ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

Кафедра системного аналізу

Пояснювальна записка

до магістерської роботи

на ступінь вищої освіти магістр

на тему: «РОЗРОБКА МОДЕЛІ АНАЛІЗУ ЗАГРОЗ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ДЛЯ КОМЕРЦІЙНИХ КОМПАНІЙ»

Виконав: студент 6 курсу, групи САДМ-61
спеціальності
124 Системний аналіз
(шифр і назва спеціальності)
Гончар А.О.
(прізвище та ініціали)
Керівник Козаченко С.Я.
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)
Нормоконтроль _____
(прізвище та ініціали)

Київ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально–науковий інститут телекомунікацій

Кафедра Системного аналізу
Ступінь вищої освіти «Магістр»
Спеціальність підготовки 124, Системний аналіз

ЗАТВЕРДЖУЮ
Завідувач кафедри
Системного аналізу
_____Т.Б.Гордієнко
“____” _____ 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Гончар Артему Олександровичу
(прізвище, ім’я, по батькові)

1. Тема роботи: Розробка моделі аналізу загроз цифрової трансформації для комерційних компаній

Керівник роботи Козаченко Сергій Якович, д.т.н., проф..
(прізвище, ім‘я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від“ _____” 2022 року №____

2. Строк подання студентом роботи 25 грудня 2022 року

3. Вихідні дані до роботи

3.1 Науково-технічна література та електронні джерела

3.2 Статистичні дані кіберзлочинів

3.3 Моделювання загрози цифровій компанії

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

4.1. Особливості цифрової трансформації

4.2. Аналіз загроз цифровізації

4.3. Адаптування рішень до загроз

4.4. Розроблення моделі цифрового ризику

5. Перелік графічного матеріалу

5.1 Об’єкт, мета, предмет магістерської роботи

5.2 Актуальність роботи

5.3 Задачі магістерської роботи

5.4 Що таке цифрова трансформація?

5.5 Бізнес-модель цифрової трансформації

5.6 Статистичні дані по Україні

5.7 Прогнозування загроз

5.8 Вирішення проблеми

5.9 Апробація роботи

5.10 Висновки

6. Дата видачі завдання ___1 листопада_2022 року_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської Роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	7 днів	Виконав
2	Пошук інформації про подібне моделі захисту цифрової компанії	5 днів	Виконав
3	Визначення актуальності дослідження	3 дні	Виконав
4	Пошук та аналіз можливостей прогнозування загроз	3 дні	Виконав
5	Збір даних про загрози	1 тиждень	Виконав
6	Реалізація моделі захисту та упередження загроз	1 місяць	Виконав
7	Розробка обов'язкових демонстраційних матеріалів	3 дні	Виконав
8	Попередній захист роботи		Виконав
9	Пред'явлення роботи в деканат		Виконав

Студент _____ Гончар А.О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Козаченко С.Я.
(підпис) (прізвище та ініціали)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється студент Гончар А.О. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 124 Системний аналіз
(шифр і назва спеціальності)
на тему: «Розробка моделі аналізу загроз цифрової трансформації для комерційних компаній
Магістерська робота і рецензія додаються.

Директор ННІТ _____ Кравченко В.І.
(підпис)

Довідка про успішність

Гончар А.О. за період навчання в Навчально-науковому інституті телекомунікацій
(прізвище та ініціали)
–2021 року до 2022 року повністю виконав навчальний план за напрямом підготовки, магістр, 124, системний аналіз з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Провідний фахівець інституту _____ _____
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студентка Гончар Артем Олександрович показав свою підготовку разом із володінням теоретичного матеріалу із розумінням методики розробки і моделювання загроз комерційним компаніям, адже якісно вміє володіти новими комп'ютерними технологіями та вміє детально користуватися навчальною, довідковою і науково-технічною літературами. Позитивними рисами дипломної роботи є актуальність, системність та послідовність викладеної інформації. Тема дипломної роботи розкрита, основні положення та висновки достатньо обґрунтовані. Всі поставлені задачі виконано.

Магістерська робота виконана на достатньому рівні і заслуговує оцінку «добре», а студенту Гончар Артему Олександровичу – присвоєння кваліфікації Магістр з системного аналізу.

Керівник роботи _____ Козаченко С.Я.
(підпис) (прізвище та ініціали)
« ____ » _____ 2022 року

Висновок кафедри про магістерську роботу

Магістерську роботу розглянуто. Студент Гончар А.О. допускається
(прізвище та ініціали)
до захисту даної роботи в Державній екзаменаційній комісії.
Завідувач кафедри Системного аналізу
(назва)
_____ Т.Б. Гордієнко
(підпис) (прізвище та ініціали)
« ____ » _____ 2022 року

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

IoT – Інтернет речей

TTP – Татктики Техніки Процедури

VPC – Віртуальна приватна хмара

XaaS – Все як послуга

SaaS – Програмне забезпечення як послуга

RaaS – Програма-вимагач як послуга

IPS/IDS – Системи виявлення та запобігання вторгнень

RDP – Протокол віддаленого робочого столу

RAT – Троян віддаленого доступу

РЕФЕРАТ

Текстова частина дипломної роботи: 70 сторінок та включає 6 ілюстрацій, 2 таблиць та 14 інформаційних джерел.

У дипломній роботі було створено модель загрози, яка допомогає передбачити загрозу цифровій трансформації.

Об'єкт дослідження – аналіз та прогнозування ризиків комерційних компаній від кіберзлочинів на основі статистичних даних.

Предмет дослідження – Хмарні загрози, атаки вимагачі, використання вразливостей, товарні атаки, Інтернет речі та Ланцюг поставки.

Мета роботи – реалізувати модель забезпечення захисту в цифровій екосистемі, з урахуванням бізнес моделі корпорації.

Методи дослідження – аналіз існуючих загроз та інструментів для кібератак на комерційні компанії.

Отримані результати –систематизовано спектр загроз для цифрової трансформації, тенденції їх виникнення, та відповідних систематизовано загальні принципу захисту компаній, та управління наявних та потенційних ризиків .

ВСТУП

З появою Covid-19, 2021 рік став кульмінаційним моментом для великих і малих компаній, пандемія змусила багатьох прискорити свою цифрову трансформацію та прийняти гібридні моделі роботи.

Зловмисники вже націлені на можливості, які відкриває бізнес в процесі цифрової трансформації. З стимулом до цифрових трансформацій обов'язково з'являться ключові вразливості, які визначать цілі атак на організації.Проте, завдяки допомогою безлічі інструментів і найкращих практи – компанії будуть стримувати всі загрози, зміцнюючи свій периметр кібербезпеки.

Нові загрози продовживатимуть перевіряти стійкість ланцюжків поставок по всьому світі. Набравши популярності серед кіберзлочинців чотирикратна модель вимагання завдавала збої в роботі не лише жертву, а і усіх субєктів комерційних компаній, такі як кліенти та партнери.

Компаніям які використовують хмарні технології необхідно буде зміцнити захист на всіх фронтах, якщо вони хочуть витримати атаки від кіберзлочинців, які використовуюють перевірені методології. Очікується, що збільшиться кількість зловмисників націлених на збіркові системи та облікові даних користувачів для входу до хмарних служб і програм. Розробникам та працівникам буде необхідно перевірити, що їхні облікові дані не знаходяться в руках зловмисників, які прагнуть скомпрометувати системи.

В цьому році буде виявлено величезну кількість вразливостей та мисливців за вразливостями, які мають намір отримати велику нагороду за помилки в системі. Прогнозується, що також буде сплеск експлойтів нульового дня. Також, через розмаїття систем, зявляться нові загрози для IT-інфраструктури, слабкі місця випробовуватимуть стакування численних вразливостей для створення нових багатоплатформних загроз.

Компаніям доведеться загартовувати себе проти сучасних загроз програм-вимагачів, які стануть ще більш цілеспрямованими. А оператори програм-

вимагачів застосовуватимуть дедалі складніші методи вимагання, наприклад, викрадання даних, щоб використовувати їх як зброю. Їхні напади стануть проблемою для команди безпеки, оскільки багатьом компаніям ще належить інвестувати в захист своїх серверів та кінцевих точок.

Поки підприємства будуть зайняті відбиттям цілеспрямованих атак, кіберзлочинці з оновленими наборами інструментів матимуть кращий успіх у менших компаній, значною мірою завдяки брокерам, які продають зловмисне програмне забезпечення. Наступного року відбудеться нова хвиля зловмисного програмного забезпечення ймовірно, включатиме впровадження особливо підступної моделі ботнету як послуги, здатної компрометації кількох платформ.

Подальший розвиток інтелектуальних пристроїв сприятиме зростанню інтересу кіберзлочинців на Інтернет речей (IoT), виходячи за межі (фізично) самих розумних пристроїв. Це дасть можливість для розробників систем безпеки об’єднатися, щоб написати нову дорожню карту для нового класу безпеки в розумних речах.

Зрештою, 2022 рік став перехідним періодом, який сповнений можливостей для компаній та кіберзлочинців.

ЗАВДАННЯ ДОСЛІДЖЕННЯ

В рамках магістерської роботи необхідно:

1. Підібрати необхідну технічну літературу
2. Проаналізувати актуальність даної роботи
3. Здійснити пошук інформації про загрози на комерційні компанії
4. Зібрати дані кількості кіберзлочиності в Україні за останні 10 років
5. Зробити аналіз ризиків комерційних компаній
6. Розробити модель для прорахунку ймовірності атак на комерційні компанії
7. Запровадити модель протидій загрозі на прикладі
8. Зробити висновки

1. ВПЛИВ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

1.1. Що таке цифрова трансформації?

Цифрова трансформація — це процес, за допомогою якого компанії впроваджують технології у свій бізнес, щоб стимулювати фундаментальні зміни.

Цифрова трансформація була модним словом протягом значної частини останнього десятиліття та різко прискорилася через пандемію COVID-19. Однак мотивація поєднувати цифрові та фізичні процеси з клієнтським досвідом ніколи не була такою потужною, як зараз. Залежно від галузі та підприємства, типи цифрової трансформації можуть відрізнятися, але загальна мета полягає в тому, щоб запровадити кардинальні зміни в стратегії компанії на ринку.

До цифрової трансформації веде багато різних шляхів, і шлях кожної компанії буде унікальним. Наприклад, компанія може запровадити штучний інтелект або хмарні обчислення, щоб покращити взаємодію з клієнтами. Або використовуючи машинне навчання може перепроектувати свій ланцюжок поставок. Компанія може навіть робити точні прогнози за допомогою штучного інтелекту та машинного навчання щодо продуктів, які захочуть клієнти через кілька місяців, а потім налаштовувати виробництво продуктів відповідно до попиту.

Організації усвідомлюють, що використання технологій є обов’язковим для досягнення їхніх цілей зростання та прибутковості. Хоча підвищення ефективності та прибутковості були ключовими рушійними силами всіх типів цифрової трансформації, пандемія змінила акценти для багатьох галузей. Безперервність бізнесу та стійкість організації стали головними пріоритетами в зміні того, як організації підходять до свого майбутнього.

Успішна стратегія цифрової трансформації вимагає від організацій визначення та формулювання своїх цифрових цілей для створення широкого організаційного узгодження. На початку важливо оцінити цифрову зрілість

компаній та готовність до змін, щоб потім точно визначити необхідні критичні можливості та компетенції.

Хоча мета цифрової трансформації полягає у використанні цифрових технологій для вирішення традиційних проблем, тобто використання технологій, щоб змінити спосіб роботи організації, позиціонувати себе на ринку та надавати переваги клієнтам.

Таблиця знизу показує як кардинально змінився підхід до роботи після цифрової трансформації.

До цифрової трансформації	**Після цифрової трансформації**
Ми віримо в дослідження. Ми ніколи не взаємодіємо з нашими клієнтами	Клієнти є основою нашої роботи. Ми їх краще розуміємо
Ми мало спілкуємося один з одним	Ми покладаємося на мозковий штурм і спілкування між командами, щоб переконатися, що всі працюють на одній стороні.
Слідкуємо за науковими роботами.	Ми приймаємо рішення в реальному часі на основі відгуків клієнтів
Ми знаємо, що краще	Наші клієнти говорять нам, що вони хочуть

Таблиця.1 Ставлення компанії до та після цифрової трансформації

Якщо бізнес-модель компанії ґрунтується виключно на фізичній взаємодії з клієнтами, постачальниками та співробітниками, то протоколи боротьби з COVID-19, ймовірно, серйозно сповільнила роботу. Багато застарілих технологічних компаній почали трансформувати свої бізнес-моделі та культуру від «одноразових продажів» до моделей обслуговування або передплати, які

підтримуються цифровими технологіями. Оскільки цифрові конкуренти не обтяжені тягарем успадкованих операцій, на ринок існує жорстка конкуренція.

