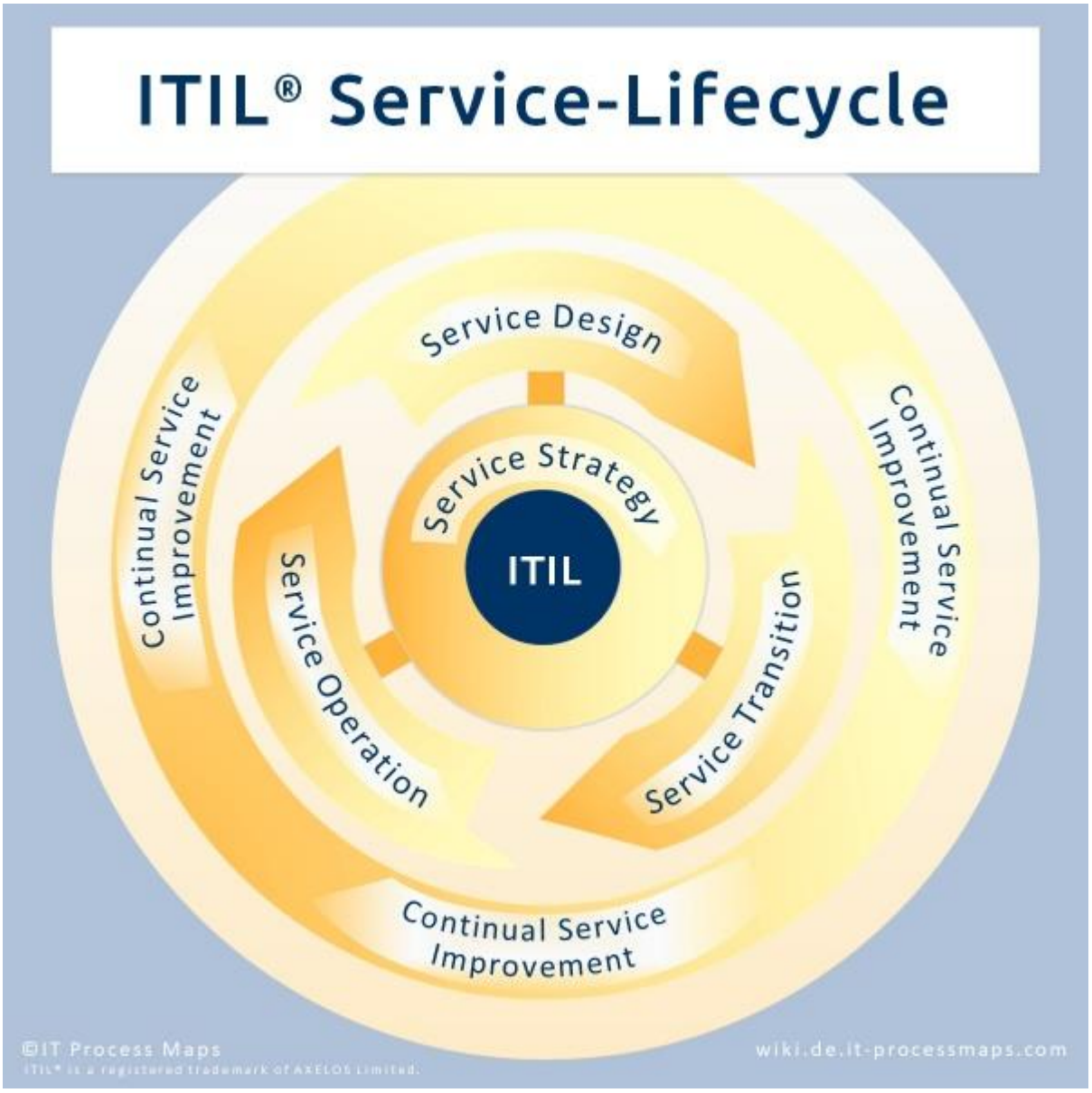

Рисунок 1.2.1 Життєвий цикл обслуговування ITIL та етапи ITIL

ITIL V3 складається з набору з п'яти основних публікацій, які разом утворюють життєвий цикл служби ITIL:

- Стратегія обслуговування[9]
- Дизайн послуг[10]
- Перехід послуги[11]
- Експлуатація послуги[12]
- Постійне вдосконалення послуг[13]

Обґрунтуванням організації книг ITIL таким чином було встановлення циклу, подібного до Демінга, план-до-перевірка-акт (PDCA), орієнтований на постійне вдосконалення. Цикл PDCA також помітно зафіксований у ISO 20000, міжнародному стандарті управління послугами, тому ITIL V3 краще узгоджується з ISO 20000, ніж попередні версії ITIL.

ITIL V3 доповнює процеси, відомі з ITIL V2, низкою нових процесів і робить більший акцент на створенні цінності для бізнесу.

Організаціям, які бажають запровадити процеси, вирівняні за ITIL V3, надається карта процесів ITIL - "переклад" ITIL V3 та процесів життєвого циклу служби в готові до використання, настроювані шаблони процесів.

1.3 ISO / IEC 27001

ISO / IEC 27001 - це міжнародний стандарт управління інформаційною безпекою[14]. Спочатку стандарт був опублікований спільно Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC) у 2005 році, а потім перероблений у 2013 році. Він деталізує вимоги щодо створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (ISMS) - мета якого - допомогти організаціям зробити інформаційні активи, якими вони володіють, більш захищеними. Європейське оновлення стандарту було опубліковане в 2017 році. Організації, які відповідають вимогам стандарту, можуть вибрати сертифікацію акредитованим органом з сертифікації після успішного завершення аудиту.

Більшість організацій мають ряд засобів контролю інформаційної безпеки. Однак без системи управління інформаційною безпекою (СУІБ) засоби управління, як правило, дезорганізовані та роз'єднані, часто застосовуються як точні рішення конкретних ситуацій або просто як умова. Засоби контролю безпеки, що функціонують, зазвичай стосуються певних аспектів інформаційних технологій (IT) або безпеки даних; залишаючи інформаційні ресурси, що не належать до IT (наприклад, документи та власні знання), в цілому менш захищеними. Більше того,

плануванням безперервності бізнесу та фізичною безпекою можна керувати цілком незалежно від IT чи інформаційної безпеки, тоді як практика управління персоналом може мало посилатися на необхідність визначення та розподілу ролей та відповідальності за інформаційну безпеку в організації.

ISO / IEC 27001 вимагає[15], щоб керівництво:

- Систематично вивчало ризики інформаційної безпеки організації, беручи до уваги загрози, вразливості та наслідки;
- Розробило та впровадило послідовний та всебічний набір засобів контролю інформаційної безпеки та / або інших форм лікування ризиків (таких як уникнення ризику або передача ризику) для вирішення тих ризиків, які визнані неприйнятними; і
- Прийняло всебічний процес управління, щоб забезпечити те, щоб засоби управління інформаційною безпекою продовжували задовольняти потреби організації в галузі інформаційної безпеки на постійній основі.

Слід зауважити, що ISO / IEC 27001 розроблений для охоплення набагато більшого, ніж просто IT.

Те, які засоби контролю будуть перевірені в рамках сертифікації за ISO / IEC 27001, залежить від аудитора сертифікації. Це може включати будь-які засоби контролю, які організація вважала такими, що входять до сфери застосування СУІБ, і це тестування може здійснюватися на будь-яку глибину або ступінь, за оцінкою аудитора, якщо це необхідно для перевірки того, що контроль впроваджений та діє ефективно.

Керівництво визначає сферу застосування СУІБ для цілей сертифікації та може обмежити її, скажімо, окремим бізнес-підрозділом або місцем розташування. Сертифікат ISO / IEC 27001 не обов'язково означає, що решта організації, що знаходиться за межами зони дії, має адекватний підхід до управління інформаційною безпекою.

Є 114 елементів управління в 14 групах та 35 категоріях контролю:

A.5: Політика інформаційної безпеки (2 елементи керування)

A.6: Організація інформаційної безпеки (7 елементів управління)

A.7: Безпека людських ресурсів - 6 засобів контролю, які застосовуються до, під час або після працевлаштування

A.8: Управління активами (10 елементів управління)

A.9: Контроль доступу (14 елементів управління)

A.10: Криптографія (2 елементи керування)

A.11: Фізична та екологічна безпека (15 засобів контролю)

A.12: Безпека операцій (14 елементів управління)

A.13: Захист зв'язку (7 елементів управління)

A.14: Придбання, розробка та обслуговування системи (13 елементів управління)

A.15: Взаємовідносини з постачальниками (5 елементів контролю)

A.16: Управління інцидентами інформаційної безпеки (7 елементів управління)

A.17: Аспекти інформаційної безпеки управління безперервністю бізнесу (4 засоби контролю)

A.18: Відповідність; з внутрішніми вимогами, такими як політика, та із зовнішніми вимогами, такими як закони (8 елементів контролю)

Елементи управління відображають зміни в технології, що зачіпають багато організацій, наприклад, хмарні обчислення, але, як зазначено вище, можна використовувати сертифікацію ISO / IEC 27001: 2013 і не використовувати жоден із цих елементів управління.

1.3.1 Узгодження COBIT 5 та ISO 27001

Основна різниця між COBIT 5 та ISO 27001 полягає в тому, що ISO орієнтований лише на СУІБ, тоді як COBIT 5 зосереджений на більш загальних IT-контролях[16]. Таким чином, COBIT 5 має більш широке охоплення загальних IT-доменів, але не має стільки детальних вимог СУІБ, як ISO 27001 (Sheikhpour & Modiri, 2012).

Декілька досліджень підходили до узгодження між COBIT та ISO 27001 (Aaen, 2003), (Sahibudin, Sharifi, & Ayat, 2008), (Sheikhpour & Modiri, 2012), (Haufe, Colomo-Palacios, Dzombeta, Brandis, & Stantchev , 2016), але ці дослідники або відобразили практики EGIT на дуже абстрактному рівні, відповідаючи критеріям схожості процесу (Nicho & Muamaar, 2016) (Haufe, Colomo-Palacios, Dzombeta, Brandis, & Stantchev, 2016), або нанесли попередні версії, які були замінені новішими версіями, такі як COBIT 4.1 та ISO 27001: 2005 (Aaen, 2003), (Sahibudin, Sharifi, & Ayat, 2008), (Sheikhpour & Modiri, 2012).

Незважаючи на ці перешкоди, такі дослідження дають цінні вказівки щодо узгодження поточних версій COBIT та ISO 27001. Одним із таких випадків є вибір, який процес є найбільш адекватним для демонстрації картографії. Шуканою ознакою є високий ступінь подібності між відповідними процесами, описаними в EGIT Practices. Для цього випуску Haufe (Colomo-Palacios, Dzombeta, Brandis, & Stantchev, 2016) пропонує метод рівня процесу для аналізу між ISO 27001 та COBIT 5.

1.4 ISO / IEC 27002

ISO / IEC 27002 - це стандарт інформаційної безпеки, опублікований Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC), під назвою “Інформаційні технології - Технології безпеки - Звід практики контролю за інформаційною безпекою”[17].

Стандарти серії ISO / IEC 27000 походять від стандарту корпоративної безпеки, подарованого компанією Shell урядовій ініціативі Великобританії на початку 1990-х років. Стандарт Shell був розроблений у британський стандарт BS 7799 у середині 1990-х років і був прийнятий як ISO / IEC 17799 у 2000 році. Стандарт ISO / IEC був переглянутий у 2005 році та перенумерований у ISO / IEC 27002 у 2007 році для узгодження з Стандарти серії ISO / IEC 27000. Його було переглянуто ще раз у 2013 році. Пізніше у 2015 році ISO / IEC 27017 був створений

із цього стандарту з метою запропонувати додаткові засоби контролю безпеки для хмари, які не були повністю визначені в ISO / IEC 27002.

ISO / IEC 27002 надає рекомендації щодо найкращих практик щодо засобів контролю за інформаційною безпекою для використання особами, відповідальними за ініціювання, впровадження або підтримку систем управління інформаційною безпекою (СУІБ). Інформаційна безпека визначена в рамках стандарту в контексті тріади(CIA):

- збереження конфіденційності (забезпечення того, щоб інформація була доступна лише для тих, хто має дозвіл на доступ)
- цілісності (забезпечення точності та повноти інформації та методів обробки)
- доступності (забезпечення доступу уповноважених користувачів до інформації та пов'язаних з нею активів, коли це потрібно).

Зміст ISO / IEC 27002: 2013

Стандарт починається з 5 вступних розділів:

- Вступ
- Сфера дії
- Нормативні посилання
- Терміни та визначення
- Структура цього стандарту

Далі слідують 14 основних розділів:

- Політика інформаційної безпеки
- Організація інформаційної безпеки
- Безпека людських ресурсів
- Управління активами
- Управління доступом
- Криптографія
- Фізична та екологічна безпека
- Операційна Безпека - процедури та відповідальність, Захист від зловмисного програмного забезпечення, Резервне копіювання, реєстрація та

моніторинг, Контроль операційного програмного забезпечення, Управління технічними вразливостями та Координація аудиту інформаційних систем

- Безпека зв'язку - управління мережевою безпекою та передача інформації
- Придбання, розробка та обслуговування системи - Вимоги до безпеки інформаційних систем, Безпека в процесах розробки та підтримки та Тестові дані
- Взаємовідносини з постачальниками - Інформаційна безпека у відносинах з постачальниками та управління наданнями послуг постачальника
- Управління інцидентами інформаційної безпеки - Управління інцидентами та вдосконаленнями інформаційної безпеки
- Аспекти інформаційної безпеки управління безперервністю бізнесу - Безперервність інформаційної безпеки та надмірності
- Відповідність - дотримання законодавчих та договірних вимог та огляд захисту інформації

У кожному розділі зазначено та окреслено засоби контролю за інформаційною безпекою та їх цілі. Контроль за інформаційною безпекою, як правило, розглядається як найкращий спосіб досягнення цих цілей. Для кожного з засобів контролю передбачено вказівки щодо впровадження[18].