Цифрова трансформація вимагає переосмислення того, як організація створює цінність. Це не просто додавання технологій до існуючих процесів - це вимагає кардинального перегляду того, як підприємство використовує технології разом з операціями та людьми для оптимізації продуктивності.

Під час процесу цифрової трансформації старі та нові потоки доходів співіснуватимуть. Але ресурси обмежені підтримкою застарілих операцій із одночасним впровадженням ціннісної пропозиції «все як послуга» (XaaS).

Зображення нижче ілюструє бачення, як багато бізнес-лідерів реалізуються через власну цифрову трансформацію. Попит клієнтів задовольняється в режимі реального часу, використовуючи правильні постачання, правильні виробничі процеси та дистрибуцію на основі Інтернету речей, машинного навчання, штучного інтелекту, блокчейну та інших революційних технологій.

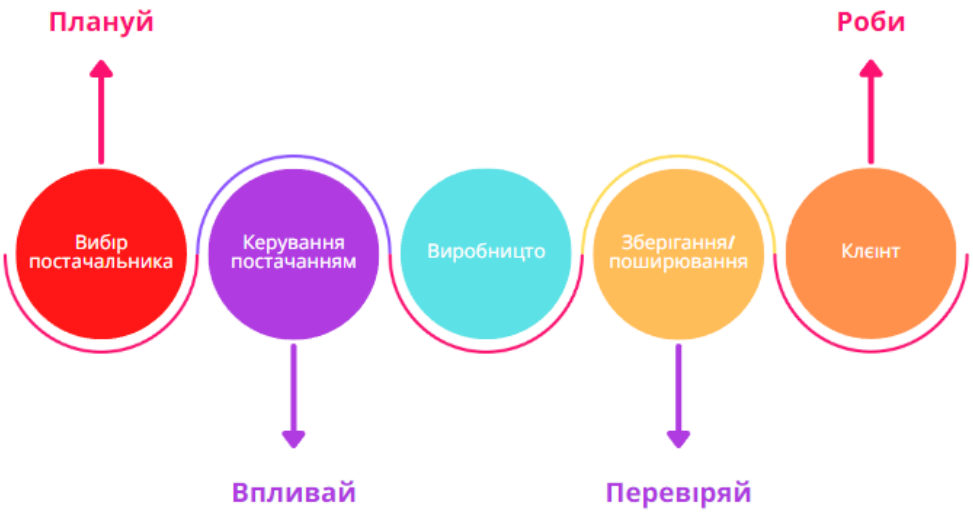

Рисунок.1 Задоволення попиту клієнтів шляхом використання передових цифрових технологій

Проста автоматизація або оцифрування існуючих процесів і продуктів — не єдина варіант. Вибір оптимального шляху серед бізнес-моделей має вирішальне значення для прискорення трансформації.

Ринок обладнання, програмного забезпечення та IT-послуг скорочуються в епоху цифрової трансформації. Через падіння вартості обчислювальної потужності компанії переходять на модель XaaS. Наприклад, галузь ланцюгів постачання рухається в цьому напрямку — це вже не лише володіння вантажівками та складами. Натомість компанії укладають контракти на транспортування та логістику як послугу, передаючи ці функції експертам з технологічних послуг, щоб забезпечити більш значні інвестиції в їх основні компетенції.

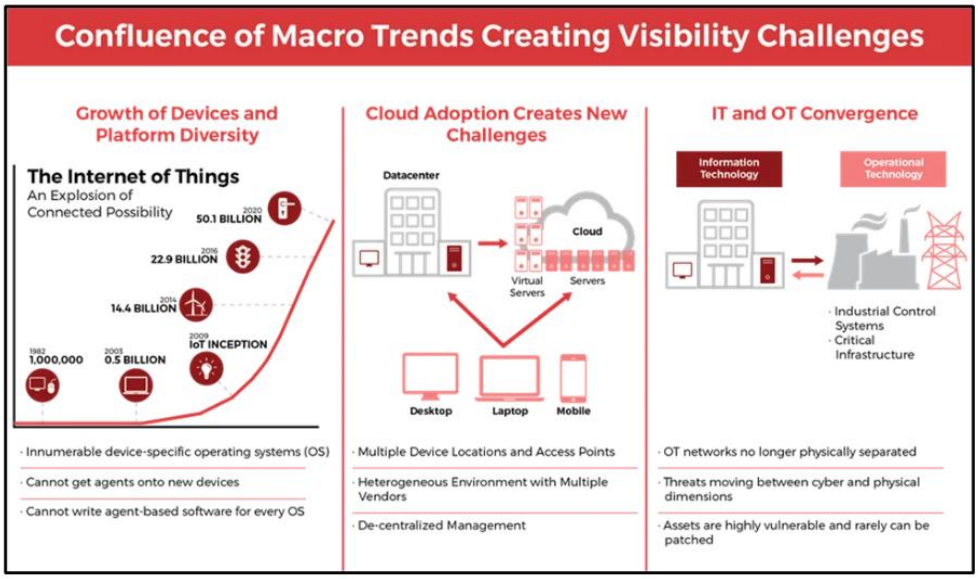

Рисунок.2 Конвергенція Інтернету речей, хмарних технологій, IT і OT кардинально змінить бізнес-моделі, ланцюги поставок і стратегії виходу на ринок.

Зображення вище, ілюструє прогалини в безпеці, які зрештою виникнуть після впровадження нових цифрових інвестицій.

Для технологічних компаній виробників оригінального обладнання цифрові інновації вимагають швидкого перетворення традиційних IT на гнучкі моделі XaaS. Але виробники застарілих технологій, які переживають цю зміну,

стикаються як з внутрішніми, так і ззовні. Вони повинні прийняти мислення цифрової трансформації всередині себе, одночасно адаптуючи свій портфель рішень, щоб також сприяти цифровим зусиллям їхніх клієнтів. Зрештою, якщо трансформація XaaS виконується ефективно, вона зміцнює, захищає та навіть створює нові джерела доходу для виробників технологій.

Є 4 типи цифрової трансформації. Цифрова трансформація не означає те саме для всіх компаній, і розглядати її як універсальний процес неможливо, оскільки всі компанії залучають клієнтів, інтегрують постачальників і виробляють продукцію по-різному. Є чотири основні типи цифрової трансформації, переваги яких організації повинні розглянути у своїй власній стратегії трансформації. Важливо усвідомлювати, що цифрова трансформація не обов'язково є єдиним, шаблонним напрямком у формі продукту чи пропозиції, натомість вимагає довгострокових зобов'язань і може розвиватися протягом усього шляху цифрової трансформації..

1.2. Що Бізнес-модель і трансформація потоку

Трансформація бізнес-моделі має на меті докорінно змінити спосіб, у який компанії створюють цінність для клієнтів. Наприклад, використовуючи історію, з якою всі знайомі, Netflix здійснив перехід від розсилки DVD-дисків до онлайн-потоку, тоді як Blockbuster не зміг здійснити перехід, що зрештою призвело до загибелі компанії. Виробники оригінального обладнання також переходять від моделі продажів і підтримки до XaaS, де «X» може позначати апаратне забезпечення, ємність пам'яті або програми.

Технологічні компанії можуть змінити свою стратегію виходу на ринок і підтримати зусилля своїх клієнтів у цифровій трансформації за допомогою гнучкості у виборі технології, яка найкраще відповідає їхнім потребам. Згадайте про появу Zoom, Peloton, Grubhub, Okta та багатьох інших компаній, які X - «залишайтеся вдома», які зайняли величезну частку ринку під час карантину.

Клієнти часто сигналізують про свою готовність до іншого типу відносин через свої моделі купівлі.

1.3. Трансформація ланцюга поставок і логістичного процесу

Компанії можуть переглянути внутрішні процеси, щоб знизити витрати, покращити якість і скоротити тривалість циклу. Застосування підключення до хмари допомагає зв’язати різні процеси та місця.

Наприклад, запровадження роботизованої автоматизації процесів може трансформувати ручні завдання, які можна знайти під час закупівель, управління ланцюгом поставок та інших адміністративних функцій. Модернізація логістичної мережі та ланцюга постачання шляхом оцифровки процесів та інтеграції машинного навчання та штучного інтелекту допомагає розпізнавати та формувати шаблони даних у практичні висновки.

1.4. Домен і трансформація виходу на ринок

Організації зазвичай впроваджують нові технології, щоб переосмислити свої продукти та послуги. Вони можуть розширити поточні послуги для нової клієнтської бази або розробити абсолютно нові технологічні пропозиції. Наприклад, пропонуючи обладнання на основі оренди, а не лише покупки, ви зможете охопити сегмент клієнтів, які раніше не обслуговувалися, яким ваша технологія може знадобитися лише тимчасово.

Як інший приклад, компанії, які продають промислове обладнання, можуть розширюватися, надаючи цифрові рішення своїй існуючій клієнтській базі та клієнтам, які використовують інше обладнання. Італійський [CNH Industrial] виробник комерційного, будівельного та сільськогосподарського обладнання, розробив власний пакет телематичних технологій для автопарку, щоб допомогти власникам оптимізувати процеси експлуатації та технічного обслуговування, та підключити їх до дилерської мережі компанії для обслуговування.

1.5. Культурна та організаційна трансформація

Прийняття цифрової культури дає змогу організаціям застосовувати гнучкі робочі процеси, розвивати упередженість у бік тестування та навчання, а також підтримувати децентралізоване прийняття рішень. Однак успішний перехід до цифрової культури вимагає переосмислення мислення та процесів, а також залучення нових талантів і здібностей.

Типова зміна мислення змінюється від управління виробництвом до зосередження на обслуговуванні клієнтів та інноваціях. Часто культурні зміни відбуваються органічно під час інших ініціатив трансформації, оскільки внутрішні команди запроваджують цифрові робочі процеси та визнають силу зміни організаційних норм.

1.6. Цифрова трансформація та виробництво

Вплив цифрової трансформації у виробництві на підприємства, їхніх постачальників, клієнтів та інших третіх сторін є приголомшливим. Незалежно від того, чи продають організації обладнання чи будівельні матеріали, технології можуть допомогти організаціям багатьма способами. Цифрові технології допомагають виробникам підвищити операційну ефективність і оптимізувати різні сфери бізнесу, від розробки продукту до ланцюга постачання.

Передові виробничі технології мають численні переваги, наприклад допомагають компаніям розблокувати цифрові бізнес-моделі, швидше адаптуватися до змін або навіть передбачити зміни до того, як вони відбудуться – усе це надзвичайно важливо для виробництва.

Цифрова трансформація у виробництві означає вдосконалення традиційних виробничих процесів, продуктів і робочої сили за допомогою цифрових технологій, таких як програмне забезпечення для автоматизації, електронна комерція, датчики, промислові роботи тощо.

Метою цифрової трансформації у виробництві є:

- Швидко адаптуватися до змін у вимогах клієнтів і ринку, щоб створити конкурентну перевагу.
- Підвисити операційну ефективність, зменшити витрати та максимізувати дохід.
- Підвищення якості вироблених товарів.
- Покращити взаємодію з клієнтами через розповсюдження або процес замовлення.
- Розширювати можливості прийняття рішень за допомогою аналітики.

Стан виробництва постійно змінюється через нестабільність глобального, економічного та політичного ландшафтів. Не кажучи вже про те, що багато виробничих підприємств серйозно постраждали від пандемії та їм потрібно було швидко адаптуватися, щоб утриматися на плаву.

Розширені мережеві можливості 5G, інтеграція IoT, машинне навчання та прогнозна аналітика на основі даних впливають на виробництво. Цифрова трансформація призвела до появи нової концепції розумних фабрик, що ґрунтується на підвищенні ефективності та стійкості.

Загалом IoT та нові технології, які стануть частиною розумних міст, покращать якість життя. Однак використання будь-якої технології породжує нові проблеми та виклики. У розумному місті, вразливі дії окремої людини чи організації можуть поставити під загрозу все місто. Через залежність різних компонентів розумних міст від інформаційно-комунікаційних технологій проблеми кібербезпеки, такі як витік інформації та зловмисні кібератаки можуть серйозно вплинути на розумне місто.

IT-директори, технічні директори та інші IT-лідери повинні знати про рішення, які обирають міста, і переконатися, що безпека закладена в них із самого початку. Вони повинні працювати на випередження, щоб зрозуміти, як їхні постачальники шифрують дані та забезпечують багатофакторну автентифікацію, наприклад, для контролю доступу до мережі.

Першочерговими завданнями в таких навчаннях має бути проведення аудиту пристроїв, аналіз прогалин, щоб визначити, де можуть бути прогалини в безпеці, а потім створення постійної стратегії пом'якшення загроз із постійною підтримкою, якщо це необхідно.

1.7. Цифрова трансформація в Україні та передумови цифрового розвитку

Україна вже визначила свою цифрову трансформацію як пріоритетну політику. Нещодавно європейська експертна спільнота визнала успіх у впровадженні таких систем, як "ProZorro" та "e-Health", запуск електронних послуг у державному та приватному секторах, а також широкому покритті мережі 4G. В Україні за останні роки з'явилася тенденція цифрового розвитку і її вважають новим рухом в економіці країни. Ще у 2018 році уряд затвердив ряд концепцій та планів щодо економічного та суспільного розвитку на наступні чотири роки. В 2019 році виконавча влада України презентувала план розвитку цифрової економіки країни,

Прискорення розвитку для переведення української економіки в цифровий формат, так у 2019 році виконавча влада України презентувала свої амбіційні плани.

Міністерство цифрової трансформації визначило мету до 2024 року:

- 100 % публічних послуг мають бути доступні громадянам та бізнесу онлайн.
- 95 % транспортної інфраструктури, населених пунктів та їхні соціальні об'єкти мають мати доступ до високошвидкісного Інтернету.
- 6 млн. українців мають бути залучені до програми розвитку цифрових навичок.
- доля IT-продукту у ВВП країни має складати не менше 10 %.

Перші кроки включали прийняття правової основи для основних цифрових прав громадянина, включаючи право на доступ до широко-смугового

Інтернету та збільшення доступності технологій для споживачів з метою зниження вартості програмного забезпечення, комп'ютерного та іншого обладнання.

Для просування цифрового порядку було розроблено ряд законів:

- про цифрову економіку;
- про цифрову інфраструктуру;
- про телекомунікації;
- про електронної торгівлі(e-Trade);
- про електронного захисту(e-Trust);
- про кібербезпеку(Cybersecurity);

Прогресивні прагнення цифрового розвитку України підтверджуються розробкою інтеграції України до Єдиного цифрового ринку Європейського Союзу, проєкт який проходив оцінку представниками профільних структурних підрозділів Європейської Комісії.

Серед країн які прагнуть вступити до ЕС Україна займає передові позиції у вдосконаленні інституційних та регуляторних сфер для розвитку цифрової інфраструктури та телекомунікаційних послуг.

Також швидкими темпами розвивається система надання публічних е-послуг та електронної ідентифікації. Мобільний додаток «Дія», який надавав доступ зі смартфона до цифрового посвідчення водія та свідоцтва про реєстрацію транспортного засобу . Для отримання доступу потрібно було вже мати водійські права та техпаспорт, а також необхідно пройти ідентифікацію за допомогою системи BankID у додатках «Приват24» або monobank . Верифікація документів співробітниками поліції відбувалася за допомогою QR-коду.

Найбільші переваги та досягненя у сфері цифрового розвитку

- поява Міністерства цифрової трансформації України;
- створення та підвищення законотворчої активності Комітету цифрової трансформації України;

- запуск порталу державних послуг та мобільного застосунку «Дія»;
- розвиток сфери електронних комунікацій та вдосконалення системи надання електронних довірчих онлайн;
- збільшення кількості ініціатив у сфері цифрової освіти;
- розробка стратегії інтеграції України до Єдиного цифрового ринку Європейського Союзу;

Найактуальніщі проблеми цифрового розвитку України на даний момент

- наявність значних прогалин в географії покриття території України можливостями доступу до мережі Інтернет;
- необхідність посилення активності у розвитку цифрових навичок всіх категорій громадян та секторів економіки;
- затягування прийняття Закону України «Про електронні комунікації»;
- брак офіційно затверджених стратегічних документів у сфері цифрового розвитку;
- прогалини в системі кібербезпеки та захисту персональних даних у мережі Інтернет;
- низьку якість досліджень в системі вищих навчальних закладів та науково-дослідних інститутів, недостатню підтримку цифрової трансформації бізнесу;

1.8. Цифровізація під час війни

Повномасштабне вторгнення Росії в Україну засвідчило значну роль цифрової трансформації економіки для забезпечення стійкості та гнучкості української держави в умовах війни. Серед пріоритетів у Міністерстві цифрової трансформації є формування єдиного цифрового ринку з ЄС,а також наближення структури цифрового сектору України до вимог в умовах війни та післявоєнного періоду.

Першою метою була підтримка економіки та армії шляхом придбання військових облігацій у застосунку «Дія». Станом на 25 жовтня 2022 року було

придбано 70 тисяч військових облігацій на суму в 70 мільйонів гривень, котрі направлені на перемогу України.

Громадянам України вперше довелось воювати не тільки на фронті бойових дій, а й на інформаційному фронті. Запустивши чатбота “єВорог” громадяни могли передавати дані про пересування російських солатів.

Завдяки авторизації через BankID, можна було відсіяти диверсантів, які передавали неправдиву інформацію та намагалися завести наших військових у пастку. Зібрані дані від сміливих та хоробрих українців дали змогу бійцям ЗСУ виконати величезну кількість важливих операцій.

Україна стала першою країною котра використовувала технології під час повномасштабної війни та отримала унікальний досвід.

Для розпізнавання загиблих росіян використовують штучний інтелект, який сканує фото та за допомогою соціальної інженерії знаходять близьких в соціальних мережах та повідомляють про це.

Знаходження нових рішень, використання технології Starlink для роботи важливих об’єктів. Зараз Україна використовує понад десять тисяч станцій, які роздають супутниковий інтернет для відновлення та підтримки критичної інфраструктури.

Започаткували перший державний криптофонд для потреби людей і військових, вже зібрано понад два мільярда гривень, всі кошти йдуть на гуманітарну допомогу та потреби військових.

Тестування програми «єОселя» - ініційована президентом України, програма доступного кредитування житла з пільговими ставками 3 % для чотирьох категорій та 7 % – для всіх інших категорій у застосунку «Дія», що сприятиме отриманню нового житла громадянам, які втратили свої домівки через повномасштабне вторгнення РФ, для захисників України, а також для медиків, педагогів, науковців, які працюють у закладі освіти й наукових установ державної або комунальної форми власності.

Наближення положень національного законодавства до європейських вимог у сферах електронної ідентифікації та електронних довірчих послуг. За підтримки EU4DigitalUA представники Мінцифри, Держспецзв'язку, ДП «Дія», Національного банку України взяли участь у восьмому Форумі з довірчих послуг у Берліні. Там було представлено проміжні результати з: розгортання eIDAS-вузла для забезпечення інтероперабельності електронної ідентифікації з eIDAS-інфраструктурою; розроблення електронного гаманця EU Digital ID Wallet. Представники Європейської комісії позитивно оцінили такі досягнення.

Щоб Україна швидше інтегрувалася до Єдиного цифрового ринку ЄС потрібно наблизити положення національного законодавства до европейських вимог, а також підготувати вітчизняний орган з оцінки відповідності. До Верховної Ради України передано на розгляд законопроєкт про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства Європейського Союзу у сфері електронної ідентифікації.

06 жовтня 2022 р. Верховна Рада України ухвалила закон про е-резидентство для іноземних підприємців та креативних лідерів, які мають можливість дистанційно вести свій бізнес в Україні, відкривати банківські рахунки та сплачувати податки на вигідних умовах[8].

Посилення можливостей національної системи кібербезпеки для протидії кіберзагрозам російської федерації проти України, в першу чергу спрямовано на інформаційно-комунікаційні системи державних органів України, а також на об'єкти критичної інфраструктури.

У жовтні 2022 року Україна долучилася до місяця кібербезпеки США та ЄС в межах кіберреформи UA30 з метою привернути увагу суспільства до кібербезпеки та створення повноцінної системи кіберзахисту. 26 лютого 2022 року міністр цифрової трансформації України Михайло Федоров оголосив про створення ІТ-армії. Він звернувся до українців, які працюють у цифровій сфері: розробників, кіберспеціалістів, дизайнерів, копірайтерів, маркетологів,

таргетологів тощо. Головна мета спільноти: боротьба з ворогом на кіберфронті. Всі свої дії щодо кібератак на окупантські сайти та сервіси ІТ-спеціалісти координують у Telegram-спільноті і Twitter. На сайті викладені інструкції за якими приєднатися до кібератак можуть не тільки фахівці, а майже будь-хто.

Також telegram-канал, де кожен може побачити канали, що практикують дезінформування, створення фейків, мову ворожнечі, і поскаржитись з метою блокування каналів, що ошукують свою авдиторію започаткувало Мінцифри.

Ці заплановані дії сприятимуть цифровій трансформації економіки задля забезпечення стійкості та гнучкості нашої держави й інтеграції України до міжнародного цифрового простору. Потенційно це призведе до залучення коштів у межах європейської програми ЄС «Цифрова Європа» та програми фінансування під'єднання вітчизняної магістралі до цифрових глобальних шлюзів і підвищення цифрового потенціалу українських компаній, їх структурної модернізації та, як наслідок, посилення їхньої стійкості в післявоєнний період.

2. СИСТЕМАТИЗАЦІЯ ЗАГРОЗ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

2.1. Аналіз існуючих загроз

Хоча загрози кібербезпеці постійно змінюються, є деякі з найвідоміших і поширених типів кіберзагроз, на які варто звернути увагу на поточному ринку:

- **Фішинг.** Ці загрози, які колись здебільшого обмежувалися погано написаними фішинговими електронними листами, набули популярності та витонченості, а атаки соціальної інженерії здійснюються на настільних комп'ютерах і мобільних пристроях за допомогою голосових дзвінків, текстових повідомлень і соціальних мереж. Ці атаки досягають більшого рівня успіху: Федеральна торгова комісія стверджує, що у 2020 році було подано 4,8 мільйона звітів про крадіжки особистих даних і шахрайство, що на 45% більше, ніж у 2019 році, при цьому фішинг становить 44% усіх кібератак. Різноманітні атаки, як-от фішинг, під час якого зловмисники переслідують цілі високого рівня, також зростають.
- **Програми-вимагачі**: під час атаки програмного забезпечення-вимагача кіберзлочинець встановлює частину зловмисного програмного забезпечення на комп'ютер або сервер, яке шифрує конфіденційну інформацію, яку він знаходить. Потім зловмисник вимагає викуп, щоб розшифрувати дані, як правило, такі платежі проводять у біткойнах, які неможливо відстежити. У 2019 році в усьому світі вимагали близько 25 мільярдів доларів викупу , а загальні витрати на відновлення та збитки наближалися до 170 мільярдів доларів. Екстремальні атаки програм-вимагачів можуть вивести з ладу ланцюжок поставок, виробничі можливості або здатність компанії працювати.
- **Ботнет-атака**: історично ботнети використовувалися для запуску атак типу «відмова в обслуговуванні» (DoS) або розподілених атак «відмова в обслуговуванні» (DDoS), а також для захоплення обчислювальних ресурсів підприємства, як правило, для майнінгу криптовалют. NetScout

повідомляє, що минулого року загальна кількість DDoS-атак вперше перевищила 10 мільйонів . Підприємства піддаються ризику не лише через те, що вони стають об’єктами атак ботнетів, але й через те, що у їхніх власних мережах встановлено шкідливе програмне забезпечення для ботів.

- **Хмарні експлойти**: використання хмарних ресурсів зростають, оскільки організації продовжують переносити частину роботи в хмару та розширюють хмарну інфраструктуру. Як і в інших експлойтах, хакери часто мають намір використовувати заражені корпоративні хмарні ресурси для викрадення даних або видобутку криптовалюти. Популярність хмарних атак зросла на 250% у 2020 році.
- **Атаки, пов’язані з роботою з дому**: обмеження, пов’язані з пандемією COVID-19, змушують мільйони корпоративних працівників працювати з дому. Оскільки гігієна домашньої безпеки користувачів зазвичай не така ретельна, як на рівні підприємства, це відкриває двері для атак, спрямованих на незахищені мережі Wi-Fi, паролі, які легко зламати, і навіть фізичну крадіжку пристроїв, таких як ноутбуки та смартфони.
- **Атаки на державний сектор**: Вважається , що резонансна атака SolarWinds, яка сталася в 2020 році, була ініційована російською розвідкою. Під час атаки кіберзлочинці впровадили бекдори в мережі десятків міжнародних компаній і державних установ, які надали їм постійний доступ протягом майже року, перш ніж їх виявили. Це підкреслило необхідність стратегій проактивної протидії цим складним операціям кібершпигунства.

2.2. Сучасні загрози цифровій трансформації

Оскільки за останні роки загрози кібербезпеці зростали, вони також стають дедалі складнішими та цілеспрямованими. Кіберзлочинці зазвичай використовують загальнодоступну інформацію, таку як дані соціальних мереж, для крадіжки особистих даних і легкого злому паролів. Завдяки цим даним, які зазвичай доступні на чорному ринку, кібератакникам легше, ніж будь-коли.