Конкретний контроль не передбачений, оскільки:

Очікується, що кожна організація проведе структурований процес оцінки ризиків інформаційної безпеки, щоб визначити свої конкретні вимоги, перш ніж вибрати засоби контролю, які відповідають її конкретним обставинам. У розділі вступу викладається процес оцінки ризиків, хоча існують більш конкретні стандарти, що охоплюють цю сферу, такі як ISO / IEC 27005. Використання аналізу ризиків інформаційної безпеки для керування вибором та впровадженням засобів контролю інформаційної безпеки є важливою особливістю ISO / IEC Стандарти серії 27000: це означає, що загальні поради щодо належної практики в цьому стандарті пристосовуються до конкретного контексту кожної організації-користувача, а не застосовуються по суті. Наприклад, не всі 39 цілей контролю мають значення для кожної організації, отже цілі категорії контролю можуть не вважатися необхідними.

Стандарти також є відкритими в тому сенсі, що "засоби інформаційної безпеки" пропонуються", залишаючи відкритими двері для користувачів, щоб вони, за бажанням, застосовували альтернативні засоби контролю, до тих пір, поки ключові цілі контролю, пов'язані з пом'якшенням ризиків інформаційної безпеки, задоволені. Це допомагає підтримувати відповідність стандарту, незважаючи на зміну характеру загроз, вразливостей та впливів на інформаційну безпеку та тенденцій використання певних засобів управління інформаційною безпекою.

Висновки за розділом 1

На базовому рівні COBIT забезпечує дорожню карту того, що потрібно зробити, а ITIL пропонує засоби досягнення цих цілей. Наприклад, менеджери можуть використовувати COBIT для вирішення, які процеси потрібні організації, а ITIL говорить їм, як їх здійснювати.[19]

Крім того, COBIT вирішує питання щодо IT-ресурсів з точки зору бізнесу в цілому, тоді як ITIL підходить до цих питань суворо з точки зору IT. COBIT йде по шляху "зверху вниз", а ITIL використовує шлях "знизу вгору"[20].

Саме по цій причині замість вибору між ними краще використати ці 2 стандарти разом. В даному випадку ISO 27001 та COBIT 2019 - це стандарти, що стосуються того, як організації керують та контролюють свої IT-системи. Ці два механізми працюють по-різному, але велика різниця між ними полягає в тому, що ISO 27001 стосується головним чином безпеки, тоді як COBIT 5 - це загалом IT. Що зовсім не означає, що COBIT 5 не може бути використано в цілях ІБ, навпаки – за допомогою поєднання з ISO 27001 вони формують більш досконалі вимоги для СУІБ.

РОЗДІЛ 2
ЗАГРОЗИ, ВРАЗЛИВОСТІ ТА ПОВ'ЯЗАНИЙ З НИМИ РИЗИК

2.1 Категорія вразливостей та загроз

Трансформація безпеки починається з виявлення, класифікації та картографування вразливих місць, загроз та ризиків. Це пояснюється в наступному розділі. Усі наступні вказівки слід розглядати як частину безперервного життєвого циклу, який робить кібербезпеку життєздатним та ефективним бізнес-процесом. Сюди входить аналіз посмертних випадків та включення минулих атак, випадків та випадків успішних злочинних дій проти підприємства або його асоційованих підприємств. Ключовим фактором успіху є організаційне навчання, інституціоналізоване в системному циклі.

З точки зору кібербезпеки, загрози та вразливості необхідно класифікувати, як і пов'язаний з ними ризик. На відміну від загальної інформаційної безпеки, основна увага приділяється розширеним загрозам та уразливостям, які ні легко виявити, ні легко усунути. Наступні підрозділи стосуються загроз, вразливостей та ризиків з огляду на потенціал кіберзлочинів та кібервійни. Рисунок 10 ілюструє, як їх відокремити від менш складних щоденних атак та інцидентів, якими керують у процесі загальної інформаційної безпеки.

Ліворуч на схемі загрози, вразливості та ризики можуть бути вирішені за допомогою стандартних методів, методів та заходів з управління безпекою. Праворуч від діаграми, більш просунуті загрози, вразливості та ризики вимагають іншого виду лікування, який є частиною кібербезпеки. На рисунку 2.1.1 також показано, як потенційна небезпека (від низького до сильного) відповідає зросту технічної досвідченості, необхідної для підготовки та розгортання атак. Показані категорії атак є наочними, і типів атак на різних рівнях може бути набагато більше[21].

Залишковий ризик значно менший, але значно важливіший з точки зору потенційного впливу на підприємство та його асоційовані компанії. Як правило, кіберзлочинність та кібервійни, ймовірно, використовують найслабші ланки ланцюжка доданої вартості підприємства або в індивідуальному захисті людини. Там, де технічна вдосконаленість, а також час і гроші, витрачені на атаку, дуже великі, зловмисники, швидше за все, ретельно вибирають свої цілі та можливості для фактичного нападу[22].

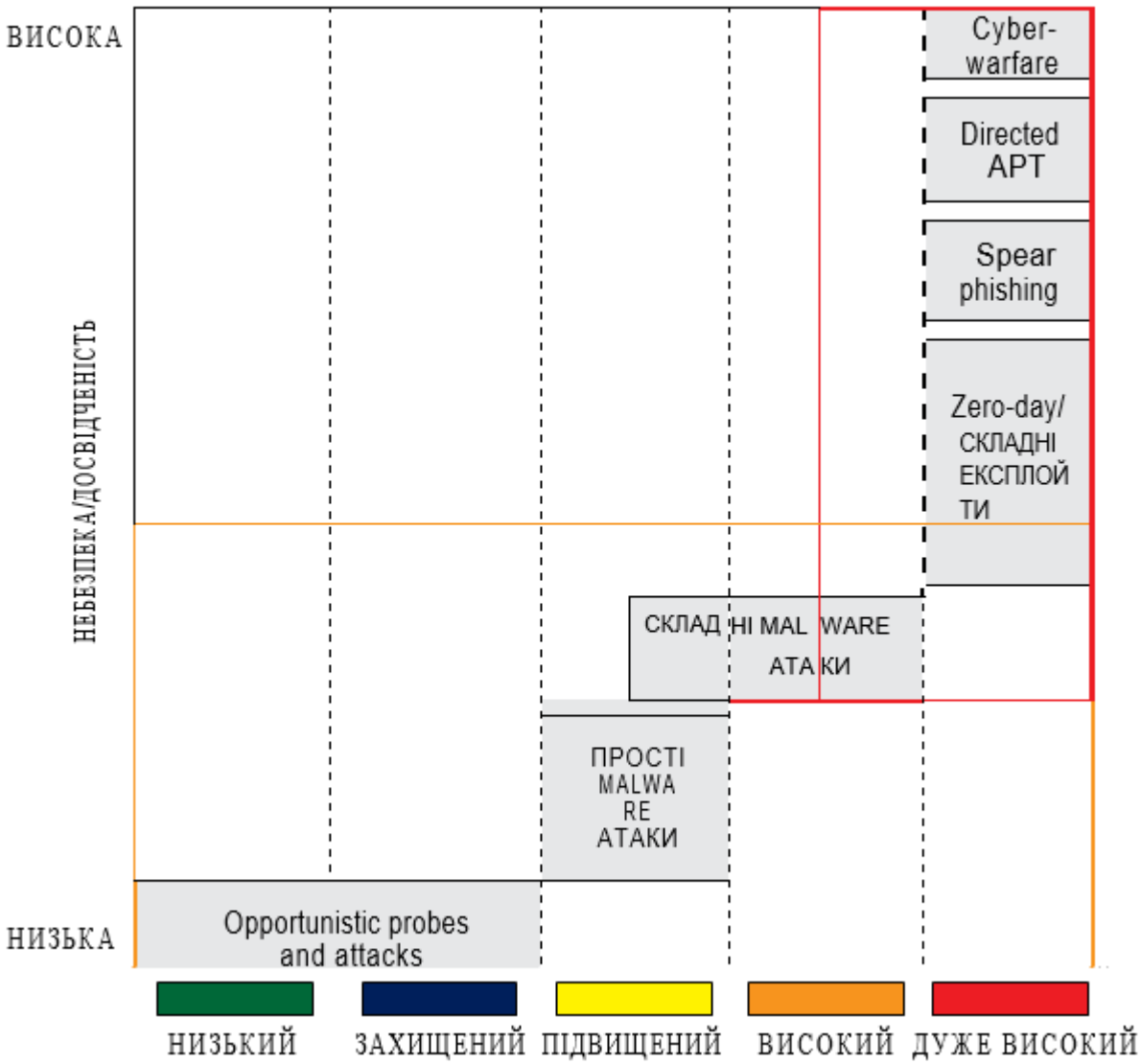

Рисунок 2.1.1 Загрози, співвідношення їх небезпеки і досвідченості атакуючих

Вибрана тут підгрупа загроз, вразливостей та ризиків є надзвичайно важливою для управління інформацією та кібербезпеки. Там, де людський інтелект і непередбачуваність є частиною фону атаки, перспектива управління безпекою,

природно, переходить із суто превентивного режиму на керований розвідкою. Частина кібербезпеки явно виходить за межі часто цитованого "не можна планувати все і запобігати цьому" і стосується саме тих (ймовірних чи неймовірних) атак та порушень, які вимагають цілеспрямованого реагування та слідчих дій.

Для подальшої класифікації ризиків слід враховувати відносну ймовірність та правдоподібність. Не кожна можливість для кіберзлочинності буде використана, враховуючи те, що існує кілька факторів[23], які можуть вплинути на ймовірність:

- Мотив - Чому інформація є настільки привабливою, або чому злочинці націлюються на якусь конкретну частину підприємства?
- Можливість - чи є явні скупчення вразливостей, які викликали б кіберзлочинність чи кібервійну? Які порівняно добре захищені та відкриті частини підприємства?
- Зусилля - яким буде час опору, відносна сила захисту та потенційні зусилля, необхідні для пробиття цих захистів?

Всі три фактори, взяті разом, дають досить вичерпну картину фактичної ризикової ситуації щодо підприємства та його асоційованих компаній. Там, де мотивів не існує, цілеспрямовані атаки є малоймовірними (незважаючи на будь-які опортуністичні атаки).

Там, де можливості для нападу обмежені, це буде сильним стримуючим фактором для злочинців, які можуть обрати «легшу» ціль. Там, де необхідні зусилля занадто високі з огляду на очікувану віддачу, знову навряд чи напади відбуватимуться заплановано і цілеспрямовано.

Звичайно, така категоризація ризиків ніколи не може виключити будь-яких атак, і інциденти можуть трапитися випадково або в рамках невибіркової серії опортуністичних кампаній, "спроб і помилок". Однак ці типи атак не є основною проблемою кібербезпеки. Природно, може бути більше вразливостей, загроз та наслідків ризику чи наслідків. Однак критерії мотиву, можливості та зусиль застосовуються завжди. На малюнку нижче показано контекст цих критеріїв для кожного з прикладів вразливості. Залежно від підприємства, список вразливих місць може відрізнятися. Типова виробнича компанія може наголосити на аспекті

технічної інфраструктури, що не відноситься до IT, тоді як консалтингова фірма може сприймати себе більш вразливою до соціальних інженерій або атак, пов'язаних з подорожами. Остаточний перелік уразливостей та загроз - це те, що, принаймні частково, повинно існувати як функція загального управління інформаційною безпекою та управління інформаційними ризиками.