Тим часом технологія, доступна для здійснення цих атак, стає все більш поширеною. Зловмисники можуть використовувати ті ж типи ресурсів, що й будь-яке підприємство, включаючи хмарні обчислення, штучний інтелект і розподілені обчислювальні ресурси, щоб збільшити ймовірність успішної атаки. Оскільки площа атаки типового підприємства збільшується через поширення пристроїв Інтернету речей, хмарної інфраструктури та використання персональних пристроїв співробітниками, цілі стикаються з більшим рівнем ризику, ніж будь-коли раніше.

Цілі атак в сфері цифрової трансформації.

Мотиви кібератак змінювалися з роками, але зазвичай вони дотримуються деяких пунктів, зокрема таких:

- **Гроші**: Кінцевою метою більшості атак, прямо чи опосередковано, є фінансова вигода. Цього можна досягти шляхом крадіжки банківських облікових даних, номерів кредитних карток, ширшої крадіжки особистих даних або прямої крадіжки грошових ресурсів, таких як криптовалюта.
- **Дані**: Це включає в себе крадіжку особистої інформації (такої як номери соціального страхування, записи про медичне страхування та інше) або корпоративних даних (включно з інтелектуальною власністю, вихідним кодом, записами клієнтів тощо). Основна мета зловмисника щодо цих даних полягає в тому, щоб використовувати їх для здійснення нових атак або продати їх заради фінансової вигоди.

- **Обчислювальні ресурси**: кіберзловмисники часто прагнуть використати доступну обчислювальну потужність підприємства для здійснення додаткових атак або через традиційний центр обробки даних, або через хмару. Ці ресурси зазвичай використовуються для видобутку цінних криптовалют або запуску ботнетів, які запускають зловмисне програмне забезпечення або інший шкідливий код для запуску DDoS-атак.
- **Загальний хаос**: хоча й менш поширені, деякі атаки все ж здійснюються, щоб створити хаос і завдати шкоди жертвам. До цієї категорії належать атаки на системи водопостачання, електромережі та іншу критичну інфраструктуру.

Цілі атак.

Кібербезпека є особливо складною через збільшення розміру поверхні атаки та кількості методів, за допомогою яких зловмисник може використовувати їх. Поширені типи цілей кібератак включають:

- **Пристрої інфраструктури**: сервери, мережеве обладнання та бездротові точки доступу, серед іншого.
- **Корпоративні програми**: зловмисники атакують ці системи, використовуючи вразливі місця в коді або доставляючи їх через зловмисне програмне забезпечення.
- **Апаратне та програмне забезпечення кінцевої точки**: клієнтські комп’ютери та операційні системи, пристрої користувача, такі як смартфони, і навіть підключені пристрої Інтернету речей, такі як принтери.
- **Пристрої Інтернету речей**: будь-який пристрій Інтернету речей, підключений до мережі, включаючи промислові датчики, камери безпеки або навіть «нешкідливі» пристрої, такі як інтелектуальні термостати та інші прилади.

- **Хмарні ресурси**: Ця категорія включає системи зберігання, загальнодоступні хмарні служби (наприклад, веб-поштові системи) і платформи хмарних обчислень SaaS.
- **Сторонні постачальники**. Підприємства дедалі частіше піддаються ризику зламу або атаки через підрядників і постачальників, чиї системи не захищені належним чином.
- **Інсайдерські загрози**: працівники або підрядники, які використовують свої облікові дані для отримання несанкціонованого доступу та навмисно чи ненавмисно наражають компанію на шкідливе програмне забезпечення та інші ризики безпеці або викрадають особисті дані чи іншу конфіденційну інформацію.

Наслідки атак на бізнес.

Успішні кібератаки можуть мати значний вплив на бізнес, зокрема:

- **Фінансові втрати**: під час успішних атак підприємства можуть безпосередньо втратити кошти зі свого прибутку. Усунення збитків внаслідок кібератаки також може бути дорогим.
- **Репутаційна шкода**: коли трапляються порушення, особливо ті, що призводять до втрати даних клієнтів, репутація компанії може серйозно постраждати в результаті (у формі новинних повідомлень, відтоку клієнтів, втрати бізнесу та порушень комплаєнсу). Чим більше порушення, тим більший ризик завдати шкоди репутації компанії — і її перспективам отримати майбутніх клієнтів.
- **Операційні проблеми**: багато атак можуть призвести до зупинки критично важливих систем, що вплине на здатність бізнесу працювати. Ці системи можуть включати системи контролю виробництва, системи обробки платежів або інші важливі комп’ютерні системи.
- **Судові позови та регулятивні штрафи**. Порушення конфіденційності через викрадені записи клієнтів часто призводять до жорстких

регулятивних штрафів, колективних позовів і державних штрафів. Порушення також може призвести до підвищення страхових ставок для атакованого бізнесу.

2.3 Кіберзлочинність в Україні

Визначаючи сучасний стан кіберзлочинності в Україні, що вона, як і будь-яке інше соціальне явище, піддається передбаченню за допомогою певних індикаторів, що відбивають її кількісні та якісні характеристики. Здійснити таке оцінювання і моделювання можна через аналіз показників поширеності кіберзлочинності в Україні: її рівня, географії, структури, динаміки тощо.

Стосовно рівня кіберзлочинності та її динаміки зазначимо, що у 2009 р. в України було зареєстровано 217 злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, у 2010 р. – 190, у 2011 р. – 131, у 2012 р. – 138, у 2013 р. – 595, у 2014 р. – 443, у 2015 р. – 598, у 2016 р. – 865, у 2017 р. – 2573, у 2018 р. – 2301, у 2019р. – 2204, у 2020р. – 2498, за 2021р. – 2790 злочинів (рис.).

Рисунок.3 Динаміка кількості кіберзлочинності в Україні

Питома вага кіберзлочиннів у загальній кількості зареєстрованих злочинів становить 0,05 % від загальної кількості зареєстрованих злочинів у 2009 р., 0,04 % – у 2010, 0,03 % – у 2011, 0,03 % – у 2012, 0,11 % – у 2013, 0,08 % – у 2014, 0,11 % у – 2015, 0,15 % – у 2016, 0,49 % – у 2017, 0,51% – у 2018, 0,43% – у 2019, 0,55% – у 2020 та 0,59% – у 2021 від злочинів.

Рисунок.4 Динаміка питомої ваги кіберзлочинів

Суттєве збільшення кількості зареєстрованих у 2013 р. кіберзлочинів окремі вчені пов'язують із тим, що «зростання вказаного виду злочинності обумовлено щорічним зростанням користувачів Інтернет-ресурсу в Україні» [6]. Як бачимо з отриманих статистичних даних по злочинності, кіберзлочини мають значний позитивний приріст. Наступним не менш важливим кроком є визначення видів кіберзлочинів, які нестимуть найбільшу небезпеку, для цього скористаємось методом АВС-аналізу. Для розв'язання поставленої проблеми проведемо АВС-аналіз методом «суми» на основі статистичних даних звіту кіберполіції України по кіберзлочинам за 2020 рік.

Кіберзлочини	кількість	Частка фактора	Наростаюче значення	Наростаюче значення	Сума	Група

		у сумі значень фактора за даними (пос.КК)		(корелція)		
У сфері платіжних систем	4796	39,96	39,97	25	64,97	A
У сфері е-комерції	3196	26,62	66,62	50	116,62	B
У сфері кібербезпеки	2650	22,07	88,68	75	163,68	B
У сфері протиправного контенту	1360	11,33	100	100	200	C

Таблиця.2 ABC-аналіз кіберзлочинів

На табл2 представлена ABC-аналіз, яка інтерпретує поділ кіберзлочинів на групи. Узагальнюючи отримані результати, заважимо, що найуразливішою є сфера платіжних систем. Впровадження контрзаходів у ній може зменшити кількість кіберзлочинів майже на 40% від усіх можливих. Ми вважаємо, що цифровізація економіки збільшить приріст кіберзлочинів. Адже більшість населення, установ, фірм та організацій почнуть переходити на повне цифрове забезпечення, тобто основну інформацію будуть зберігати у цифровому просторі та на серверах.

2.4 Тенденції загроз цифрової трансформації

Хмарні загрози. Хмарні зловмисники як були так і залишаються на місці, вони продовжують стежити за технологічними тенденціями та продовжувають використовувати перевірені атаки, щоб завдати шкоди користувачам хмарних технологій.

Хмара, з її, здавалося б, нескінченною здатністю зберігати й обробляти величезні обсяги даних, має дозволити компаніям відносно легко перейти на

віддалену роботу після пандемії Covid-19. І наступного року хмарна міграція залишиться ключовим аспектом норми нової бізнес операції. Gartner прогнозує, що глобальні витрати на хмарні послуги перевищать 482 мільярди доларів США у 2022 році, що на 54% більше, ніж у 2020 році (313 мільярдів доларів США). І оскільки користувачі постійно переходять у хмару, зловмисники обов'язково підуть цьому прикладу.

Щоб максимізувати свою фінансову вигоду, зловмисники обов’язково охоплять усі підстави. Вони будуть продовжувати здійснювати випробувані типи атак і в той же час здійснювати ті, які використовують нові тенденції в технологіях, щоб залишатися попереду гри.

Підприємства не тільки продовжуватимуть використовувати програми та рішення типу «програмне забезпечення як послуга» (SaaS), але й планується розширити в наступному році. Gartner прогнозує, що користувачі SaaS витрачатимуть близько 172 мільярди доларів США у 2022 році, це найвищі витрати серед усіх публічних хмарних сервісів. І тому, що тактики, техніки та процедури (TTP), які використовують зловмисники, все ще працюють — і ймовірно, все ще працюватиме для нової групи користувачів SaaS — вони продовжуватимуть використовувати їх у 2022 році.

Зловмисники, як і раніше, використовуватимуть стратегії, які не потребують зусиль, але мають високу віддачу, щоб отримати доступ до хмари програми та послуги. Використання ними фішингових електронних листів для викрадення облікових даних є одним із прикладів та метод, який збережеться в наступному році. Вони також продовжуватимуть компрометувати програми SaaS і послуги через незахищені файли, неповернуті ключі доступу, отримані образи незахищених контейнерів з ненадійних джерел, і незріле або погано реалізоване керування доступом до ідентифікаційних даних політики.

Дійсно, кіберзлочинці зазвичай тяжіють до стратегій, які працюють. Зловмисники, для прикладу, все ще використовують відомі вразливості

минулих років, оскільки багато середовищ досі не виправлено. Крім використання нових вразливостей, які будуть виявлені в наступному році, вони продовжуватимуть використовувати старі, які все ще працюють.

Очікується, що групи кіберзлочинців, такі як TeamTNT, будуть націлюватися на хмару обчислювальної потужності для незаконного майнингу криптовалюти в наступних роках. Оскільки більше цифрових валют з'явиться, підрозділи кіберзлочинців продовжуватимуть використовувати хмарні обчислювальні ресурси жертв ітерації раніше помічених атак.

З іншого боку, кіберзлочинці також слідкуватимуть за технологічними трендами. Будь-яка технологія широко розповсюджене стає прибутковою мішенню для зловмисників, як і те, як зловмисники націлювалися на такі технології, як Java.10 Adobe Flash.11 і WebLogic.12

Зловмисники починають все частіше використовують цей підхід у своїх атаках. Інструменти DevOps13 і конвеєри в хмарних інтегрованих середовищах розробки (IDE). Прогнозується, що кіберзлочинці будуть проводити більше кампаній, використовуючи принципи DevOps у ланцюжках поставок, Kubernetes середовища, розгортання інфраструктури як коду (IaC) і конвеєри.

Також розробники та системи збірки слугуватимуть початковими точками входу для зловмисників, які прагнуть поширювати зловмисне програмне забезпечення на кілька компаній через атаки на ланцюги поставок. Зберігаються токени та паролі розробників, ключі до операцій підприємства, а використання скомпрометованих облікових даних розробника також збільшує шанси зловмисника розгорнути зловмисне програмне забезпечення поза радаром.

Впровадження хмари є фундаментальним елементом цифрової трансформації. Таким чином, це важливо для підприємствам підтримувати безпеку свого хмарного середовища, повертаючись до основ хмарної безпеки, які включають розуміння та застосування моделі спільної відповідальності. з

використанням добре архітектурної системи фреймворк, шифрування, виправлення та забезпечення належного рівня досвіду. Підприємствам також необхідно застосувати більш суворі протоколи безпеки навколо систем збірки та коду, який перевіряють розробники, особливо якщо надісланий код матиме участь у важливих виробничих процесах.

До цього кінця, групи безпеки можуть застосовувати такі заходи, як керування привілеями з короткочасним доступом токенів, створення журналу аудиту за допомогою інструментів командного рядка та моніторинг конвеєра шляхом програмне забезпечення для керування безпекою з відкритим кодом.