Таблиця 2.1.1 Вразливості і пов’язаний з ними ризик

Вразливість	**Загроза**	**Ризик та вплив**
Направлений фішинг[24]	Зловмисники можуть отримати доступ за допомогою фіш-адресата або комбінованого соціально-технічні дії.	Первісна втрата або витік даних, що приводить до вторинного фінансового та операційного впливу
Water holing[25]	Зловмисники можуть отримати контроль над привабливими веб-сайтами і подальший контроль над відвідувачами.	Початкові поведінкові помилки, що призводять до вторинних фінансових і операційних наслідків
Wireless/mobile APT[26]	Атаки можуть скомпрометувати бездротові канали та / або мобільні пристрої, щоб забезпечити тимчасовий або постійний контроль.	Частковий або повний контроль однієї або декількох бездротових установок і / або мобільних пристроїв; прямий або непрямий вплив на все критично важливі IT-додатки і сервіси
Zero-day[27]	Атаки використовують експлойти нульового дня для обходу існуючих засобів захисту.	Частковий або повний контроль над додатками і базовими системами / інфраструктурою, що призводить до вторинного операційного впливу
Надмірні привілеї[28]	Внутрішні атаки можуть відбуватися з використанням невідповідних привілеїв і прав доступу.	Повний і (технічно) законний контроль поза рамками організаційного GRC, вторинні фінансові, операційні та репутаційні наслідки
Соціальна інженерія[29]	Зловмисники використовують соціальні уразливості для отримання доступу до інформації та / або систем.	Частковий або повний контроль над людьми, подальша компрометація IT-сторони, вторинний вплив на приватне /

		індивідуальне благополуччя

Продовження табл.2.1.1

Home user APT[30]	Атаки використовують той факт, що домашня середовище може бути менш добре захищена, ніж організаційна.	Частковий або повний контроль над додатками, системами і домашньої інфраструктурою, вторинні фінансові, операційні та репутаційні наслідки, включаючи вплив на приватне / індивідуальне благополуччя добробут
Extended IT infrastructure APT[31]	Атаки можуть бути спрямовані на IT-інфраструктуру, що лежить в основі критично важливих організаційних процесів.	Повний контроль інфраструктури, ризик розширення контролю, включаючи державні інфраструктури або ділових партнерів
Non-IT technical infrastructure APT[32]	Атаки можуть долати бар'єр між IT та іншими критичними інфраструктурами підприємства.	Частковий або повний контроль над нестандартної IT і технічною інфраструктурою, наприклад, диспетчерський контроль і збір даних (SCADA), вторинне оперативне вплив
Vendor/business partner exploit[33]	Існують атаки на надійних бізнес-партнерів або постачальників, які ставлять під загрозу ключове програмне забезпечення або поставки.	Первинна атака через IT організації, спрямована на третіх осіб, з фінансовими, операційними і репутаційні наслідками

Виходячи з перечисленого вище, можемо прийти до висновків щодо мотивів, можливостей і зусиль:

Таблиця 2.1.2 Вразливості і їх аналіз

Вразливість	**Мотив**	**Можливість**	**Зусилля**
Направлений фішинг	Фінансовий, конкурентне шпигунство, крадіжка даних і т.д; часто підготовчий етап до основної атаки	Доступ до електронної пошти до цілі	Від середнього до високого, залежно від якості фішу

Water holing	Фінансовий, конкурентне шпигунство, крадіжка даних і т.д .; часто є підготовкою до основної атаці	Доступ до електронної пошти цілі, контроль над привабливими веб-сайтами (тимчасова) близькість до мети	Висока, залежно від точності націлювання

Продовження табл.2.1.2

Wireless/mobile APT	Фінансовий, шпигунство, шантаж / вимагання, крадіжка персонально ідентифікованої інформації (PII) і т.д.	Наявність відповідних експлойтів нульового дня, організована обробка експлойтів	Від низького до середнього
Zero-day	Фінансові, оперативні, крадіжка даних, шантаж / вимагання, контроль над технічною інфраструктурою		Від середнього до високого
Надмірні привілеї	Фінансові, особисті (наприклад, незадоволений співробітник), крадіжка даних, шантаж / вимагання, репутаційні	Недоліки в управлінні ідентифікацією та доступом, корупція і т.д.	Від низького до середнього
Home user APT	Фінансові, шпигунство, крадіжка даних, крадіжка PII і т.д.	Фізичний або логічний доступ до цілі	Від низького до високого, залежно від рівня захисту цільового середовища
Extended IT infrastructure APT	Оперативні, шантаж / вимагання, контроль над технічною інфраструктурою, пошкодження або видалення даних, кібервійна	Логічний доступ до цілі, перед яким часто інші форми атаки	Високий до дуже високий, залежно від рівня захисту цільового середовища
Non-IT technical infrastructure APT	Оперативна діяльність, шантаж / вимагання, контроль над технічною інфраструктурою, пошкодження або видалення даних, кібервійна	Логічний доступ до цілі, перед яким часто інші форми атаки	Високий до дуже високий, залежно від рівня захисту цільового середовища
Vendor/business partner exploit	Фінансові, особисті (наприклад, незадоволений співробітник), крадіжка даних, шантаж / вимагання, репутація	Логічний доступ до цілі, перед яким часто є інші форми атаки	Від низького до високого, залежно від зусиль, необхідних для вступних атак

2.2 Виявлення системних слабких сторін

Розглядаючи різні сценарії ризику та їх вплив на підприємство, “слабкі місця” поступово стануть зрозумілими. Не всі вразливі місця та загрози можуть бути застосовні до підприємства або його асоційованих компаній, і в деяких випадках рівень захисту буде достатньо високим, щоб забезпечити розумний рівень стримування. Що стосується лікування ризиків та управління ризиками, слід вивчити потенційні основні причини або фактори, що сприяють кожній вразливості, загрозі та ризику. Дуже часто це вказує на загальні слабкі місця або недоліки, які можна віднести до компонентів системної моделі безпеки.

Як приклад, фішинг (спис або динаміт13), водяні отвори та значні частини соціальної інженерії мають однакові точки контакту або входу: електронна пошта, соціальні мережі чи інші прямі канали зв'язку. Незважаючи на те, що технічний зміст і якість атак не можна передбачити і демонструє широкі розбіжності, ключовим фактором для розпізнавання атаки є початковий контакт з підприємством та одним або кількома його партнерами:

- Початкова слабкість / сприяючий фактор - Успішне спілкування з користувачем.
- Основна причина (причини) - організаційний ризик, особистий ризик реагуванням на початковий контакт - успіх атаки залежить від виникнення людської помилки.
- Системна слабкість - представлена людьми, культурою та появою.

Щоб навести інший приклад, атаки на бездротових або подорожуючих користувачів та розширені атаки на нижчі рівні IT-інфраструктури часто використовують подібні методи з точки зору

Вразливості, засновані на IT, і експлойти нульового дня. Знову ж таки, точний характер будь-якої атаки важко передбачити, але головним є низький і технічно вдосконалений пункт входу в цільову систему, тобто технічний недолік:

- Початкова слабкість / сприяючий фактор - наявність відомого або невідомого технічного недоліку, що дозволяє в'їзд

- Основна причина (причини) - Технічний ризик, організаційний ризик, дозволяючи існування IT-слабких місць - успіх атаки залежить від кількості відкриттів або наявності відповідних експлойтів
- Системна слабкість – представлена технологіями, архітектурою та можливостями і підтримкою

Важливо виявити та описати ці системні слабкі місця, щоб зрозуміти, як і де найімовірніше трапляються атаки та порушення безпеки. У контексті мотивів, можливостей та зусиль ймовірність нападу тісно пов’язана із шляхом найменшого опору, принаймні з точки зору нападника.

Інтеграція історії нападів та інцидентів

Більшість підприємств певною мірою зазнавали порушень безпеки, інцидентів та атак. Однак досвід, отриманий в результаті таких випадків, часто трактується поодиноко, враховуючи, що наслідки можуть бути шкідливими. Так само на підприємствах спостерігається невдала тенденція швидко переходити в режим відмови після успішної атаки чи інциденту. Це, швидше за все, спричинено тим, що сучасні підприємства, мабуть, погано переносять помилки чи упущення. Майже автоматично такі випадки за замовчуванням шукають людей чи речі, які звинувачують, як правило, із серйозними особистими наслідками для причетних. Як неминучий результат, більше енергетичних та організаційних зусиль спрямовано на заперечення наявності помилок, спростування тверджень про необережність чи неправомірні дії та загальний захист особистих інтересів. Це може зайти аж до суперечки про те, чи слід дійсно подію, пов’язану з безпекою, класифікувати як «атаку» чи «інцидент», і результат часто є повним запереченням значення тригера. Природно, що такі «не події» за визначенням навряд чи будуть використовуватися як джерела інтелекту та навчання. В порядку щоб подолати ці перешкоди для належного аналізу та подальшого використання інформації про атаки та події, слід встановити прості правила, подібні до тих, що вперше були запроваджені в так званих організаціях високої надійності:

- Деперсоналізуйте атаку чи інцидент. Хто брав участь (якщо це не внутрішня атака), менш цікавий, ніж те, що сталося. Людська помилка - це пояснення, але не вирок.
- Зосередьтеся на попередніх системних слабких місцях, які могли сприяти нападу чи інциденту: Знову ж таки, цікавіше достовірно визначити будь-які важкі факти чи збіги, які могли створити вікно можливостей.
- Ставтеся до даних про напади та події як до навчальних матеріалів, а не лише як до криміналістичних доказів.
- Відокремте команду, яка навчається, від слідчої групи, враховуючи, що бажаний результат помітно відрізняється для обох команд.

Щоб належним чином зрозуміти ризик кібербезпеки та системні слабкі сторони, минулі атаки та інциденти слід проаналізувати та повністю інтегрувати у процес управління ризиками. Це включає вирішення таких питань:

- Чи є загальний досвід щодо нападу чи інциденту? Чи є якісь системні слабкі місця?
- Чи можна запобігти повторення цього виду нападу чи інциденту? Чи можна усунути вразливі місця та загрози?
- Якщо попередні напади / інциденти неможливо надійно запобігти, чи можна стримувати чи пом'якшити вплив?
- Якщо ні усунення, ні пом'якшення наслідків недоступні, чи можна надійно визнати початок нападу / інциденту? Чи доступні будь-які контрзаходи на момент нападу?

Детальні дані про минулі напади та інциденти є важливим фактором, що підтримує аналіз ризику. Там, де існує адекватна кількість інформації, реальні події минулого також додають цінності виявленню системних слабких місць та першопричин. У порівнянні із загальнодоступною статистикою минулі напади та інциденти можуть забезпечити показник позиціонування підприємства з точки зору фактичного ризику та порівняно із загальнодоступними даними за секторами, регіонами чи країнами.

На практиці ні опубліковані дані, ні аналіз історії атак та інцидентів не дають повного уявлення про вразливості, загрози та ризики кібербезпеки. Однак інтеграція будь-якої наявної історії принаймні підтримає лікування та управління ризиками та надасть цінну інформацію. Слід зазначити, оскільки нові типи атак, як правило, еволюціонують з часом, що покладання на історію атак та інцидентів само по собі недостатньо для управління нинішнім та майбутнім ризиком кібербезпеки.

2.3 Організаційний ризик

Організаційний ризик[34], разом із кіберзлочинністю та кібервійною, є частиною організаційного проекту, а також здатності дотримуватися системного життєвого циклу кібербезпеки. Це включає організаційну стратегію та структуру, аспекти управління кібербезпекою та організаційна культура. Більшість ризиків тісно пов’язані із проблемами досягнення змін та відображенням ситуації, яка є. Це схоже на організаційний ризик у загальній інформаційній безпеці, але наслідки більш виражені в галузі кібербезпеки. На малюнку 13 наведено огляд ризику. У процесі трансформації кібербезпеки вирішення організаційних ризиків є дуже важливою складовою дисциплін управління та управління.

Організаційний дизайн часто сприяє досить жорсткому розподілу обов'язків і створює елеватори для корпоративної безпеки, захисту інформації та інших функцій. Що стосується кібербезпеки, то основний ризик є результатом зосередження керівництва та управління безпекою у порівняно невеликих та вузьких організаційних підрозділах. Тоді вторинний ризик (див. табл. 2.3.1) є наслідком нерівномірно розподіленого IT-знання та навичок, необхідних для запобігання, розпізнавання та управління порушеннями безпеки та інцидентами. Там, де лише декілька людей здатні повністю зрозуміти та боротися з кібербезпекою, часто важко поширити ці знання та досягти бажаного рівня захисту та безпеки.

Таблиця 2.3.1 Аналіз організаційних ризиків

Ризик	Опис	Потенційні наслідки
Дизайн і структура - якість та розподіл знань	Кібербезпека структурована в елеватори, що перешкоджає обміну знаннями.	Схильність до нападів, оскільки більшість співробітників не в змозі розпізнати напади, кіберзлочинність та кібервійни

Продовження табл.2.3.1

Дизайн і структура - надмірна впевненість	Неправильне сприйняття керівництвом фактичного стану кібербезпеки	Недостатнє фінансування, обмежена увага керівництва, що спричиняє вплив до атак
Дизайн і структура — інтерфейси	Недоліки у співпраці для розпізнавання атак та порушень та реагування на них	Управління кібербезпекою роздроблене, залишаючи прогалини, які можуть бути використані.
Управління, дотримання та контроль - недоліки контролю	Відсутність управління та дотримання положень, недостатня засоби кібербезпеки	Недостатня підготовка, визнання, розслідування та реагування на напади та порушення; підвищений рівень помилок людини
Управління, дотримання та контроль - надмірний контроль	Надто складна система управління та дотримання вимог, засоби управління, що враховують навіть найдрібніші деталі	Жорстка структура управління створює можливості для атак і порушення.
Культура — довіра	Культура довіри частково або повністю заперечує кіберзлочини та кібервійни.	Неявна або явна довіра може бути використана в соціальних та технічних атаках.
Культура — пильність	Індивідуальна пильність зменшується в контексті управління, дотримання та контролю.	Напади та порушення можуть бути не визнані своєчасно.
Культура — заперечення	Привабливість щодо нападів апріорі заперечується.	Фактичні атаки можуть не розпізнаватися або трактуватися неправильно.

У багатьох випадках вищий менеджмент підприємства менш знайомий з аспектами кіберзлочинності та кібервійни. Як і в більш загальній сфері

інформаційної безпеки, керівники вищого рівня потерпають від неправильного сприйняття, а також упереджених поглядів. Одним із значних ризиків, що виникає внаслідок обмеженого або хибного погляду на кібербезпеку, є надмірна впевненість багатьох підприємств. Їх офіційна позиція полягає в тому, що, очікуючи зростання кібератак, вони почуваються "дуже впевнено" або "впевнено" 16 щодо свого захисту. Цей ризик посилюється тим, що ці підприємства застосовують консервативний підхід до витрат на безпеку.

На відміну від інших дисциплін загальної безпеки, кібербезпека не є окремим і кінцевим полем діяльності. Оскільки напади та порушення з часом еволюціонують, реакції організації повинні змінюватися та адаптуватися. Для вирішення інциденту часто потрібна спільна робота декількох частин підприємства, наприклад, інформаційна безпека, антикризове управління та безперервність бізнесу. Ризик, що виникає, виявляється в тому, що взаємозв'язки між цими різними дисциплінами не визначені або недостатньо визначені.