Загрози програм-вимагачів. Сервери стануть основним майданчиком для програм-вимагачів. Як будь-яка підступна кіберзагроза, програми-вимагачі виживають і процвітають, постійно розвиваючись. Раніше, інциденти програм-вимагачів зазвичай стосувалися кінцевих точок як основних точок входу, котрі падають жертвою атак, відкриваючи шкідливі листи або відвідуючи шкідливі веб-сайти, які таємно розгортають програми-вимагачі. Але коли сталася пандемія, можна зауважити очевидні зміни в тому, як оператори програм-вимагачів здійснили свої атаки.

Зловмисники, які хочуть отримати доступ до цільових організацій, тепер зосереджуються на викритих послугах та на стороні обслуговування. Гібридна робота, модель, у якій працівники працюють обома віддалено та на місці, стає новою нормою для організацій, передбачається, що ця тенденція продовжуватиметься в наступний рік. Модель гібридної роботи має багато переваг, таких як підвищена гнучкість і продуктивність, але він також має деякі незаперечні мінуси кібербезпеки.

Через збільшену поверхню атаки з менш захищених домашніх робочих середовищ і серверів, важко точно визначити, наскільки шкідливі зловмисники приходять і здійснюють атаки — і як команди з кібербезпеки можуть зупинити програми-вимагачі атакує в нульовий час.

Виходячи з інцидентів безпеки, які спостерігали цього року, також очікується великий розвиток програм-вимагачів у наступному році. По-перше, атак програм-вимагачів стане більше цілеспрямовані та дуже помітно, що ускладнює для підприємств захист своїх мереж і системи проти цих атак. Оскільки сучасне програмне забезпечення-вимагачів є відносно новим, можливо підприємствам ще належить зробити такі ж інвестиції в захист серверів від програм-вимагачів та захист як вони зробили для кінцевих точок. Крім того, постійно бракує кваліфікованих фахівців з кібербезпеки є обтяжуючим фактором щодо захисту організацій від загроз програм-вимагачів.

TTP, які використовуються операторами програм-вимагачів, швидше за все, залишаться незмінними, але їх використовуватимуть для подальшого переслідування комплексних цілей, які, можливо, будуть більшими, ніж основні цілі попередніх років.

Друга подія, яка передбачається, полягає в тому, що оператори програм-вимагачів також використовуватимуть більш сучасні і складні методи вимагання, які будуть нагадувати сучасну постійну загрозу національній державі (APT) атаки. Коли зловмисники зможуть проникнути в середовище своїх жертв, вони можуть просто викрасти конфіденційні дані та перейти безпосередньо до вимагання своїх жертв, пропускаючи шифрування або крок блокування доступу взагалі.

З погляду основного засобу успішного вимагання, спрямувати фокус на відмови в доступі до критично важливих даних на користь витоку та видобутку вкрадених даних озброєння. Вектори атак, які оператори програм-вимагачів використовують для націлювання на підприємства, наприклад віртуальні приватні мережі (VPN), фішингові електронні листи та відкриті порти протоколу віддаленого робочого столу (RDP), залишиться. Однак у 2023 році хмара ставатиме мішенню частіше. Оскільки все більше підприємств мігрують у

хмару, вони приносять із собою свої конфіденційні дані та ресурси, спонукаючи кіберзлочинців до викрадення.

Крім використання передових методів безпеки для забезпечення безпеки серверів, підприємства отримають вигоду в дотримання вказівок із захисту серверів для всіх відповідних операційних систем і програм. Забезпечення правильного налаштування серверів допоможе захистити підприємства від програм-вимагачів атак та інших загроз.

Оскільки сервери мають передбачуваний набір програм на основі їхніх конкретних ролей, це також доцільно для організацій, які використовують контроль додатків. Ця практика безпеки дозволяє блокувати програми або обмежити додатки, за винятком тих, які IT-команди внесли в безпечний список.

Використання вразливостей. Треба стати більш пильними, маючи справу з рекордно високим рівнем експлойтів нульового дня, знайденими в 2021 році, підприємства мають підвисити готовність щодо потенційних прогалин у систем, оскільки ще більше вразливостей очікується, що будуть знайдені.

Наступний рік має побити історичний рекорд експлойтів нульового дня, які допомогли сформувати ландшафт загроз 2021року: 66 експлойтів нульового дня були знайдено. Прогнозується, що в 2023 році буде виявлено ще більше експлойтів нульового дня, що не обов’язково вказуватиме на погіршення якості коду, а скоріше буде підживлюватися різними факторами. Ці фактори включатимуть зростання інтересу ЗМІ у висвітленні експлойтів, що створюють заголовки, шукачі вразливостей, зацікавлені в прибуткових винагородах за помилки, подібно до тих, які пропонує Zero Day Initiative (ZDI) для запобігання атакам нульового дня, а також помилки впровадження та недогляди, які виникатимуть, коли все більше компаній переходитимуть на цифрові технології.

Можливо, буде знайдена лише частина активно експлуатованих уразливостей галуззю кібербезпеки, тому виявлення більшої кількості вразливостей також вказуватиме на все більше ефективні методи виявлення та

зміни ставлення до розкриття інформації. Програми винагород за помилки досягла великих успіхів у напрямку раннього виявлення вразливостей на користь підприємств, як свідчить про те, як стимули ZDI сприяли розробці віртуальних патчів для клієнтів рішення безпеки, в середньому на 81 день випереджаючи публічні дані постачальника.

Однак ці вразливості можуть використовуватися максимально швидко, швидкість розгортання вразливості можуть зменшити до кількох днів або навіть годин, і експлойт буде написаний та використаний для систем в бета-версії, перш ніж її можна буде залатати та випустити патч для користувачів.

Проміжок виправлення — час між виявленням уразливості та розгортанням виправлення, це — залишатиметься золотою жилою для намірливих зловмисників, які, без сумніву, розраховуватимуть на затримки розгортання критичних виправлень помилок, щоб дати їм достатньо часу для розробки своїх дій. Запізнення з графіком розгортання патчів може статися, коли виправлення помилок потрібно пройти тестування в програмному забезпеченні, як це було у випадоку, коли користувачам веб-переглядача було надано виправлення для механізму JavaScript Google Chrome V8 з випуском Chrome 77 у вересні 2019 року, через місяць після того, як помилку V8 уже було виправлено.

Це поставить підприємства у важке становище, оскільки вони стикаються з двосторонньою проблемою передбачення прискорених експлойтів протягом періоду очікування виправлень помилок і впровадження їх як тільки вони будуть розгорнуті. Усунення цих вразливостей не є єдиним процесом; наприклад, виправлення кінцевих точок більш оптимізоване, ніж виправлення серверів, що часто спричиняє більше часу простою та витрати.

Замість того, щоб активно вивчати фрагменти коду на наявність недоліків, зловмисники почнуть звертатися до виправлень, оскільки це зручні покажчики на діри в системі, за якими вони можуть адаптувати свій код шкідливого ПЗ. У

2022 році спеціальний сегмент кіберзлочинців пильно стежитиме за компаніями в очікуванні будь-якого розкриті вразливості та розгорнутання виправлення, які допоможуть їм прискорити свої атаки.

Зловмисники не просто планують скористатися нещодавно знайденими вразливими місцями, але й продовжуватимуть використовувати старі недоліки.

Це ще більше підкреслить потребу підприємств та їхніх партнерів, постачальники мають визначити пріоритетність керування виправленнями. Уразливості, виявлені в попередні роки, залишаться актуальними, зловмисники не змінюючи ціль можуть їх об'єднають, щоб посилити свої атаки в наступному році.

Так само буде наплив змішаних атак, які будуть націлені на кілька програмних продуктів одночасно шляхом послідовного з'єднання, наприклад, уразливості в Google Chrome з уразливістю в Microsoft Windows, щоб отримати привілейований доступ до систем. Перевагою цього майбутнього зростання кількості атак є те, що це неминуче приверне увагу аналітиків безпеки до менш вивчених поверхонь атак. Передбачається більше досліджень, присвячених серверним технологіям, які можуть пролити світло на слабкі місця в такі платформи, як Microsoft Exchange і SharePoint, пом'якшуючи вплив будь-яких майбутніх атак на їхніх кінцевих користувачів.

Хмарна безпека також має бути пріоритетом для підприємств, багато з яких стали прихильниками хмарних технологій після пандемії, які прискорили свою цифрову трансформацію. Залежність багатьох хмарних проектів, побудованих на програмному забезпеченні з відкритим кодом, можуть залишити їх відкритими до атак, які накопичують відомі вразливості, оскільки ці бібліотеки часто не оновлюються або регулярно перевіряються на наявність публічно оприлюднених недоліків. Для команд безпеки пошук надійних джерел хмарних недоліків будуть корисними для захисту хмарних активів, оскільки

залишається брак пов’язаних із хмарою та звіти про загальні вразливості та ризики (CVE) щодо локальних помилок.

Підприємствам, як ніколи, потрібно буде переконатися, що їхні команди IT-безпеки мають навики адаптуватись і виправити цей неминучий сплеск експлойтів. Це передбачає надання цим командам підтримку та ресурси, які їм знадобляться для проведення інвентаризації пристроїв в IT-середовищі управління активами, відстежування оновлення безпеки від постачальників, щоб вони могли якнайшвидше відповісти уразливості, і практикувати віртуальне виправлення або ізоляції машини для захисту будь-якої точки входу потенційної загрози.

Масовані атаки шкідливим ПЗ. Підприємства залишаться прибутковою здобиччю для операторів програм-вимагачів, які шукають величезних виплат, але заголовки подвигів мисливців за великою дичиною залишать лише малих і середніх компаній (SMB), готових до вибору серед дочірніх компаній програм-вимагачів як послуги (RaaS) і дрібних кіберзлочинців, які користуються товарним зловмисним програмним забезпеченням і залишаються невідомими.

Протягом останніх кількох років увага громадськості була прикута до програм-вимагачів, а програми-вимагачі вважається типом товарного зловмисного програмного забезпечення та моделлю як послуги. Але інші готові типи зловмисного програмного забезпечення, такі як трояни віддаленого доступу (RAT), викрадачі інформації, майнери криптовалюти, дроппери та завантажувачі шкідливих програм будуть циркулювати в колах кіберзлочинців. Це підштовхне товарний ринок шкідливих програм перетвориться на підступну, але грізну загрозу.

Оператори програм-вимагачів скористалися інструментами зловмисного програмного забезпечення, щоб зробити свої атаки ефективнішими, а інші зловмисники використовували атаки для запуску політично мотивованих кампаній. Оператори програм-вимагачів також спостерігали за використанням

шкідливих програм, таких як Cobalt Strike, Koadic, PowerShell Empire і Metasploit разом із наявними утилітами системного адміністрування — техніка під назвою «жити за рахунок землі» — щоб уникнути виявлення.

Ці інструменти мають більш розширені функції та доступні ціни, що створює таке шкідливе програмне забезпечення доступні для зловмисників, які прагнуть розширити свій інструментарій. Багато налаштованих частин зловмисного програмного забезпечення зрештою комерціалізується в підпіллі кіберзлочинців для використання іншими зловмисниками, що дає змогу передбачити наступне покоління кіберзлочинців як більш інноваційне і краще оснащене, ніж той, хто відповідав за розробку програм-вимагачів близько 15 років тому.

Прогнозується, що ринок інструментів атаки на товари не тільки розвиватиметься разом з початківцями зловмисниками, але також дасть їм засоби для розширення своїх мереж і з'єднання з ними кіберзлочинці-однодумці. Зрештою, продавці не лише надають готове до використання шкідливе програмне забезпечення, але й також підсолодили угоду інструкціями, порадами та посібниками з усунення несправностей.

Сервісна модель, у якій товарне шкідливе програмне забезпечення продається як частина контрактів на обслуговування, а не як одноразове придбання зловмисного програмного забезпечення, добре підійде зловмисникам нижчого рівня, які мають завершити навчання від потреби в інструментах зловмисного програмного забезпечення до пошуку надійних партнерів у злочинах, коли вони стають більш досвідченими нападники.

Така співпраця призведе до більш стійкої злочинної діяльності, про що свідчить, зловмисники змогли відновити ботнет шкідливого програмного забезпечення Emotet, використовуючи ботнет банківської системи. Троян Trickbot, лише через кілька місяців після ліквідації власної інфраструктури Emotet правоохоронними органами. Прогнозується, що атаки на товари

досягнуть пікової точки у 2022 році, зловмисники не матимуть потреби в розробці спеціального шкідливого програмного забезпечення, зловмисне програмне забезпечення знадобиться, щоб краще керувати їхніми афілійованими компаніями в складній цілеспрямованій атаці.

Враховуючи це, простір зловмисного програмного забезпечення давно назріває для більш складної пропозиції за допомогою якого зловмисники можуть покращити свій арсенал. У наступних роках, швидше за все, відбудеться дебют ботнет як послуга, призначений для компрометації та контролю як хмарних платформ, так і платформ Інтернету речей одночасно, дуже схоже на розширену версію ботнету ZeuS.