На багатьох підприємствах управління інформаційною безпекою та їх відповідність розроблено до рівня, де існують детальні вказівки для користувачів, включаючи політику, стандарти та спеціалізовані процедури. Що стосується кіберзлочинів та кібервійни, існує декілька сценаріїв ризику, які необхідно розглянути.

Якщо положення про управління та відповідність та відповідні засоби контролю не існують, інформаційна безпека може недостатньо охоплювати кібербезпеку. На практиці це часто зустрічається там, де мало обізнаних про кіберзлочинність, кібервійну

та пов'язані інциденти. Наприклад, у малих та середніх підприємств може бракувати функціональних ресурсів, часу та бюджету, що призводять до недоліків в управлінні безпекою та дотриманні вимог, а також відсутність належного контролю. В інших випадках упередженість надмірної довіри (як уже згадувалося раніше) перешкоджає розвитку та вдосконаленню управління кібербезпекою, оскільки керівництво не визнає необхідності постійних зусиль.

І навпаки, управління та дотримання в галузі кібербезпеки іноді призводять до дуже детальних та жорстких систем управління та дотримання з численними засобами контролю, призначеними для охоплення всіх аспектів безпеки та поведінки людей. Існує ризик надмірного контролю, особливо там, де індивідуальна поведінка суворо прописана і

контрольований. Підприємства, що перебувають у режимі надмірного контролю, часто демонструють дуже передбачувану, але тим не менш мляву та громіздку реакцію на випадки кіберзлочинів або кібервійни. Значна частина цього ризику пов'язана з тим, що організаційні підрозділи та асоційовані організації можуть бути зобов'язані правилами, тоді як зловмисники можуть використовувати їх.

Організаційна культура, що виражається у відносинах між самим підприємством та асоційованими людьми, є вирішальним елементом у перетворенні кібербезпеки.

Культурні фактори представляють низку важливих сценаріїв ризику, які можуть сприяти атакам та порушенням безпеки. Там, де керівна організація визначила та визначила цільовою організаційну культуру, ця цільова держава вимагає фактичного та поведінкового втручання від усіх рівнів людей, а в більшості випадків від зовнішніх ділових партнерів.

Багато підприємств покладаються на принцип явної (і неявної) довіри для управління інформаційною безпекою. Хоча це може бути гарною практикою для формування доброзичливого та позитивного робочого середовища, це представляє ризик з точки зору кібербезпеки. Там, де існує культура довіри, вона може бути використана внаслідок внутрішніх або зовнішніх атак (іноді в змові), а різні APT можуть досягти стійкості, оскільки постійні порушення не виявляються і не розслідуються. Навіть там, де підприємства пишаються своєю культурою довіри, управління ризиками з точки зору кібербезпеки повинно передбачити та реагувати на той факт, що він може бути використаний.

Значна частина кібербезпеки покладається на особисту пильність та індивідуальну готовність та здатність розпізнавати незвичну діяльність, потенційні

загрози та наявні вразливі місця. Залежно від організаційної структури (див. Попередній підрозділ) та існуючих механізмів управління та дотримання, природний рівень обережності та пильності, наявний у більшості людей, часто знижується тим, що «інші мають справу з цим» (силоси та нерівномірний розподіл знань). Так само, стан надмірного контролю змусить людей зректися відповідальності та пильності на користь просто дотримання правил. Ці та інші явища, очевидно, збільшують вплив нападів та порушень, особливо прогресивних, спрямованих на культурні слабкості.

На великій кількості підприємств потенційні загрози та ризики кіберзлочинів та кібервійни прямо заперечуються через різноманітні фактори. На малих та середніх підприємствах досить часто спостерігається ставлення "ми малі та нецікаві до винних". На більших підприємствах припущення

«Ризик та небезпека кіберзлочинності завищені», схоже, взяли своє місце, принаймні певною мірою. Культурний ризик заперечення існування або тяжкості нападів та порушень, ймовірно, пов'язаний з нерівномірним розподілом знань та наслідком неправильного сприйняття чи неправильного тлумачення вищим керівництвом.

2.4 Соціальний ризик

Кібербезпека як дисципліна включає соціальне середовище людей, підприємств та пов'язані з ними процеси. На додаток до інших типів ризиків, соціальний ризик в першу чергу виникає внаслідок людей та їхньої поведінки, людських факторів, що використовують IT, та стихійних або поступових змін у загальній системі. На таблиці нижче перелічено різноманітні сценарії соціального ризику.

Таблиця 2.4.1 Соціальні ризики

Ризик	Опис	Потенційні наслідки
Люди — навички	Люди не мають достатніх навичок для розуміння та впровадження	Концепції та дії з кібербезпеки не можуть бути повністю реалізовані, що призводить до підвищеного ризику атак

	кібербезпеки.	і порушення.
Люди — правила	Люди неохоче приймають і інтерналізують правила кібербезпеки.	Недоліки, зростаюча кількість вразливостей та загроз, більше можливостей для атак
Люди — дотримання	Люди мимоволі чи свідомо здійснюють або допускають порушення безпеки.	Напади, спричинені слабкими місцями людей, змовою чи внутрішніми атаками; корупційні дії; інфільтрація

Продовження табл.2.4.1

Культура - керівництво та відповідальність	Особиста відповідальність може бути зменшена (або перебільшена) як функція переважаючого стилю керівництва	Недостатній або надмірний акцент на особистій відповідальності може призвести до дисфункціональної поведінки та відповідне збільшення ризику нападів або порушень.
Культура - суспільний контекст	Суспільний контекст, несприятливий для кіберзлочинів та кібервійни або майже не знає про них	
Культура — людська помилка	Високий потенціал або частота помилок внаслідок різних факторів	Суспільство в цілому або загальна культура не сприяють індивідуальному прийняттю думок про кібербезпеку. Напади або порушення частіші через людські помилки
Людський фактор - складність	Кібербезпека є надто складною і, отже, дисфункціональною.	Невдачі або недоліки та збільшення потенціалу атаки / порушення
Людський фактор - зручність	Люди ігнорують або відмовляються від кібербезпеки на користь зручності.	Зручність на основі зручності або неадекватне використання IT та систем із вразливими місцями та погрози
Людський фактор - розриви	Індивідуальне (керівництво) налаштування на заперечуючі аспекти кібербезпеки	Невігластво, упередження, короткочасність, штурм, обмежена раціональність та інші фактори збільшують ризик нападів / порушень
Поява - звична поведінка	Сильні звички у людей перешкоджають вдосконаленню /	Схеми поведінки не відповідають бажаним моделям поведінки, що збільшує ризик безпеки.

	впровадженню кібербезпеки.	
Поява - зміна парадигми	Суспільні / культурні парадигми використання IT	Фундаментальні зміни в способі використання IT збільшують ризик безпеки.
Поява - інтерпретаційне упередження	Суспільні / культурні парадигми використання IT Процеси в кібербезпеці трактуються неправильно або не повністю зрозумілі	Помилкове тлумачення збільшує кількість вразливостей та загроз..

2.5 Людський фактор

Люди використовують IT безперешкодно і складно, як в організаційній, так і в приватній обстановці. Для цього часто потрібен повний набір IT-навичок, особливо там, де люди покладаються на програми та процеси для обробки конфіденційних даних або транзакцій. На практиці багато додатків та операційних систем пропонують детальну модель безпеки, в той час як користувальницький інтерфейс спрощений, щоб забезпечити зручне повсякденне використання. У багатьох випадках IT-пристрої, такі як смартфони, очевидно, прості у використанні, але налаштування функцій безпеки може бути непростим завданням для багатьох людей.

Водночас за останні кілька років кількість загальновживаних додатків та пристроїв значно зросла. Як правило, люди стикаються з більш ніж двома організаційними та особистими пристроями, а кількість застосованих IT-додатків та послуг зростає нелінійним чином. І навпаки, рівень IT-навичок, який зазвичай зустрічається у людей, не суттєво підвищився. У міру того, як концепції, процеси та вимоги до кібербезпеки стають все більш складними та вимогливими, більшість людей більше не володіють необхідними навичками, щоб “слідувати правилам” або розуміти безпосередні наслідки їх моделей використання IT.

В організаційному середовищі придбання нових IT-навичок є тривалим процесом. Для багатьох людей немає часу та бюджету, щоб забезпечити постійний

розвиток з точки зору використання IT та ризику безпеки. Як результат, ризик успішних атак та порушень значно зростає, як і ризик атак соціальної інженерії.

Кібербезпека неминуче покладається на правила, вбудовані в загальну СУІБ. Що стосується людей, то правила безпеки часто сприймаються як незручні та громіздкі.

Навіть там, де всеохоплююча організаційна культура рішуче віддає перевагу вичерпним правилам безпеки, люди часто неохоче сприймають те, що вони вважають непотрібними обмеженнями у своїй щоденній роботі. Правила, які прийняті з неохотою (у кращому випадку), навряд чи будуть інтегровані як необхідна і розумна частина кібербезпеки. Середня

Ефектом управління на основі правил кібербезпеки може бути зречення особистої відповідальності. Суворе дотримання правил може розглядатися як передача відповідальності за порушення безпеки особі або відомству, що видає правила.

Ці природні слабкі сторони з точки зору правил безпеки можуть збільшити ризик атак, спрямованих на суворе середовище, засноване на правилах. Зловмисники, швидше за все, використовують випадки невідповідності або необережного виконання правил, тим самим збільшуючи свій потенціал для успіху.

Більша перспектива ризику невідповідності розширює це. На практиці ненавмисні слабкі місця та прогалини часто виявляються першопричиною нападів, спрямованих на людей у межах підприємства. Більш серйозно, навмисне невиконання часто сприяє поєднаним формам нападів, таким як змова, корупція або навіть повномасштабне проникнення на підприємство.

2.6 Індивідуальний культурний ризик

Кіберзлочинність та кібервійни часто використовують індивідуальні (або особисті) культурні риси, які глибоко закладені в людях. Ці передбачувані фактори можуть визначати режим атаки, вектор атаки та елементи соціальної інженерії, що використовуються для підтримки технічних кроків, що обходять організаційний

захист. Індивідуальна культура тісно пов’язана з особистою відповідальністю (фактичною та сприйманою) у кібербезпеці.

Індивідуальні стилі керівництва від вищого керівництва до керівників команд є вирішальним фактором приписування особистої відповідальності, що підтримується різними політиками та процедурами, які зазвичай існують на підприємствах. З точки зору кібербезпеки, підприємства та люди є найбільш вразливими там, де переважаючий стиль керівництва веде до дисфункціональної поведінки. Детальне керівництво, яке базується на контролі, може надмірно підкреслити особисту відповідальність та дисциплінарні заходи, навіть за незначні помилки чи упущення. Звичайно, люди в цих середовищах, як правило, будуть обережними, іноді до того, що про відомий ризик чи загрози навіть не згадують. На іншому кінці спектра, стиль керування, як правило, недостатньо підкреслює почуття особистої відповідальності, і люди можуть не оцінювати ризик недотримання правил та процедур кібербезпеки. Обидві крайності ілюструють, як індивідуальна культура та стилі керівництва можуть призвести до підвищеного ризику нападу.

З людської точки зору, на підприємства сильно впливає суспільний контекст і ставлення до кіберзлочинів та кібервійни. У багатьох країнах та культурах загальна обізнаність є порівняно низькою, і як політичне, так і суспільне сприйняття ризику та загроз схильні занижувати ризик. Особи, які виховуються та отримують освіту в суспільному контексті з низьким рівнем обізнаності щодо безпеки, можуть бути не в змозі легко прийняти спосіб мислення, призначений підприємством. Як результат, існує високий ризик успішних атак та порушень безпеки, особливо тих, що мають компоненти соціальної інженерії. Це наслідки невідповідності між організаційними і поглядами на суспільну безпеку («Чому я повинен це робити? Ми всі знаємо, що в цій країні немає кіберзлочинності») не слід недооцінювати.

Однією з найважливіших першопричин успішних атак є людські помилки частини людини чи людей, на яких нападають. Хоча існує багато способів боротьби з людською помилкою, кращий підхід, як видається, є саме неправильним. Помилки розпізнаються, приписуються особі, за ними слідують винні та дисциплінарні заходи. Очевидно, що людські помилки, що призводять до нападу, настійно

говорять про те, що все-таки зловмисник винен; однак частіше за все людей на підприємстві звинувачують у тому, що вони «дозволяють щось відбуватися». Як наслідок, люди будуть швидко заперечувати людські помилки та заперечувати чи приховувати будь-які фактичні помилки, що трапляються. На організаційному рівні помилки будуть категорично заперечуватися, щоб уникнути подальшої відповідальності чи збитку для репутації. Для кіберзлочинців або агентств, які займаються кібервійною, це відкриває цікаві можливості. Якщо помилки ні відомі (принаймні всередині підприємства, що перебуває під атакою), не розпізнані та прийняті, повторні атаки все одно можуть бути успішними.

2.7 Ризик, пов'язаний з людськими факторами

Людські фактори є важливим джерелом ризику кібербезпеки, породженого індивідуальним та груповим використанням IT-додатків, процесів та технологій із підтримкою IT. Мабуть, найважливішим фактором ризику є складність18 в організаційних IT. У поєднанні з іншими ризиками (наприклад, відсутність навичок та досвіду, людські помилки) складність збільшує кількість потенційних точок вступу. На практиці складні IT-середовища часто схильні до помилок на людському рівні просто тому, що людям важко використовувати різні процеси та програми.

Іншим важливим фактором ризику в кібербезпеці є зручність як уподобання людини. Сьогодні IT розроблені для “зручності використання” та зручного, безпроблемного використання. Однак багатьом людям все ще важко використовувати механізми безпеки, вбудовані в процеси та програми. Там, де це так, відомі проблеми в інформаційній безпеці неминуче виникають і створюють значне збільшення ризику нападів або порушень. Фактор зручності присутній незалежно від технічних заходів безпеки. Мобільне, подорожнє та домашнє використання IT - порівняно менш добре захищене середовище, в якому зловмисники легко використовують поведінку, керовану зручністю.

Поведінка людини часто формується внаслідок низки суперечливих закономірностей, які можна назвати "розривами". Замість постійного мислення та

дій у галузі кібербезпеки люди приймають суперечливі або контрпродуктивні установки та моделі поведінки. Часто розриви існують на всіх рівнях підприємства, і вони, як правило, досить швидко узагальнюються, якщо їх поширюють вищі рівні управління. Приклади включають:

Особисте заперечення - ризик кіберзлочинів та кібервійни свідомо заперечується через неправильне сприйняття реального ризику або в результаті політичних цілей та завдань.

- Обмежена раціональність - факти та складні схеми ризику спрощуються, щоб дозволити лікування. ("Ми не можемо планувати проти всього, почнемо з очевидного ризику").
- Суперечливі цілі. Сприйняття ризику та апетит до ризику пристосовуються до інших (здавалося б, більш сильних) цілей. ("Ми маємо загальну мету зниження витрат, і це також стосується безпеки").

З цих прикладів очевидно, що розриви як людський фактор є першопричиною багатьох атак та порушень. Неперервні рішення та подальші наслідки у всіх аспектах кібербезпеки часто створюють нові вразливі місця та загрози.

2.8 Ризик непередбачуваних ситуацій

Термін "emergency" описує стихійні або довгострокові зміни в системах управління, які є непередбачуваними та спричиненими низкою, здавалося б, не пов'язаних факторів впливу. Поява проявляється через людей та їх поведінку, а також через процеси та спосіб їх виконання. Як і у випадку зі складністю, сторона процесу може змінюватися внаслідок появи, але переважаючі фактори, що викликають зміни, виявляються у людей, які керують і виконують процеси. Отже, виникнення трактується тут, а не в наступному розділі «Технічний ризик».

Одним із чинників ризику, що найчастіше зустрічаються на практиці, є звична поведінка людей. Як правило, IT-користувачі з часом прийняли велику кількість моделей поведінки, і це відображається на їхніх навичках та діях. Коли з'являються нові IT-процеси або вводяться додатки, ці моделі поведінки змінюються поступово,

поки не досягнуть стадії звичної поведінки. З точки зору кібербезпеки, звички часто використовуються зловмисниками. Приклади включають фішинг на списах, водяні лунки та інші типи атак, що покладаються на передбачувану або звичну реакцію, яку люди, ймовірно, можуть виявити. Інший приклад - сильна (але тепер цілком ірраціональна) звичка використовувати програмне забезпечення для заставки, яка виникла в 1990-х. Здавалося б, привабливе програмне забезпечення заставки використовувалось як вектор зараження шкідливим програмним забезпеченням, і люди застосовували його, незважаючи на те, що сучасні екрани вже давно подолали проблему «вигорання».

Іншим ризиком появи є зміна парадигми у використанні ІТ як з боку технологій, так і з боку людей. Це часто трапляється, коли нові форми використання ІТ з'являються на ринку (нові програми, послуги чи обладнання) або завдяки інноваційному використанню та поведінці на основі існуючих ІТ. Прикладом може бути використання телевізора, що виникає, за допомогою потокового, а не телевізійного мовлення, або використання планшетних комп'ютерів, а не ноутбуків, як основних робочих пристроїв. Хоча нова парадигма виникає швидко, безпека (з точки зору технологій та людей) зазвичай займає більше часу, щоб досягти необхідного рівня захисту. Як результат, нові практики в результаті змін парадигми часто призводять до періоду часу, коли напади та порушення стають набагато частішими.

Загроза кіберзлочинів та кібервійни часто посилюється, як було видно раніше, обмеженнями людини з точки зору навичок, розуміння та здатності адекватно реагувати та реагувати на сприйняті або фактичні загрози. Більшість людей розробляють власні (виникаючі) стратегії боротьби з незручною думкою про відсутність безпеки. Небезпекою такого типу виникнення є неправильне тлумачення та упереджений погляд на світ. На практиці люди часто приймають переконання та гіпотези, які здаються логічними, але межують із забобонними. Приклади включають "вимкнення комп'ютера на ніч зробить його більш захищеним" або "постійне вимкнення бездротової локальної мережі [WLAN], якщо не серфінг, зробить мене більш безпечним". Існує безліч прикладів неправильно

інтерпретованих процесів кібербезпеки, які призводять до хибної оцінки ситуації та подальших нових дій, що зміцнюють початкову віру. Це, очевидно, сприяє конкретним формам нападів, які підривають довіру людей до власних (упереджених) переконань.

2.9 Технічний ризик

APT[35] та інші типи атак часто містять як технічні, так і соціальні елементи. Технічний ризик, який існує в організаційному середовищі, зазвичай розподіляється між багатьма учасниками ланцюжка доданої вартості, а саме підприємством і постачальниками або постачальниками. У сучасних дериметрізованих IT-середовищах може існувати безліч векторів атак та точок входу, які необхідно враховувати в кібербезпеці.

У додатку А наведено огляд загального технічного ризику, заснованого на рівнях абстракції в IT-середовищі. На найвищому рівні (архітектура) вимоги до безпеки в першу чергу стосуються взаємодії IT-середовищ, таких як

внутрішньоорганізаційний, мобільний / подорожній та домашній. Нижні рівні відповідають логіці рівня додатків, рівня операційної системи та рівня інфраструктури.

Оцінка та управління ризиками кібербезпеки повинні включати ці різні технічні рівні з огляду на те, де і як можуть статися напади або порушення. З огляду на минулу історію типових атак, технічний ризик часто зосереджується на відносно невеликій кількості основних причин, тоді як корисне навантаження та наслідки атаки набагато різноманітніші. Як приклад, багато атак спочатку базуються на експлойті з нульовим днем, але їх вплив після успішного отримання контролю над ціллю варіюється від оперативного (наприклад, відмова в обслуговуванні) до соціального (наприклад, шантаж або вимагання). При управлінні кібербезпекою усунення ризиків на технічному рівні має зосереджуватися на першопричинах.

2.10 Ризик, пов'язаний з архітектурою

Сучасні IT-архітектури, як правило, децентралізовані та деперіметрізовані. Сюди входить зростаюча кількість хмарних платформ та послуг, а також зміна обчислювальної потужності та моделей використання до інтелектуальних мобільних пристроїв, таких як планшетні ПК або смартфони. Як наслідок, зросла як кількість потенційних цілей атаки поза межами організації, так і кількість векторів атаки. І навпаки, ступінь контролю над деперіметризованими середовищами значно зменшився, наприклад, на підприємствах, що дозволяють часткову або повну інтеграцію мобільних пристроїв, що належать користувачам (принесіть свій власний пристрій [BYOD]).

У розподілених та децентралізованих IT-архітектурах ризик для сторонніх розробників, ймовірно, зросте, часто як функція переміщення критичних програм, платформ та елементів інфраструктури в хмару. Що стосується платформ, інфраструктури зберігання та сховищ даних, заснованих на хмарі, фокус кібербезпеки переходить до контрактів та угод про рівень обслуговування (SLA). Одночасно сторонні хмарні провайдери стикаються з підвищеним ризиком атак та проломів через агломерацію та кластеризацію конфіденційних даних та інформації. Окрім технічного ризику, що виникає від сторонніх послуг, існує додатковий юридичний ризик. Підприємства, які зазнали втрати конфіденційних даних, можуть не мати можливості подати позов проти винних, оскільки це, можливо, доведеться ініціювати хмарним постачальником.

Незалежно від загальних механізмів захисту інформації, прийнятих підприємством, в IT-архітектурах часто є відкриті області. Ступінь впливу проти кіберзлочинності та кібервійни, за визначенням, високий, оскільки зловмисники націлюються на “слабкі місця” в архітектурних елементах та системах. На відміну від невибіркових та опортуністичних атак, APT та кіберзлочинність завжди покладаються на підготовчі дослідження та розуміння цільового підприємства. Це, в свою чергу, підвищує рівень експозиції для слабких або незахищених частин загальної архітектури. Приклади включають застарілі системи, невідпаковані

частини архітектури (рівень додатків або операційної системи, див. Наступний підрозділ), використання мобільних пристроїв «подвійною персоною» та багато інших.

2.11 Ризик рівня додатків

Впроваджуючи та адаптуючи свої хмарні стратегії, підприємства, як правило, включають пропозиції SaaS[36], іноді поширюючи це на критичні бізнес-процеси та відповідні програми. Незважаючи на те, що ці сервісні пропозиції можуть принести бізнес-переваги, вони тим не менше генерують вразливі місця в потоці даних, які можуть бути використані кіберзлочинністю та кібервійною. Ризик, що виникає, посилюється тим фактом, що багато постачальників та постачальників обладнання (наприклад, для мобільних пристроїв) пропонують хмарні безкоштовні програми, призначені для забезпечення лояльності користувачів. Часто це стосується синхронізації даних, обробки популярних типів файлів, таких як музика або зображення, та особистої інформації, наприклад електронної пошти та записів календаря.

Прикладний рівень в загальному IT-середовищі особливо сприйнятливий до атак нульового дня, про що свідчить багато практичних прикладів. Навіть великі постачальники програмного забезпечення часто оновлюють і виправляють свої програми, але нові вектори атак, що використовують такі програми, з’являються майже щодня. З точки зору кіберзлочинності та кібервійни, ринок атак нульового дня є досить жвавим, і проміжок часу від відкриття до визнання та виправлення зростає.

Подібним чином, поширення складних шкідливих програм зростає протягом останніх кількох років. З точки зору кіберзлочинів та кібервійни, останні зразки шкідливих програм демонструють вищий рівень витонченості та стійкості, ніж більш базові приклади, що використовуються любителями. Хоча постачальники програмного забезпечення швидко вирішують шкідливі програми з точки зору їх розпізнавання та видалення, існує значний залишковий ризик того, що зловмисне

програмне забезпечення стане стійким на цільових підприємствах. Вторинні атаки шкідливого програмного забезпечення - де APT використовують вже встановлене просте шкідливе програмне забезпечення - часто є успішними, коли умови навколишнього середовища сприяють помилкам користувачів або відсутності пильності, а саме в домашніх або подорожуючих сценаріях. На практиці видалення основного шкідливого програмного забезпечення (досить простий процес) часто усуває будь-які подальші підозри та призводить до того, що користувачі та менеджери безпеки переживають помилкове відчуття безпеки. Вторинне (дуже складне) шкідливе програмне забезпечення могло проникнути в систему, представивши відомий і простий шматок первинного шкідливого програмного забезпечення як приманку.

2.12 Ризик, пов’язаний з рівнем операційної системи

Кіберзлочинність та ризик кібервійни навіть вищий на рівні операційної системи, враховуючи, що проникнення на ринок популярних операційних систем набагато вище, ніж для популярних додатків. APT дуже часто націлені на низькорівневі частини операційних систем для досягнення стійкості та меншої видимості. Хоча відповідні зусилля щодо використання вразливостей можуть бути вищими, баланс ризику та винагороди, як правило, є більш привабливим для злочинців.

Основним ризиком у кібербезпеці є той факт, що все більше і більше внутрішніх систем покладаються на застарілі версії операційних систем, особливо там, де підприємства використовують власно розроблені програми. З точки зору бізнесу, вартість адаптації цих додатків є надмірною, і підприємства, як правило, інкапсулюють застарілі області в загальну архітектуру. Однак, оскільки постачальники операційних систем припиняють життєвий цикл для різних версій, виправлення більше не доступне, а цілеспрямовані атаки на застарілі системи стають більш імовірними.

Як і у випадку з додатками, експлуатування операційних систем з загрозою нульового дня є високим ризиком, який може посилитися власними недоліками в розробці самої моделі безпеки операційної системи. Історично склалося, що операційні системи на базі ПК зазнали певного процесу вдосконалення базової моделі безпеки. Однак сучасні мобільні операційні системи часто розробляються під тиском часу виходу на ринок, і існує вищий рівень толерантності до власних концептуальних недоліків та недоліків. Відповідно до принципу нападу на найслабшу ланку ланцюга, APT та менш складні випадки кіберзлочинності, як правило, атакують периферійні операційні системи[37].

2.13 Ризик IT-інфраструктури

На інфраструктурному рівні IT-середовища існують різні точки входу для цілеспрямованих атак та APT. Сама топологія мережі часто влаштована більш традиційним чином, із брандмауерами, демілітаризованими зонами (DMZ) та іншими захисними елементами.

У сценарії різноманітних атак зсередини та зовні підприємства топології мережі можуть бути вразливими, враховуючи те, що не завжди застосовується концепція поглибленого захисту. Однак при аналізі ризиків, пов'язаних з кібербезпекою, часто не помічають саму мережу, включаючи LAN, WAN, WLAN та інколи MAN.