Цілком можливо, що такий інструмент вийде з російськомовного набору кіберзлочинного підпілля, завдяки своїй сумнозвісній інноваційної сцени зловмисного програмного забезпечення, але ботнет FreakOut також має бути конкурентом, оскільки продовжує розвиватися з додатковими функціями.

Передбачається, що ринок атак на товари, бізнес-модель якого базується на створенні коду зловмисного програмного забезпечення робота замість того, щоб зловмисник рухався всередині мережі, будучи в основному неефективним проти більш надійних засобів захисту, які частіше зустрічаються в корпоративних налаштуваннях, наприклад системи безпеки, які використовуйте машинне навчання. Прогнозується, що інструменти зловмисного програмного забезпечення для товарів і послуг матимуть більший успіх у 2023 році, націлившись на малий і середній бізнес, які будуть використовуватися зловмисниками, які сподіваються менше стикатися з захистом від своїх цілей і менша конкуренція з боку інших кіберзлочинців. Зокрема, передбачається, що пристрої IoT, які використовуються малим і середнім бізнесом, стануть основними цілями для таких атак. Тому малий і середній бізнес буде повинні бути більш розбірливими при виборі постачальників, купуючи свої пристрої IoT у виробників які мають солідну історію виправлень.

У малих і середніх підприємствах рідко є спеціалізовані групи безпеки, а коли вони є, ці команди, швидше за все, обмежені через обмежене фінансування, в якому кібербезпека є лише операційними витратами. Глобально витрати на кібербезпеку мають перевищити 150 мільярдів доларів США до кінця 2021 року, але малий і середній бізнес витрачає лише понад 40 мільярдів доларів США щорічно на рішення IT-безпеки. Через обмеження бюджету багато малих і середніх підприємств зроблять безпеку кінцевих точок своїм головним пріоритетом, а потім захист своєї мережі.

Однак деякі підприємства малого та середнього бізнесу можуть бути навіть більш підготовленими, ніж інші. Ті, що більше онлайн-сервіси, що значною мірою покладаються на хмарні сервіси та платформи, будуть більше обізнані, це пов’язано з використанням зловмисного програмного забезпечення для їх критично важливих операцій, через характер їх бізнесу. Ці компанії, швидше за все, зроблять безпеку частиною свого порядку денного, враховуючи рішення з кібербезпеки як частину собівартості продажів.

Загрози Інтернет-речей. Інформація, пов’язана з IoT, стане гарячим товаром у підпіллі кіберзлочинців, стимулюючи підприємства пам’ятати про прогалини в безпеці, які можуть призвести до витоку або підробці даних. Розумні пристрої вже давно є спокусливими речами в очах зловмисників, які розраховують на факт що обмежена обчислювальна потужність більшості пристроїв IoT залишає мало місця для вбудованої безпеки. Зламані пристрої IoT використовувалися в різних видах атак, наприклад, у атаках на розподілену відмову в обслуговуванні (DDoS).

Залишатися конкурентоспроможними або принаймні працювати під час глобального карантину, прогнозується, що компанії, особливо ті, хто займається інтелектуальним виробництвом, піддадуться більшій кількості кіберзагроз у міру переходу перейти до гібридної моделі роботи та продовжувати використовувати служби віддаленого підключення.

Щоб зберегти свою діяльність герметичною, більше підприємств, чия робоча сила покладається на пристрої IoT, звернуться до систем запобігання та виявлення вторгнень (IPS/IDS), інструментів мережевої експертизи (NFT), мережі інструменти виявлення аномалій поведінки (NBAD), а також інструменти виявлення та реагування мережі (NDR). Може допомогти їм уважно стежити за тим, що відбувається в їхніх мережах. Хмарні користувачі, які покладаються на сторонніх постачальників безпеки, повинні будуть пильно відстежувати використання ними хмарних ресурсів для будь-якої аномальної активності, захищати свою віртуальну приватну хмару (VPC) від атак які можуть виникнути в їхній хмарній інфраструктурі, і переглянути можливості потенційних постачальників, щоб переконатися, що вони відповідають їхнім потребам.

Але в 2023 році зловмисники матимуть більш високі прагнення, які виходитимуть за межі викрадення гаджетів Інтернету речей, як зручною базою для атаки для їхньої злочинної діяльності або як засіб пересування всередині мережі. Кіберзлочинці незабаром приєднаються до золотої лихоманки, оскільки все більше виробників автомобілів, включаючи відомих гравців як General Motors, Honda і Toyota — заробляють на трафіку даних, що доставляється підключеними автомобілями. Ці транспортні засоби оснащені набором камер, лазерів та інших датчиків, які разом реєструють умови водіння та поведінку водія, включно зі швидкістю та відстанню автомобіля, а також види розважальних засобів масової інформації, якими користуються його пасажири.

Цих статистичних даних у реальному часі є безліч бізнес-додатків для комерційних клієнтів, таких як вимірювання успішності реклами, вимірювання споживчий попит, а також визначення знижок на автострахування на основі даних про водіння. Ці дані також можуть бути використані для моніторингу продуктивності компонентів автомобіля, які покращить свої власні ланцюжки поставок.

Очікується, що попит на інформацію про розумні автомобілі стане новим бізнесом, який швидко розвивається, до 2030 року оцінюватиметься приблизно в 450–750 мільярдів доларів США без жодних ознак втрати потужності. Прогнозується, що до 2025 року щомісяця надходитимуть 10 ексабайт даних від підключених автомобілів. Розумна архітектура автомобіля також може бути далі оптимізовано, якщо його більш складні функції та процеси збору даних переходять до хмари — фактично, багато програм і систем, які використовуються в нових моделях розумних автомобілів, уже розміщені на внутрішніх хмарних серверах, але це може відкрити для автовиробників загрози, таких як атаки відмови в обслуговуванні (DoS) і атаки типу "людина посередині" (MitM).

Якщо вони хочуть підготувати свою продукцію до майбутнього, виробникам автомобілів у 2023 році потрібно буде з ними тісно співпрацювати, постачальники засобів безпеки спільно вирішують, як вони хочуть запровадити безпеку. Приклади цього партнерство вже налагоджено. Були такі перші ініціативи, як Open EV Software. Платформа, очолювана консорціумом Mobility in Harmony (MIH) та його партнерами, Arm, Microsoft. Існує також співпраця між Volkswagen і Microsoft, яка прагне створити хмарну платформу, яку виробники автомобілів зможуть використовувати для розробки більш просунутих і безпечних рішень для автоматизованого водіння для підключених автомобілів.

Більше подібних проектів заклали б основу для автомобільної промисловості розробити спеціальну операційну систему для розумних транспортних засобів з кінцевою метою автомобільної екосистеми, побудованої на єдиній операційній системі, яка зробить це можливим у майбутньому моделі підключених автомобілів будуть оснащені стандартизованими функціями безпеки.

Атаки на ланцюги поставок. Глобальні ланцюги поставок будуть опинятись під прицілом техніки чотириразового вимагання, оскільки компанії розвивають свою пропозицію ланцюгові операції.

Пандемія Covid-19 яскраво просвітила крихкість ланцюгів постачання. Масовий економічний дефіцит і затримки виникли через кілька факторів, включаючи підвищений попит, доставку дефіцит контейнерів і працівників, і багаторічна залежність від ощадливіших систем виробництва. Коли проблеми з ланцюгом поставок почали ставати всесвітнім тягарем, вартість ланцюгів постачання також почала ставати ще більш очевидною — не лише для підприємств, що перебувають у скрутному становищі, але також і для кіберзлочинців, яких не лякають, а радше підживлюють глобальна пандемія. Зокрема, атаки на ланцюги поставок дедалі більше взаємопов'язані з кампанії програм-вимагачів минулого року, прикладом яких є гучні атаки REvil/Sodinokibi на великі організації, включаючи Quanta Computer, JBS Foods і Kaseya.

Зловмисники, користуючись і посилюючи значний збій у ланцюзі поставок, ще більше спричинять сплеск моделі чотириразового вимагання у 2023 році. Вони максимально використають свої кібератаки на відомих жертв з метою сплати великих сум грошей у чотирикратному розмірі: зберігання важливих даних жертви з метою отримання викупу, погроза витоку даних та оприлюднити порушення, погрожуючи переслідувати клієнтів жертви та нападати на постачання мережі жертви або продавців.

Минулого року кіберзлочинна група DarkSide націлилася на Colonial Pipeline, найбільшу нафтопереробну система трубопроводів у США. Група перешкоджала компанії отримати доступ до її комп'ютерних систем і викрала понад 100 ГБ корпоративних даних. Було помічено, що група постійно впроваджуючи інноваційні стратегії атак, пропонуючи як DDoS. Роблячи це дає змогу філіям DarkSide запускати чотирикратні методи вимагання, які можуть сильно вплинути на пропозицію ланцюгів постачання. Отже, зловмисники

можуть заборонити доступ до критично важливих даних, таких як виробництво, забороняти доступ до машин, що використовуються у виробництві, або зв'язуватися з клієнтами та зацікавленими сторонами, тиснути на організації, які постраждали, щоб вони заплатили.

Ланцюги поставок також будуть у центрі уваги брокерів доступу як послуги (AaaS). Коли вразливе середовище скомпрометоване, брокери AaaS можуть продавати доступ до мережі компанії, адміністративні облікові записи та облікові дані автентифікації для кіберзлочинців за різними цінами.

Економічні зрушення, викликані пандемією, змусять підприємства інвестувати у свій ланцюг поставок. Вони зосередяться на створенні більш надійних операцій ланцюга поставок за допомогою засобів диверсифікації.

Протягом багатьох років країни віддавали перевагу глобалізації, яку критикували як причиною надмірної залежності багатьох країн від отримання поставок з одного географічного джерела. Замість глобалізації операції в ланцюзі постачання перейдуть до регіоналізації, що допоможе забезпечити ці підприємства задовольняти підвищені вимоги та нестабільні виробничі витрати.

Диверсифікація стратегії будуть відрізнятися для всіх компаній — одні ланки в ланцюжку поставок будуть локальними, інші — локальними перебувати в різних країнах або регіонах.

Однак диверсифікацію непросто здійснити належним чином і безпечно; це може бути дорогим і ресурсомістким зусиллям. Оскільки організації шукають постачальників, які знаходяться ближче до дому, щоб зменшити економічні ризики та допомогти зберегти бізнес на плаву, вони також можуть бути мимоволі відкривати двері для ризиків безпеки. Довгострокові постачальники, з якими вони працюють роками будуть замінені новими компаніями, які їм потрібно буде оцінити. Ці нові постачальники можуть пропонувати хмарні програми та послуги з політикою безпеки, яка може бути не на належному рівні або взагалі не надавати пріоритет хмарній безпеці.

Період, протягом якого дві організації узгоджують свої процеси, є критичним — і зловмисники можуть здійснювати цілеспрямовані атаки, щоб скористатися змінами та незнайомістю, пов’язаними з новим партнерством.

Наприклад, зловмисник може видати себе за когось із нового постачальника та надіслати фішинговий електронний лист із проханням до одержувача заповнити відповідну інформацію про компанію.

Щоб підтримувати безпеку ланцюгів постачання, коли компанії розвивають свої стратегії, їм слід застосовувати нульовий підхід довіри в їхній практиці безпеки.

Модель нульової довіри допомагає захистити спосіб, у який організації взаємодіють з іншими компаніями та обмінюються даними за допомогою постійної перевірки протягом усього терміну служби підключення. Завдяки цій моделі організації можуть бути впевнені, що здоров’я користувачів, пристроїв, програм і служб, з якими вони взаємодіють, постійно контролюється та оцінено.

3. МОДЕЛЬ УПЕРЕДЖЕННЯ ЗАГРОЗ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

3.1 Загальний принцип захисту комерційних компаній

Потужна колекція рішень безпеки для боротьби з сучасними загрозами повинна включати:

- **Брандмауер**: перша лінія захисту від зовнішніх загроз, брандмауер запобігає проникненню зловмисного трафіку у внутрішню мережу.
- **Захист від зловмисного програмного забезпечення**: як правило, це інструмент на основі кінцевої точки, програми для захисту від зловмисного програмного забезпечення сканують вхідні програми, повідомлення та документи, щоб переконатися, що вони не заражені шкідливим програмним забезпеченням.
- **Тестування на проникнення та аналіз уразливості мережі**: вони перевіряють вашу мережу, щоб оцінити рівень безпеки.
- **Виявлення вторгнень**: аналоги інструментам тестування на проникнення, ці інструменти контролюють вашу мережу, щоб визначити, чи зловмисник успішно порушив периметр мережі.
- **Автентифікація**: сучасні версії цих систем використовують для виявлення незвичайної поведінки користувачів, щоб визначити, штучний інтелект чи є користувачі тими, за кого себе видають.
- **Аудит паролів**: ці інструменти сповіщають користувачів і системних адміністраторів про необхідність змінити паролі, якщо виявляється, що їх легко зламати.
- **Шифрування**: якщо зловмисник проникає у мережу або втікає за допомогою апаратного забезпечення, шифрування може запобігти доступу до конфіденційних даних.
- **Хмарні системи безпеки**: ці інструменти спеціально розроблені для захисту хмарних ресурсів, на відміну від даних, що зберігаються в локальних системах.