У мережі відомо, що активні компоненти та відповідне програмне забезпечення є значним ризиком атаки. Рівень ризику змінюється залежно від розташування (експозиції) компонента та технічних характеристик. У сценарії APT для домашнього користувача точкою входу зазвичай виявляється маршрутизатор споживчого рівня з функціональністю WLAN, який сприйнятливий до атаки на диск. На відміну від професійного обладнання, яке зазвичай використовується на підприємствах, пристрої споживчого рівня зазнають дуже коротких життєвих циклів, і прошивка може бути більш вразливою. Вторинний ризик, особливо в домашніх умовах, проявляється в поведінковому контексті використання

постачальників пристроїв. Користувачі рідко володіють необхідними навичками та знаннями, щоб посилити заводську конфігурацію, 19 залишаючи значні прогалини в безпеці.20

Апаратний ризик може здатися дещо віддаленим, але існує у дивовижній кількості випадків. Приклади включають тип проникнення "безкоштовного подарунка" за допомогою портативних пристроїв (універсальна пам'ять послідовної шини [USB], миші, привабливі "гаджети"), а також цільове втручання в апаратне забезпечення у чутливих областях IT-середовища. Найчастіше при реєстрації та моніторингу ігноруються цілі пристрої або незначні зміни конфігурації апаратного забезпечення. Як правило, апаратний ризик[38] розглядається як занадто віддалений, щоб його можна було включити до стандартизованого управління інформаційною безпекою, незважаючи на те, що АПТ з організованою злочинністю чи фоном кібервійни використовують апаратні маніпуляції як бажаний (менш впізнаваний) вектор атаки.

Висновки за розділом 2

Цілком очевидно, що процес оцінки ризиків для підприємства є обов’язковою дією, так само як і виявлення вразливостей і прогалин в безпеці. У розділі 2 було перечислено загальний список вразливостей і загроз, від яких не застраховане жодне підприємство:

- Направлений фішинг
- Water holing
- Wireless/mobile APT
- Zero-day
- Надмірні привілеї
- Соціальна інженерія
- Home user APT
- Extended IT infrastructure APT
- Non-IT technical infrastructure APT

- Vendor/business partner exploit

На підставі множини даних вразливостей було сформовано і проаналізовано ризики для ІБ організації.

РОЗДІЛ 3
РОЗРОБКА МОДЕЛІ ОЦІНКИ ЗАХИЩЕНОСТІ

3.1 Аналіз процесів COBIT 5

У розділі проведено аналіз процесів стандарту з точки зору ІБ і кібербезпеки. Результати приведені у таблицях по доменам процесів.

Процеси стандарту розібрані по їх функціям(activities) з урахуванням значення для інформаційної безпеки і кібербезпеки організації, відповідно до книги з описом процесів від ICASA[39].

Домен «Координація, планування та організація» (Align, Plan & Organise - APO):

Таблиця 3.1.1 Аналіз процесів APO01, APO02

Процес COBIT 5	**Результат для ІБ**	**Значення для кібербезпеки**
APO01.02 Establish roles and responsibilities.	Визначення ролей та обов'язків, пов'язаних з IT.	Визначте організацію кібербезпеки, узгоджуючи ролі та обов'язки із загальною інформаційною безпекою
APO01.03 Maintain the enablers of the management system.	Інформаційна безпека та відповідні політики	Забезпечити політику кібербезпеки (управління) та допоміжні стандарти, узгоджені та інтегровані із загальним набором інформаційної безпеки та відповідними політиками
APO01.04 Communicate management objectives and direction.	Навчальна та інформаційна програма з питань інформаційної безпеки	Розробити програму підготовки та підвищення обізнаності з питань кібербезпеки, включаючи елементи, засновані на оцінці ризику.
APO01.06 Define information (data) and system ownership.	Ролі та обов'язки щодо інформаційної безпеки	Визначте ролі та обов'язки кібербезпеки як частину загальної моделі RACI.
	Вказівки щодо класифікації даних	Надайте вказівки, пов’язані з кібербезпекою, щодо того, що означає „конфіденційна” та „особиста” інформація, зокрема щодо нападів та порушень.

Продовження табл.3.1.1

APO01.07 Manage continual improvement of processes.	Документування процесів, технологій та програм, а також стандартизація	Надайте план та перспективу щодо вдосконалення управління кібербезпекою, включаючи нові стандарти та вимоги дотримання.
	Навчання персоналу інформаційної безпеки	Проводити навчання з кібербезпеки відповідно до програми підвищення обізнаності та навчання та пропонувати спеціальні навчальні шляхи для фахівців з кібербезпеки
APO01.08 Maintain compliance with policies and procedures.	Оцінка відповідності інформаційній безпеці	Визначте та проведіть перевірки відповідності, пов'язані з кібербезпекою, у загальному графіку оцінок.
APO02.02 Assess the current environment, capabilities and performance.	Можливості інформаційної безпеки	Розробити базовий рівень можливостей для кібербезпеки, включаючи критерії та показники ефективності.
APO02.03 Define the target IT capabilities.	Вимоги до інформаційної безпеки в цільових IT-можливостях	Визначте цільові стани, як частину загальної трансформації, для кібербезпека через регулярні проміжки часу (наприклад, щорічно) та як функція фактичних атак та порушень.
APO02.04 Conduct a gap analysis.	Орієнтир можливостей інформаційної безпеки	Проводити регулярні (наприклад, щоквартально) еталони з кібербезпеки
	Прогалини, які слід усунути, та зміни, необхідні для реалізації цільової спроможності.	Усунути прогалини шляхом офіційного процесу управління змінами в кібербезпеці.
APO02.05 Define the strategic plan and road map.	Стратегія інформаційної безпеки	Визначте та включіть цілі та завдання з кібербезпеки на стратегічному рівні та включіть їх до стратегії безпеки.
	Стратегічна дорожня карта інформаційної безпеки	Надайте та включіть етапи та дати завершення цілей та завдань з кібербезпеки.

Таблиця 3.1.2 Аналіз процесів APO03-APO05

Процес COBIT 5	**Результат для ІБ**	**Значення для кібербезпеки**
APO03.03 Select opportunities and solutions.	Впровадження архітектури інформаційної безпеки та стратегія міграції	Перевірити будь-який архітектурний ризик, що випливає з проблеми, пов'язаної з кібербезпекою, включаючи міграцію.
APO04.01 Create an environment conducive to innovation.	Інноваційний план інформаційної безпеки .	Включити інновації з управління кібербезпекою як частину загальних інновацій в галузі інформаційної безпеки
APO04.02 Maintain an understanding of the enterprise environment.	Оцінка впливу на інформаційну безпеку нових ініціатив	Оцініть потенційні вразливі місця, загрози та пов'язаний з ними ризик нових ініціатив.
APO04.03 Monitor and scan the technology environment.	Визначено нові тенденції в галузі інформаційної безпеки	Дослідження та виявлення нових тенденцій у сфері кіберзлочинності, кібервійни та пов'язані із цим заходи безпеки.
APO04.04 Assess the potential of emerging technologies and innovation ideas.	Оцінка відповідності вимогам інформаційної безпеки	Перевірити потенційний вплив кібербезпеки нових технологій та інновацій, а також включити відомі ризики та проблеми.
APO04.05 Recommend appropriate further initiatives.	Поради щодо інформаційної безпеки щодо результатів випробувань на основі підтвердження концепції	Надавати поради, засновані на оцінці ризику, щодо можливих нападів або порушень та необхідні заходи та заходи з кібербезпеки.
APO05.01 Establish the target investment mix.	Цільова інвестиційна суміш інформаційної безпеки	Визначити відповідні інвестиції в управління кібербезпекою в системному контексті.
APO05.02 Determine the availability and sources of funds.	Варіанти фінансуваня	Забезпечити відповідне фінансуваня кібербезпеки; отримати необхідне прийняття ризику там, де фінансуваня недостатнє.
APO05.06 Manage benefits achievement.	Оновлений профіль ризику інформаційної безпеки	Перевірити та оновити профіль ризику кібербезпеки на основі даних про атаки / порушення / події та реагування на них.

Таблиця 3.1.3 Аналіз процесів APO06, APO07, APO09

Процес COBIT 5	**Результат для ІБ**	**Значення для кібербезпеки**
APO06.02 Prioritise resource allocation.	Пріоритетність ініціативи	Пріоритетні ініціативи з кібербезпеки та необхідні ресурси в системному контексті.
APO06.03 Create and maintain budgets.	Бюджет інформаційної безпеки	Підготувати та підтримувати бюджет кібербезпеки
APO07.01 Maintain adequate and appropriate staffing.	Вимоги інформаційної безпеки до кадрового процесу	Визначити вимоги до кадрового забезпечення кібербезпеки.
APO07.03 Maintain the skills and competencies of personnel.	План навчання з інформаційної безпеки	Визначити план навчання з кібербезпеки
	Тренінг з підвищення обізнаності щодо інформаційної безпеки	Розробити програму підвищення обізнаності щодо кібербезпеки
APO09.02 Catalogue IT services.	Каталог послуг інформаційної безпеки	Додати до каталогу послуги, пов’язані з кібербезпекою.
APO09.03 Define and prepare service agreements.	SLA	Оцінити рівень послуг постачальників за критеріями та вимогами в галузі кібербезпеки.
APO09.04 Monitor and report service levels.	OLA	Визначити рівні експлуатації послуг, пов’язаних з кібербезпекою
	Звіти про ефективність роботи служби захисту інформації	Підготувати (постачальника) звіти про ефективність кібербезпеки.
APO09.05 Review service agreements and contracts.	Оновлені SLA	За необхідності перегляньте положення контрактів, пов’язані з кібербезпекою, та за потреби оновлюйте SLA

Таблиця 3.1.4 Аналіз процесів APO10, APO12

Процес COBIT 5	**Результат для ІБ**	**Значення для кібербезпеки**
APO10.04 Manage supplier risk.	Оновлений рейтинг ризику постачальника	Оновити рейтинг ризику для всіх постачальників, на яких поширюються вимоги щодо кібербезпеки.
APO10.05 Monitor supplier performance and compliance.	Результати огляду моніторингу відповідності постачальників	Оцінити та переглянути постачальників на відповідність кібербезпеці та ефективність
APO12.01 Collect data.	Дані про ризик інформаційної безпеки	Збирати дані про ризик, пов'язаний з кібербезпекою, нападами, порушеннями та інцидентами; включати зовнішні дані та статистику, якщо це доречно.
APO12.02 Analyse risk.	Результати аналізу ризиків інформаційної безпеки	Проаналізуйте ризик кібербезпеки
	Сценарії ризику інформаційної безпеки	Визначте та підтримуйте сценарії ризику, пов’язані з кібербезпекою

Домен BAI - Створення, придбання та впровадження(Build, Acquire & Implement):

Таблиця 3.1.5 Аналіз процесів BAI01- BAI03

Процес COBIT 5	**Результат для ІБ**	**Значення для кібербезпеки**
BAI01.02 Initiate a programme.	Концепція програми бізнес-кейс, включаючи обов’язкові заходи щодо захисту інформації	Визначте бізнес-кейси та програму кібербезпеки на основі передбачених санкцій заходів безпеки та найважливіших пріоритетів бізнесу.
BAI01.08 Plan projects.	План проекту, що включає цілі, завдання та вимоги щодо інформаційної безпеки	Плануйте проекти, пов’язані з кібербезпекою, відповідно до програми.

Продовження табл.3.1.5

BAI01.11 Monitor and control projects.	Звіт про оцінку проекту інформаційної безпеки, який визначає слабкі сторони контролю та рекомендовані плани коригувальних дій	Надайте звітність проектів щодо проектів з кібербезпеки з конкретним посиланням на слабкі місця, що виникають внаслідок нових форм кіберзлочинності та кібервійни.
BAI02.01 Define and maintain business functional and technical requirements.	Вимоги до інформаційної безпеки	Визначте вимоги до кібербезпеки як підмножину загальних вимог до інформаційної безпеки.
BAI02.03 Manage requirements risk.	Дії щодо зменшення ризику	Визначте та задокументуйте ризик, пов'язаний із рішеннями, включаючи залишковий ризик після пом'якшення наслідків та потенційний вплив нападів і порушень
BAI03.01 Design high-level solutions.	Специфікації інформаційної безпеки відповідають високому рівню дизайну	Розробити специфікації кібербезпеки високого рівня відповідно до моделі безпеки та динаміки системи
BAI03.02 Design detailed solution components.	Проектування інформаційної безпеки в компонентах рішення	Розробити детальні кроки, дії та заходи з протидії ризику та впровадити їх у систему кібербезпеки
BAI03.10 Maintain solutions.	Оновлені рішення безпеки	Оновлення рішень з питань кібербезпеки відповідно до потреб бізнесу та експлуатаційних вимог.

Таблиця 3.1.6 Аналіз процесів BAI04, BAI05

Процес COBIT 5	**Результат для ІБ**	**Значення для кібербезпеки**
BAI04.01 Assess current availability, performance and capacity and create a baseline.	Перелік технічних та процедурних питань захисту інформації, пов'язаних з доступністю, продуктивністю та можливостями	Визначте та включіть будь-які проблеми, пов'язані з кібербезпекою, зокрема атаки та порушення, пов'язані з доступністю, продуктивністю та можливостями

Продовження табл.3.1.6

BAI04.02 Assess business impact.	Оцінка впливу на доступність, ефективність та потужність інформаційної безпеки	Проводити оцінки впливу на IT та бізнес-процеси, які потенційно можуть зазнати атак та порушень; узгодити з BCM та іншими оцінками впливу.
BAI05.01 Establish the desire to change.	План спілкування з вищим керівництвом	Визначати та планувати комунікації щодо кібербезпеки та пов'язані з ними кроки та заходи; створити обізнаність вищого керівництва та заручитися підтримкою кібербезпеки; включати культурний вимір
BAI05.04 Empower role players and identify short-term wins.	Список потенційних короткострокових виграшів	Пріоритетні плани та проекти з кібербезпеки визначте за часом і визначити короткотермінові цілі та переваги, тобто негайні дії щодо зменшення кількості атак та порушень (якщо такі є).
BAI05.05 Enable operation and use.	Практичні заходи інформаційної безпеки	Планувати та реалізовувати дії з огляду на майбутній стан як частину трансформації кібербезпеки; чітко виділити трансформаційний аспект.
BAI05.07 Sustain changes.	Огляди експлуатаційного використання	Інтегруйте оперативні огляди з моніторингом та контролем кібербезпеки.

Таблиця 3.1.7 Аналіз процесу BAI06

Процес COBIT 5	**Результат для ІБ**	**Значення для кібербезпеки**
BAI06.02 Manage emergency changes.	Огляд інформаційної безпеки після впровадження надзвичайних змін	Переглянути та консолідувати будь-які надзвичайні зміни, пов’язані з кібербезпекою, наприклад, під час захисту від атак або виконання слідчої діяльності; включити будь-які серйозні зміни, такі як вимкнення систем тощо.
BAI06.04 Close and document the changes.		Документувати(підлягає аудиту та виявленню) будь-які зміни, що мають відношення до кібербезпеки, включаючи ділові зміни.

Домен DSS - Доставка, обслуговування та підтримка(Deliver, Service and Support):

Таблиця 3.1.8 Аналіз процесів DSS01, DSS02

Процес COBIT 5	Результат для ІБ	Значення для кібербезпеки
DSS01.05 Manage facilities.	Оновлені звіти про оцінку об'єктів	Визначити та внести ризики та вразливості / загрози, пов’язані з об’єктами, зокрема для технічної інфраструктури, яка може бути ціллю.
DSS01.02 Manage outsourced IT services.	Плани забезпечення сторонніх гарантій	Включити вимоги до кібербезпеки до сторонніх рівнів обслуговування та контрактів; включити вимоги до кібербезпеки та тестування в сторонні плани забезпечення.
DSS01.03 Monitor IT infrastructure.	Оновлені правила моніторингу активів	Розширити правила моніторингу, щоб охопити всі вимоги щодо кібербезпеки; зокрема включати моніторинг потенційних або фактичних атак та порушень.
DSS01.04 Manage the environment.	Оновлена політика оточення	Надайте інформацію про спеціалізовані служби, обладнання та пристрої для моніторингу та контролю оточення.
DSS02.02 Record, classify and prioritise requests and incidents.	Класифіковані та пріоритетні інциденти інформаційної безпеки та запити на послуги	Розробити критерії класифікації, пов’язані з кібербезпекою, та узгодити загальний облік та класифікацію інцидентів; надати поточні дані про інциденти, що стосуються кібербезпеки.
DSS02.04 Investigate, diagnose and allocate incidents.	Процедура збору доказів	Виявити інциденти, що стосуються кібербезпеки, захищати дані та всі потенційні докази; дотримуватись правил зберігання та електронного виявлення; включіть докази BC / DR відповідно.
DSS02.05 Resolve and recover from incidents.	План реагування на аварії	Розробити відповіді щодо кібербезпеки відповідно до підготовки, розслідування, усунення та викорінення основних причин.
DSS02.07 Track status and produce reports.	Отриманий досвід	Консолідувати дані та докази подій; отримувати уроки навчився для кібербезпеки; визначити необхідні вдосконалення та потреби у трансформації.

Таблиця 3.1.9 Аналіз процесів DSS03, DSS04

Процес COBIT 5	**Результат для ІБ**	**Значення для кібербезпеки**
DSS03.02 Investigate and diagnose problems.	Оновлена основна причина проблем	Розслідувати та діагностувати напади, порушення та інциденти; включати близькі промахи та невдалі спроби (за наявності); встановити першопричину, якщо це можливо, та отримати загальні характеристики.
DSS03.03 Raise known errors.	Оновлені записи відомих помилок	Піднімати відомі проблеми в галузі кібербезпеки; зокрема включити системні слабкі місця.
DSS04.01 Define the business continuity policy, objectives and scope.	Оновлена політика щодо безперервності бізнесу	Вставити відповідне посилання на політику та процедури кібербезпеки; включити відповідні сценарії кіберзлочинів / кібервійни у політику ВС.
DSS04.02 Maintain a continuity strategy.	Оновлено BIA	Інтегрувати стратегію та тактику кібербезпеки для боротьби з нападами / порушеннями та ескалації інцидентів; оновити BIA та оцінку ризиків щодо вразливостей / загроз кібербезпеки та пов'язаних з ними ризиків.
DSS04.03 Develop and implement a business continuity response.	Оновлено BCP	Розробити та вирівняти BCP для сценаріїв, пов’язаних з кібербезпекою.
DSS04.04 Exercise, test and review the BCP.41		Перевірте пункти пропуску, пов'язані з кібербезпекою, та випадкові домовленості
DSS04.05 Review, maintain and improve the continuity plan.	Оновлено BCP	Включити пункти пропуску, пов'язані з кібербезпекою, та випадкові домовленості у циклі PDCA.

Таблиця 3.1.10 Аналіз процесу DSS05

Процес COBIT 5	**Результат для ІБ**	**Значення для кібербезпеки**
DSS05.01 Protect against malware.	Політика запобігання зловмисному програмному забезпеченню	Узгодити політику, стандарти та норми кібербезпеки з загальною політикою інформаційної безпеки та навпаки.
	Оцінка потенційних загроз	Оцініть конкретні загрози, такі як експлойти нульового дня, шкідливе програмне забезпечення військового класу та засоби атаки APT.

Продовження табл.3.1.10

DSS05.02 Manage network and connectivity security.	Політика безпеки підключення	Виявляти та вставляти мережеві компоненти, схильні до атак / порушень, зокрема експлойти нульового дня та типу APT
	Результати тестів на проникнення	Проведіть відповідне тестування на проникнення на схильних до атак мережеві компоненти; обмежитися відповідним технічним рівнем, щоб розрізнити загальну перспективу інформаційної безпеки та кібербезпеки.
DSS05.03 Manage endpoint security.43	Політики безпеки для пристроїв кінцевих точок	Включати атаки / порушення на кінцеві точки та відомі атаки APT.
DSS05.07 Monitor the infrastructure for security-related events.	Тікети на інцидент безпеки	Оцінити події на наявність ознак кіберзлочинності або кібервійни; ескалація відповідно.
	Характеристики інцидентів безпеки	Оцініть, чи інциденти мають відношення до кібербезпеки, або чи інциденти можуть бути розглянуті за допомогою загальних процедур та дій щодо захисту інформації
	Журнали подій безпеки	Встановити механізми аналізу та огляду журналів, пов'язаних з кібербезпекою.

Домен MEA - Моніторинг, вимірювання та оцінка(Monitor, Evaluate and Assess):

Таблиця 3.1.11 Аналіз процесів домену MEA

Процес COBIT 5	**Результат для ІБ**	**Значення для кібербезпеки**
MEA01.03 Collect and process performance and conformance data.	Оброблені дані моніторингу	Визначити вимоги до моніторингу, показники, набори даних та методи збору для моніторингу кібербезпеки; визначити відповідні аналітичні методи (DSS05.07).
MEA01.05 Ensure the implementation of corrective actions.	Процес відстеження коригувальних дій з питань інформаційної безпеки	Визначте коригувальні дії, що стосуються напади / порушення / інциденти; вбудовувати будь-які коригувальні дії та пов'язане з ними планування в загальна трансформація кібербезпеки

Продовження табл.3.1.11

MEA02.04 Identify and report control deficiencies.	Результати оцінки та коригувальні дії	Визначте слабкі місця в кібербезпеці з точки зору ризику та висвітліть будь-які каскадні ефекти в динаміці системи.
MEA02.05 Ensure that assurance providers are independent and qualified.	Компетентність у навичках та знаннях	Оцінити постачальників гарантій кібербезпеки; зібрати відповідний інтелект; виконувати попередні перевірки за необхідністю
MEA03.01 Identify external compliance requirements.	Вимоги щодо дотримання зовнішньої інформаційної безпеки	Визначити будь-які закони чи нормативні акти, що впливають на кібербезпеку; включати конкретні положення, передбачені прерогативою національної безпеки (або еквівалентом); включати будь-які вимоги, що стосуються кібервійни.

3.2 Розробка моделі оцінки захищеності інформаційної системи

Проаналізувавши процеси у минулій частині розділу я сформувала наступну схему, на основі якої можна створити файл у Excel чи написати програму, за допомогою якої можна провести оцінку стану захищеності системи(див. Рис.3.2.1). На зображені видно, що ми використовуємо вимоги стандартів ISO/IEC 27001 та ITIL, формуємо на їх основі питання для персоналу з ІТ відділу та інших відділів і пов’язуємо це з процесом COBIT 5. Можна розбити питання і процеси по доменам ІБ на основі ISO/IEC 27001 для оцінки по категоріям.

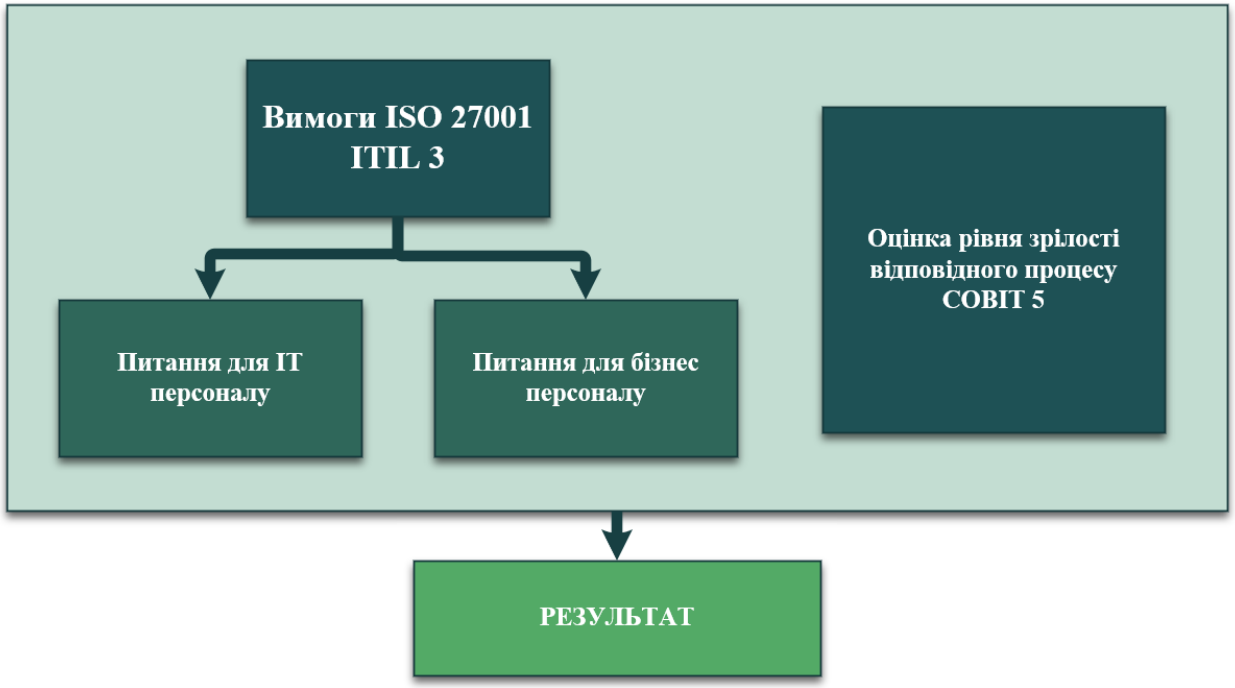

Рисунок 3.2.1 Схема оцінки захищеності інформаційної системи

Виходячи з вимог стандартів формуються питання для персоналу IT відділу і для персоналу інших відділів, зв'язно з питаннями проводиться оцінка зрілості пов'язаного з ними процесу. Окрім прямої відповіді на питання персонал має надати деталі, які будуть прийняті до уваги при прийнятті рішення щодо результату оцінки.

Приклад реалізації такої моделі можна побачити у Додатку Б.

Висновки за розділом 3

У результаті роботи , де по деталям було розібрано процеси COBIT 5 для аналізу їх зрілості з точки зору ІБ, визначено:

- буквально кожний процес має вплив на ІБ організації;
- виходячи з проведеного аналізу, найбільш вагомими для захищеності ІС будуть саме процеси доменів APO, BAI та DSS;
- у останнього домену майже всі процеси напряму пов'язані з забезпеченням ІБ, неперервності бізнесу та цілком функціональності ІС.

За рахунок поєднання стандартів закриваються діри у безпеці як з технічної точки зору, так і з організаційної – тут найбільша заслуга стандарту COBIT 5, який ліквідує прогалину між керівництвом організації і управлінням IT.

ВИСНОВКИ

У дипломній роботі було проаналізовано відомі міжнародні стандарти у сфері інформаційних технологій та інформаційної безпеки, досліджено найпоширеніші вразливості, проаналізовано ризики ІБ інформаційної системи, їх мовірність і складність реалізації.

На основі досліджень було сформовано схему у редакторі Visio, на основі якої відбувається оцінка захищеності. Для досягнення поставленої мети роботи було використано метод аналізу відповідності рівня захищеності критеріям стандартів COBIT 5, ISO 27001, ITIL.

За результатами проведення роботи було сформовано список вразливостей, загроз та ризиків, на підставі яких було сформовано вимоги до ІС.

Практичне значення роботи полягає у формуванні рекомендацій щодо методології оцінки рівня захищеності інформаційної системи, які можуть бути успішно впроваджені за рахунок подібних сумісних стандартів. Також на практичному прикладі було продемонстровано варіант реалізації оцінки захищеносі інформаційної системи через контрольний список в Excel. Даний список може використовуватися в подальшому як засіб для самоаудиту організації.