Також, всіма цими інструментами має керувати здатна та добре навчена команда безпеки (SOC) разом із сильною стратегією кібербезпеки.

Кібербезпека розвинулася, щоб протистояти безлічі загроз і атак, з якими типове підприємство стикається щодня. Деякі з найкращих практик захисту підприємства включають:

- **Перевірте свої системи та задокументуйте свій режим безпеки**: почніть із детального аудиту кожної системи в мережі, рівня ризику, який вам загрожує в разі атаки, і того, як ви збираєтеся захистити свої дані.
- **Розкажіть користувачам про реалії фішингу**: фішинг залишається основним шляхом для зловмисників отримати доступ до мережі. Багато чому цьому можна запобігти, якщо користувачів ознайомити з тим, як працює фішинг, на що слід звернути увагу та поведінки, якої слід уникати.
- **Аудит паролів і примусове використання надійних паролів**: слабкі паролі неймовірно легко зламати, включаючи всі «словникові слова». Навіть кілька слів із цифрами, які замінюють схожі на вигляд літери, або слова з цифрами в кінці більше не вважаються безпечними. Як пише криптограф Брюс Шнайер , «практично все, що можна запам’ятати, можна зламати».
- **Інвестуйте в інструменти кібербезпеки**: системи захисту, описані в попередньому розділі, є важливими інструментами для компаній будь-якого розміру. І ви повинні мати план їх розгортання.
- **Слідкуйте за третіми сторонами**: якщо ви працюєте зі службами хмарних обчислень, важливо стежити за порушеннями безпеки та будь-якими вразливими місцями, пов’язаними зі службою, і переконатися, що ваші дані належним чином захищені.

- **Релігійно створюйте резервні копії даних**. Переконайтеся, що резервні копії виконуються щодня (або частіше) і зберігаються в окремому місці, захищеному унікальними обліковими даними для входу.

Які існують способи запобігання кібератаці?

Запобігання кібератакам вимагає постійної старанності та пильності. Ці поради допоможуть захистити вас:

- **Зрозумійте свій рівень ризику**: малий бізнес і середній споживчий бізнес без значних цінних цифрових активів все ще знаходяться під загрозою атаки. (Лише минулого року 47% малих підприємств зазнали кібератаки.) Якби ваша компанія втратила всі свої цифрові дані за одну ніч через кібератаку, чи змогли б ви продовжувати працювати? Як би ти видужав?
- **Навчання має вирішальне значення**: гарантія того, що всі співробітники розуміють ризики, а також найкращі практики та політику безпеки значною мірою допоможуть захистити організацію.
- **Виправлення всього програмного та апаратного забезпечення:** успішні експлойти зазвичай трапляються, коли підприємство не може застосувати патч (частина програмного забезпечення, яка виправляє вразливість), навіть якщо патч уже випущено.
- **Заблокуйте фізичний доступ**: уся цифрова безпека у світі буде неефективною, якщо злодій зможе фізично проникнути у вашу будівлю та викрасти обладнання.
- **Пропонуйте доступ лише до необхідних ресурсів**: працівникам відділу маркетингу не потрібен такий же рівень доступу до мережі, як персоналу бухгалтерії. Розділіть доступ до послуг і надайте його лише за потреби.
- **Встановіть заходи безпеки та регулярно перевіряйте системи**: запуск набору засобів моніторингу мережі, захисту від зловмисного програмного забезпечення та виявлення вторгнень може значною мірою допомогти

запобігти кібератакам. Регулярно перевіряйте свої системи моніторингу безпеки, щоб переконатися, що вони працюють належним чином.

Кібератаки, безсумнівно, продовжуватимуть посилюватися, особливо враховуючи те, що компанії на постійній основі використовують протоколи роботи з дому. Згідно з одними оцінками, загальна вартість кіберзлочинності в усьому світі до 2025 року перевищить 10 трильйонів доларів США.

Потреба захистити підприємство в кожній потенційній точці входу ставатиме все більш важливою з часом, а зловмисники продовжуватимуть змінювати свою тактику. Тим часом ризик зростає, а збитки від успішних атак зростають. Забігаючи вперед, стає зрозуміло, що кожне підприємство має зробити безпеку першочерговою турботою.

3.2 Модель запобіганню загроз

Збільшене навантаження покладається не лише на IT-відділ, але й на внутрішню службу ризиків. Бізнес-лідери роблять стратегічний вибір щодо інвестицій, технологій, ресурсів і навичок, необхідних для ведення цифрового бізнесу, і все це матиме вплив на побудуванні стратегії цифрових ризиків та має вирішальне значення для її успіху. Негайним кроком для організацій є наявність надійних заходів щодо короткострокової прибуткової та довгострокової життєздатності кібербезпеки, а найпростішим підходом є виконання типової оцінки інформаційної безпеки та/або кібербезпеки систем.

Питання, на які необхідно відповісти: «Чи достатньо цього? Чи є питання кібербезпеки єдиним ризиком для цифрової організації?» їхніх компаній. Ці стратегічні рішення неминуче містять елемент ризику. Водночас бізнесу доводиться протистояти зовнішнім загрозам. Наприклад, у міру того, як підприємства зазнають цифрової трансформації та все більше їхніх активів стають цифровими, зростає загроза кіберзлочинності та ризики щодо конфіденційності даних.

Хоча цифрова трансформація створює великі можливості для організацій, вона також вводить новий вимір до традиційного погляду на ризик.

На даний момент групи управління ризиками залишаються на основі реагування з переважним фокусом на традиційних загальних заходах IT-контролю та методах оцінки ризиків, і обмежені процесами, системами та більш широким бізнес-розумінням, яким вони оснащені. Оскільки технологічні перетворення змінюють ландшафт ризиків, організаціям потрібно буде розробити абсолютно новий підхід до цифрових ризиків.

Потужність і цінність Індустрії 4.0 полягає в потоках інформації та можливості інтегрувати цифрову інформацію з багатьох різних джерел і місць, щоб керувати фізичним актом ведення бізнесу. Таким чином, інформація тече в безперервному циклі, де дані з одного процесу інформують наступний. Цей постійний цикл включає використання багатьох фізичних і цифрових технологій, включаючи аналітику, адитивне виробництво, робототехніку, високопродуктивні обчислення, обробку природної мови, штучний інтелект і когнітивні технології, передові матеріали та доповнену реальність.

На малюнку нижче показано, як потік інформації відбувається через ітераційну серію з трьох кроків, що називається циклом фізично-цифрово-фізично (PDP).

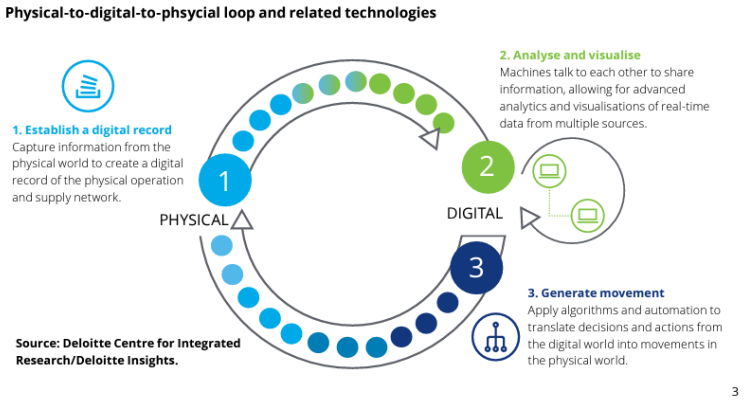

Рисунок.5 Цикл фізично-цифрово-фізично

Це створює нові ризики, наприклад, здатність цифрового середовища проводити розслідування у випадку шахрайства або порушення безпеки, включаючи збір доказів даних, які можна представити в суді.

Потрібно створити забезпечення захисту даних у всій цифровій екосистемі на різних етапах життєвого циклу даних — даних у використанні, даних у дорозі та даних у спокої.

1. Встановіть цифровий запис. Збирайте інформацію з фізичного середовища для створення цифрового запису фізичної роботи та мережі постачання.
2. Аналізуйте та візуалізуйте. Машини спілкуються одна з одною, щоб обмінюватися інформацією, забезпечуючи розширену аналітику та візуалізацію даних у реальному часі з багатьох джерел.
3. Створіть рух. Застосуйте алгоритми та автоматизацію, щоб перевести рішення та дії з цифрового світу в рухи у фізичному середовищі.

Основні виклики, які спостерігаються в цифровому середовищі:

- формулювання детальної цифрової стратегії.
- оцінка доцільності існуючої IT-платформи.
- відповідність законодавчим і нормативним вимогам.
- визначення та використання відповідних цифрових талантів.

Цифровізація означає різні речі для різних зацікавлених сторін.

Погляд компанії:

- Стратегія та бачення: визначте цифрове бачення та стратегію.
- Впровадження: перетворення інструментів і можливостей, які використовуються для надання послуг.

- Управління програмою: зосередьтеся на своєчасному та економічно ефективному впровадженні цифрової ініціативи для відповідних бізнес-команд.

Погляд на ризики:

- Контекстний ризик: адекватність вибору цифрових активаторів цифрової програми в контексті бізнес-цілей.
- Ризик впровадження: архітектура, заснована на ризиках, для цифрових інструментів, а також технології, операції, постачальники, відповідність, безпека та стійкість.
- Ризик управління: ефективне управління цифровими трансформаціями для забезпечення міжфункціональної синергії та усунення ризиків, що виникають через взаємозалежні процеси.

Існує 10 сфер ризику: стратегічний, технологічний, операційний, сторонній, регуляторний, криміналістичний, кібернетичний, стійкість, витік даних і конфіденційність — як ландшафт ризиків у будь-якій цифровій екосистемі. Виходячи з застосованих зон ризику для цифрових ініціатив, необхідно розробити різні заходи контролю відповідно до провідних стандартів і галузевих практик.

Критичним аспектом у визначенні засобів контролю є врахування характеру та рівня цифровізації операцій, оскільки більшість із цих сфер перебувають на стадії зародження та тісно пов’язані з системами або ручними процесами, тому можуть існувати обмеження для впровадження засобів контролю.

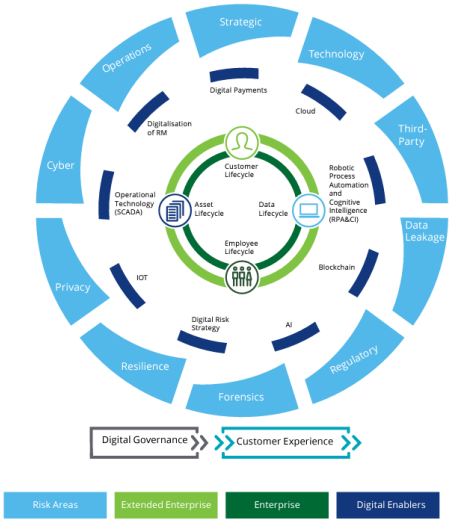

Рисунок.6 Фреймвор цифрового ризику

Розуміння зон ризику має вирішальне значення для виявлення та боротьби з усіма ризиками, яким може наражатися організація в цифровому середовищі. Далі коротко пояснюються всі сфери ризику, розглянуті в структурі:

1. **Технології.** Потенціал збитків через технологічні збої або застарілі технології. Технологічні ризики впливають на системи, людей і процеси. Ключові області ризику можуть включати масштабованість, сумісність і точність функціональності впровадженої технології
2. **Третья сторона.** Включає ризики, що виникають через невідповідні засоби контролю в операційному середовищі постачальників/третіх сторін. Ключові засоби контролю стосуватимуться обміну даними, інтеграції технологій, залежності операцій, стійкості постачальників тощо.
3. **Кібернетика.** Захист цифрового середовища від несанкціонованого доступу та забезпечення конфіденційності та цілісності технологічних систем. Основні засоби контролю можуть включати посилення платформи, мережеву архітектуру, безпеку програм, керування вразливістю та моніторинг безпеки.