Мету роботи досягнуто, поставлені задачі виконано.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 2382:2015 Information technology — Vocabulary [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/63598.html

2. COBIT | Control Objectives for Information Technologies | ISACA [Електронний ресурс]. – Режим доступу: https://www.isaca.org/resources/cobit

3. ISACA: Advancing IT, Audit, Governance, Risk, Privacy [Електронний ресурс]. – Режим доступу: https://www.isaca.org

4. COBIT [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/COBIT

5. COBIT 5 framework for the governance of enterprise IT [Електронний ресурс]. – Режим доступу: https://www.itgovernance.co.uk/cobit

6. COBIT - Факторы влияния COBIT 5 [Електронний ресурс]. – Режим доступу: https://cobit.ucoz.ru/index/faktory_vlijanija_cobit_5/0-21

7. ITIL [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/ITIL

8. What is ITIL V3? | ITIL Framework [Електронний ресурс]. – Режим доступу: https://freshservice.com/itil/itil-v3

9. ITIL v3 (Information Technology Infrastructure Library)/Service Strategy [Електронний ресурс]. – Режим доступу: https://en.wikibooks.org/wiki/ITIL_v3_(Information_Technology_Infrastructure_Library)/Service_Strategy#:~:text=Service%20Strategy%20is%20the%20center,develop%20over%20the%20long%20term.

10. ITIL v3 (Information Technology Infrastructure Library)/Service Design [Електронний ресурс]. – Режим доступу: https://en.wikibooks.org/wiki/ITIL_v3_(Information_Technology_Infrastructure_Library)/Service_Design

11. ITIL v3 (Information Technology Infrastructure Library)/Service Transition [Електронний ресурс]. – Режим доступу:

https://en.wikibooks.org/wiki/ITIL_v3_(Information_Technology_Infrastructure_Library)/Service_Transition

12. ITIL v3 (Information Technology Infrastructure Library)/Service Operation [Електронний ресурс]. – Режим доступу: https://en.wikibooks.org/wiki/ITIL_v3_(Information_Technology_Infrastructure_Library)/Service_Operation

13. ITIL v3 (Information Technology Infrastructure Library)/ Continual Service Improvement [Електронний ресурс]. – Режим доступу: https://en.wikibooks.org/wiki/ITIL_v3_(Information_Technology_Infrastructure_Library)/Continual_Service_Improvement

14. ISO/IEC 27001 [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/ISO/IEC_27001

15. What is ISO/IEC 27001? | Implement, Certify & Comply [Електронний ресурс]. – Режим доступу: https://www.itgovernance.co.uk/iso27001

16. A Model for Assessing COBIT 5 and ISO 27001 Simultaneously [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/326507013_A_Model_for_Assessing_COBIT_5_and_ISO_27001_Simultaneously

17. ISO/IEC 27002 [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/ISO/IEC_27002

18. ISO/IEC 27002 code of practice [Електронний ресурс]. – Режим доступу: https://www.iso27001security.com/html/27002.html

19. Стандарты ITIL, MOF, ITSM, COBIT [Електронний ресурс]. – Режим доступу: https://koptelov.info/publikatsii/standarty-itil-mof-itsm-cobit/

20. COBIT vs. ITIL: The Ultimate IT Governance Framework Comparison [Електронний ресурс]. – Режим доступу: https://www.simplilearn.com/cobit-vs-itil-article#:~:text=What%20are%20the%20Differences%20Between,how%20to%20carry%20them%20out.

21. Компьютерные атаки и технологии их обнаружения [Електронний ресурс]. – Режим доступу: https://protect.htmlweb.ru/attack.htm

22. Как хакеры выбирают свои цели? [Електронний ресурс]. – Режим доступу: https://www.securitylab.ru/blog/company/PandaSecurityRus/346768.php

23. О.С. Макарова, С.В. Поршнев ОЦЕНИВАНИЕ ВЕРОЯТНОСТЕЙ КОМПЬЮТЕРНЫХ АТАК [Електронний ресурс]. – Режим доступу: https://bit.mephi.ru/index.php/bit/article/view/1273

24. Направленный фишинг – современная угроза безопасности [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/280200/

25. Watering hole attack [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Watering_hole_attack

26. What Is an Advanced Persistent Threat (APT) [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html

27. Zero-day (computing) [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Zero-day_(computing)

28. ДЕСЯТКА КРУПНЕЙШИХ УГРОЗ БЕЗОПАСНОСТИ БАЗ ДАННЫХ И БОРЬБА С НИМИ [Електронний ресурс]. – Режим доступу: https://www.dataarmor.ru/десятка-крупнейших-угроз-безопаснос/

29. Соціальна інженерія (безпека) [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Соціальна_інженерія_(безпека)

30. APT Security: What You Need to Know about Advanced Persistent Threats [Електронний ресурс]. – Режим доступу: https://heimdalsecurity.com/blog/apt-security/

31. advanced persistent threat (APT) [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/glossary/term/advanced_persistent_threat

32. advanced persistent threat (APT) [Електронний ресурс]. – Режим доступу: https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

33. What a business partner's breach could mean to your practice [Електронний ресурс]. – Режим доступу: https://www.medicaleconomics.com/view/what-business-partners-breach-could-mean-your-practice

34. Класифікація ризиків [Електронний ресурс]. – Режим доступу: https://pidru4niki.com/16650214/menedzhment/klasifikatsiya_rizikiv

35. Anatomy of Advanced Persistent Threats [Електронний ресурс]. – Режим доступу: https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html

36. Risks You Need to Consider When Using SaaS Providers [Електронний ресурс]. – Режим доступу: https://securityboulevard.com/2020/12/risks-you-need-to-consider-when-using-saas-providers/

37. 5 Risks Of Outdated Software & Operating Systems [Електронний ресурс]. – Режим доступу: https://www.bitsight.com/blog/outdated-software-issues ISO/IEC 27001 [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/ISO/IEC_27001

38. АНАЛИЗ И УПРАВЛЕНИЕ РИСКАМИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ [Електронний ресурс]. – Режим доступу:https://studme.org/179791/informatika/analiz_upravlenie_riskami_sfere_informat sionnoy_bezopasnosti

39. COBIT® 5: Enabling Processes [Електронний ресурс]. – Режим доступу: https://community.mis.temple.edu/mis5203sec001sp2019/files/2019/01/COBIT5-Ver2-enabling.pdf

40. BS 7799: 1995 – Code of Practice for Information Security Management.

41. ISO/IEC 17799:2001 – Information technology. – Information Security Management – Code of Practice for Information Security Management

42. ISO 7498-2:1989 – Information technology – Open Systems Interconnection – Basic reference model – Part 2: Security architecture.

ДОДАТОК А

ТЕХНІЧНІ РИЗИКИ

Ризик	Опис	Потенційні наслідки
Архітектура — деперіметризація	Деріметрізуються значні частини IT-архітектури.	Децентралізовані, мобільні та домашні середовища є більш вразливими та менш підданими організаційному контролю.
Архітектура - третя сторона	Частинами IT-архітектури керують треті сторони (Платформа як послуга (PaaS), Інфраструктура як послуга (IaaS))	Кібербезпека переходить на контрактну основу (лише непрямий контроль), що потенційно збільшує ризик нападів і порушень.
Архітектура - відкриті ділянки	Частини загальної архітектури мають високий ризик / схильність до атак та порушень.	Атаки фокусуються на відкритих ділянках (наприклад, застарілі, непрацюючі, подвійне використання персоналу)
Прикладний рівень - хмара / програмне забезпеченя як послуга(SaaS)	Важливі програми працюють у хмарі та / або підписуються як SaaS.	Високий ризик вразливості сторони постачальника та пов'язаних з ними атак (Інфраструктура- мережі)
Рівень застосування - нульовий день	Для критично важливих програм існують експлойти нульового дня	Високий ризик цілеспрямованих атак з використанням точок входу нульового дня
Рівень програми - шкідливе програмне забезпеченя	Додатки змінюються або пошкоджуються різними типами шкідливих програм.	Високий ризик тимчасових або постійних векторів відкритих атак та пов'язаних з ними наслідків
Рівень операційної системи - застарілість	Для певних програм потрібні застарілі версії операційних систем.	Високий ризик уразливостей, що виникають внаслідок закінчення терміну підтримки / відсутності виправлень для застарілих операційних систем, які часто надають перевагу як вектор атаки

Продовження табл.

Рівень операційної системи - нульовий день	Експлойти нульового дня для операційних систем	Високий ризик атак з використанням точок входу нульового дня
Рівень операційної системи — модель безпеки	Модель безпеки операційної системи неадекватна для кібербезпеки	Прогалини або слабкі місця в моделі безпеки перешкоджають безпечній конфігурації, високий ризик використання відомих слабких місць
Інфраструктура— мережі	Слабкі сторони та структурні вразливості топології (глобальна мережа [WAN] / локальна мережа / мережа столичних районів [MAN]	Частини комбінованої топології мережі сприйнятливі до атак та порушень; див. також компоненти та мікропрограму.
Інфраструктура - компоненти та прошивка	Мережеві компоненти та прошивка містять уразливості, виправлення може бути рідкісним, використання застарілих компонентів	Високий ризик атак на основі відомих слабких сторін мікропрограмного забезпечення компонентів, часто побічно
Інфраструктура - апаратне забезпечення	Модифікація обладнання (включаючи постачальника)	Ризик атак на основі заміненого або модифікованого обладнання, включаючи кібервійну
Технічна інфраструктура - вбудовані системи	Уразливості у вбудованих системах, модифікації апаратного чи програмного забезпечення	Високий ризик атак на основі відомих слабких місць у вбудованих системах; модифіковані вбудовані компоненти можуть використовуватися в кібервійні
Технічна інфраструктура - системи управління	Уразливості в системах управління та управління (наприклад, SCADA)	Високий ризик нападів на основі відомих слабких місць у контролі та системи управління; АПТ можуть використовуватися в кібервійні

ДОДАТОК Б

ПРИКЛАД РЕАЛІЗАЦІЇ СХЕМИ У EXCEL ФАЙЛІ

Питання	Питання (Control Objective) для бізнес персоналу	Питання	Питання (Control Objective) для IT персоналу	Відповідь	Опишіть існуючі ключові засоби контролю безпеки що стосуються запитання	Опишіть основні слабкі місця щодо цього питання	Опишіть будь-які поточні дії щодо цього питання	Поточний рівень зрілості процесу(читати Рівні) 0 - 5	Домен безпеки
1	Чи знаєте Ви та члени вашого підрозділу про політику інформаційної безпеки чи проводили для вас будь-який тренінг з підвищення обізнаності політики співробітн?	1	Чи була розроблена структура політики інформаційної безпеки, включаючи відповідальність за розробку, перегляд та затвердження політик?	Немає відповіді				1	I. Політика безпеки
2	Чи підтримується та застосовується керівництвом вашого департаменту надана політика?	2	Чи була впроваджена база політики, що призвело до створення політики інформаційної безпеки, яка підтримується на найвищих рів-нях організації?	Немає відповіді				5	I. Політика безпеки
3	Чи існує процес перевірок відповідності працівників політиці?	3	Чи внутрішній персонал регулярно контролює безпеки для виявлювання результативності та адекватності?	Ні				3	I. Політика безпеки
		3.1	Якщо ви відповіли стверд-но на запитання 3, чи використовується ефективність на основі політики безпеки?	Так				0	I. Політика безпеки
4	Чи вимагали коли-небудь ваш відділ або працівники зробити виняток із пунктів політики?	4	Чи існує поточний процес визначення та постійного перегляду винятків із політик?	Немає відповіді				1	I. Політика безпеки
4.1	Чи знайомі ви з процесом прийняття рішень?	4.1	Чи знайомі ви з процесом прийняття рішень?	Частково					I. Політика безпеки
5	Чи існують політики та процедури щодо обробки паперових копій документів?								I. Політика безпеки
6	Чи знайомі ви з політикою використання електронної пошти та інтернету?								I. Політика безпеки
7	Чи співпрацює ваш відділ з IT-відділом для стратегічного планування?	5	Чи виконується стратегічне IT-планування для визначення бізнес-вимог, які можуть вплинути на вимоги до технологій, персоналу та інформаційної безпеки?						II. Організаційна безпека
8	Чи повідомлено на членів вашого відділу обов'язки з питань інформаційної безпеки, і якщо так, чи мають вони конкретні вказівки щодо захисту критичної інформації?	6	Чи створена організаційна структура безпеки, яка визначає роли та обов'язки щодо захисту інформації?						II. Організаційна безпека
9	Чи проводяться перевірки біографічних довідкових даних і чи перевіряється вони в процесі найму та підбору персоналу?	7	Чи виконуються та перевіряються попередні та контрольні перевірки під час найму та найму та процесів?						II. Організаційна безпека
		8	Чи перетворюється та відповідають вимогам до навичок безпеки поточні можливості співробітників служби безпеки та оцінюється чи відповідають вимогам організації щодо безпеки?						II. Організаційна безпека
		9	Чи завіт навички безпеки у співробітників, щоб жодні важливі функції безпеки не залежали від одного працівника?						II. Організаційна безпека
		10	Чи існують конкретні критерії, якими повинен відповідати договір партнер чи постачальник щодо вимог безпеки?						II. Організаційна безпека
10	Чи включає ваш відділ вимоги інформаційної безпеки в договори з третіми сторонами, які обробляють або зберігають конфіденційні дані або системи?	11	Чи проводиться перевірка ризику, під час створ з третьою стороною чи підрядною службою для визначення таких ризиків, як обробка конфіденційних даних та обмін власною інформацією чи інтелектуальною власністю?						II. Організаційна безпека