4. **Конфіденційність.** Ризик, що виникає через неналежне поводження з особистими та конфіденційними персональними даними клієнта/співробітника, що може вплинути на конфіденційність особи. Основні засоби контролю включають повідомлення, вибір, згоду, точність та інші принципи конфіденційності.
5. **Стратегічність.** Зазвичай випливає з цілей і завдань організації. Він може бути зовнішнім по відношенню до організації і, коли виникає, змушує змінити стратегічний напрямок організації. Як правило, це вплине на досвід клієнтів, вартість бренду, репутацію та конкурентну перевагу на ринку.
6. **Криміналістика.** Здатність цифрового середовища для проведення розслідувань у разі шахрайства або порушення безпеки, включно зі збором доказів даних, які можна представити в суді.
7. **Операційний.** Подія, внутрішня чи зовнішня, яка впливає на здатність організації досягати бізнес-цілей за допомогою визначених операцій. Включає ризики, що виникають через неадекватні засоби контролю в операційних процедурах.
8. **Нормативна.** Дотримання законодавчих вимог, включаючи закони про технології, галузеві закони та нормативні акти. Вони включатимуть нормативний універсал електронних комунікацій і транзакцій, який має загальне застосування, і галузеве регулювання, включаючи фінансові послуги, страхування та медичні схеми, наскільки це можливо.
9. **Витік даних.** Забезпечення захисту даних у цифровій екосистемі на різних етапах життєвого циклу даних: дані у використанні, дані в дорозі та дані в спокої. Ключові зони контролю зосереджені на даних. Класифікація, збереження даних, обробка даних, шифрування даних тощо.

10. **Стійкість.** Ризик збою в роботі або недоступності послуг через високу залежність від тісно зв’язаної технології. Ключові сфери розгляду включають безперервність бізнесу, аварійне відновлення IT/мережі, відмовостійкість і управління кризовими ситуаціями.

Портфель цифрових ризиків. Приклад портфеля послуг для зменшення ризиків, пов’язаних із цифровими засобами:

1. Стратегія цифрових ризиків. Створення структури управління для усунення ризиків під час впровадження цифрових програм.
2. Хмара. Розуміння та управління ризиками впровадження державних/приватних/гібридних хмарних технологій для інфраструктури, платформи та програмного забезпечення.
3. Blockchain. Використання архітектури Blockchain для захисту від внутрішніх і зовнішніх загроз.
4. RPA. Забезпечення безпечної реалізації RPA та використання RPA для кібербезпеки та управління ризиками.
5. IoT. Розробка архітектури IoT на основі ризиків для збору даних і керування віддаленими системами.
6. OT (SCADA). Захист інфраструктури OT за допомогою безпечної інтеграції з екосистемою корпоративних технологій.
7. Цифрові платежі. Захистіть пропозиції цифрових платежів, використовуючи структурований підхід, що ґрунтується на ризиках.
8. Стратегія ризиків штучного інтелекту. Забезпечення впевненого впровадження та впровадження штучного інтелекту.
9. Цифровізація RM. Забезпечення управління ризиками за допомогою цифрових технологій.

Навігація підходу цифрових ризиків для створення ефективного управління ризиками в цифровому середовищі:

1. Виявлення. У відповідності з цифровим баченням організації вивчіть вибір цифрових інструментів і проаналізуйте контекст, щоб оцінити цифровий слід і його вплив.
2. Розроблення. На основі фреймворку розробітт цифрову архітектуру, орієнтовану на оцінку ризиків, адаптовану до цифрових потреб організації та операційного середовища.
3. Впровадження. В контексті бізнесу впровадження цифрової архітектури, заснованої на оцінці ризиків, для вибраних цифрових інструментів, що підтримується загальним управлінням ризиками.
4. Моніторинг. Впровадьте постійний процес перевірки, який розвивається у відповідь на збої та нові розробки в цифровій сфері, законодавчі та нормативні вимоги.

Підхід до управління цифровими ризиками має починатися з розуміння цифрового сліду організації та створення реєстру цифрових ризиків на основі системи цифрових ризиків:

1. Підтримуйте управління ризиками, проводячи семінари та навчання з підвищення обізнаності про ризики. Сприймайте це як проактивну вправу, вбудовуючи її в стратегію організації, а не просто залишаючи її.
2. Періодично відстежуйте, переглядайте та оновлюйте структуру цифрових ризиків, щоб забезпечити повний і точний ландшафт цифрових ризиків.
3. Уможливлення управління ризиками за допомогою інструментів буде доцільним для систематичної ідентифікації та управління еволюцією цифрового ризику.

3.3 Модель запобіганню та протидії вразливості Log4Shell

Щоб знайти IT-фахівця, який не знає про вразливість Log4Shell вам доведеться шукати всюди. Сектор операційних технологій (OT) не є винятком, але точний рівень уразливості для технології OT ще не повністю розкритий.

Уразливість вперше була оприлюднена на початку грудня 2021 року. Оскільки IT-світ продовжує зміцнювати свої мережі для захисту від можливих вторгнень, середовища OT можуть вимагати більш цілеспрямованого підходу.

Потенційний ризик для сектору OT. Хоча ми не знаємо про будь-які опубліковані компроміси OT, вони є легкою мішенню для зловмисників, які хочуть використати Log4j, враховуючи, наскільки він поширений у програмах Java, розроблених за останнє десятиліття.

Один потенційний вектор може бути націлений на компанії, які мають мережі OT. Подумайте про такий гіпотетичний сценарій: зловмисник може отримати початковий доступ до IT-мережі через вразливу програмну систему керування телефоном. Після налаштування цієї системи для роботи в якості проксі-сервера у внутрішній мережі вони можуть виявити вразливу систему журналювання та моніторингу, налаштовану як двосторонню для збору інформації. Маючи доступ до такої системи в обох мережах, зловмисник може почати прямий доступ до технології OT — яка може бути небезпечною за дизайном — або зловмисник може отримати доступ до інженерних робочих станцій, які можуть бути безпосередньо підключені до неавтентифікованих пристроїв OT.

Для всіх типів пристроїв, згаданих у цьому потенційному сценарії, було видано принаймні одне публічне попередження щодо вразливості, пов’язаної з Log4Shell.

Таким чином, уразливість Log4Shell може вплинути на ключові технології, які містять і підтримують системи OT. Деякі з них включають:

- Сервери (наприклад, Historians, межові сервери).
- Робочі станції (наприклад, HMI).
- Мережеве обладнання (міжмережеві екрани, маршрутизатори та комутатори).

- Вбудовані пристрої (наприклад, веб-камери, автомобільні навігаційні системи, паркомати та медичні пристрої).

Дії, які команди безпеки ОТ повинні вжити зараз.

Уразливості Log4Shell (CVE-2021-44228 і CVE-2021-45046) є новими. Найкращі стратегії пом’якшення для середовищ ОТ все ще можна знайти в належному проектуванні та архітектурі системи (наприклад, еталонна модель ISA 62443) або архітектурі нульової довіри. З цією метою наведені нижче критичні міркування щодо обмеження впливу Log4Shell у ОТ:

1. Визначте системи високого ризику та завчасно встановлюйте виправлення, якщо це можливо:

- Системи ОТ, найближчі до корпоративних мереж, піддаються найбільшому ризику і, швидше за все, будуть використані загрозою як опорна точка в ОТ.
- Деякі ключові постачальники ICS вже випустили рекомендації. Надайте пріоритет ідентифікації та виправленню Log4j, використовуючи поради постачальника або активне сканування, здатне ідентифікувати реалізації Log4j.
- Середовище ОТ, як правило, повне обладнання, яке не можна виправити, закінчило життя (EOL), є кібернестабільним або «незахищеним за дизайном». Якщо виправлення неможливе, переконайтеся, що ці системи ізольовано, щоб захищені зони та/або встановлено засоби контролю.

2. Переконайтеся, що як мінімум існує сегментація IT/OT і захист периметра:

- У кібербезпеці ОТ корпоративна зона вважається ненадійною, тому найбільшим заходом зі зниження ризику буде забезпечення того, створення набір правил із найменшими привілеями, що обмеже потік даних між IT та ОТ лише «виправданими для бізнесу» портами/протоколами та джерелами/адресатами.

- Цей набір правил з найменшими привілеями має значно зменшити загрозу від командних і контрольних можливостей Log4j з боку суб'єктів загрози.

3. Моніторинг мережі OT:

- Якщо в мережі OT розгорнуто систему виявлення вторгнень (IDS) і системи мережевого моніторингу, ви можете налаштувати її за допомогою IOC Log4Shell для виявлення та ескалації сповіщень для швидшого реагування на потенційне використання.
- Використовуйте програмне забезпечення для керування журналами, щоб шукати спроби використання.
- Наведене нижче зображення є прикладом пошуку загроз на основі гіпотез за допомогою X-Force Threat Hunting Framework. рекомендуємо командам з кібербезпеки розробити вичерпні списки TTP і виконувати полювання на основі гіпотез, коли будуть випущені майбутні експлойти:

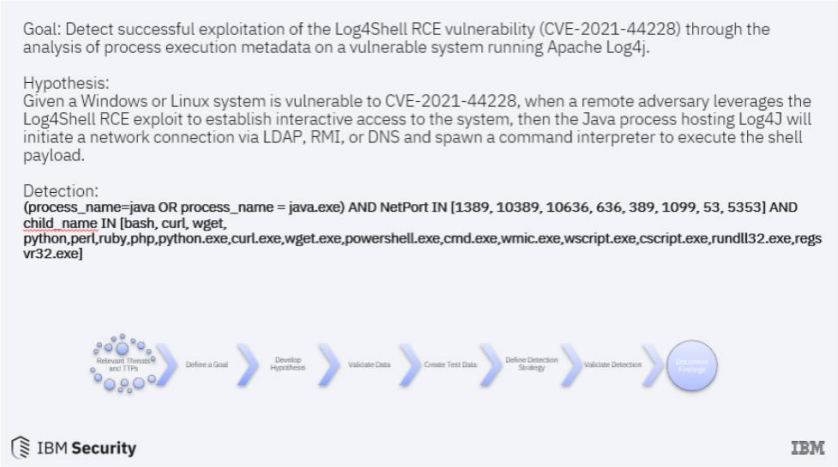

Рисунок.7 Інфраструктура пошуку загроз для виявлення вразливості Log4Shell RCE.

4. Специфікація програмного забезпечення:

- Системи OT зазвичай є запатентованими. Повний перелік програмного забезпечення цих систем часто недоступний. Працюйте зі своїми

постачальниками, щоб збирати, підтримувати та оновлювати інвентар програмного забезпечення, щоб відстежувати, які компоненти постачальники можуть використовувати у своїх системах.

5. Оновіть і відпрацюйте плани реагування на інциденти ОТ:

- Переконайтеся, що для середовищ ОТ розроблено спеціальний план реагування на інциденти.
- Переконайтеся, що підручники та процедури ОТ розроблені та відпрацьовані, щоб члени групи реагування на інциденти могли ефективно підтримувати такі події. Використовуйте уроки, отримані з цих вправ, щоб регулярно оновлювати свої плани.

Не забувайте про свої системи IoT. Крім того, організації не повинні ігнорувати свої системи IIoT. Ці системи підключаються до хмарних або приватних мереж за допомогою вбудованих і периферійних пристроїв і можуть включати веб-камери, медичні пристрої, паркомати, навігаційні системи тощо. Якщо ці пристрої залишаться вразливими, вони можуть дозволити зловмисникам перейти в корпоративне або хмарне середовище.

Це питання, яке швидко розвивається. Усі групи безпеки ОТ повинні продовжувати бути старанними та забезпечувати захист цих систем, як описано вище.

ВИСНОВКИ

Цифрова трансформація в різних галузях призвела до швидкої зміни бізнес-середовища, яке пропонує експоненціально зростаючі можливості для нових можливостей та ініціатив. Одним із найважливіших факторів успіху в цю цифрову еру є організаційна гнучкість. Підприємства можуть створити масштабовану та адаптовану цифрову подорож, що включає чітко визначену цифрову стратегію, відповідне бізнес-кейс та індивідуальний і гнучкий підхід. Разом з цифровою трансформацією організаціям вкрай важливо також керувати ризиками, які привносяться в навколишнє середовище, і їх впливом на існуючу

екосистему, щоб отримати оптимальну віддачу від своїх цифрових ініціатив. Незважаючи на всі виклики та ризики, які створює середовище, що розвивається, організації не можуть не помічати можливості, які відкриває «перехід до цифрових технологій», а також глибокий вплив, який він матиме на них. Уже сьогодні Україна активно бореться з даною проблемою, створено уповноважений орган – Кіберполіція України. На даний момент вона виконує такі функції як: реалізація державної політики у сфері протидії кіберзлочинності; завчасне інформування населення про появу новітніх кіберзлочинів; впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини; реагування на запити закордонних партнерів, що надходитимуть каналами національної цілодобової мережі контактних пунктів; участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності; участь у міжнародних операціях та співпраця в режимі реального часу. забезпечення діяльності мережі контактних пунктів між 90 країнами світу; протидія кіберзлочинам. На майбутній період пропонуємо удосконалити національну систему кібербезпеки України, щоб вона могла: забезпечити передню лінію оборони проти кіберзагроз шляхом посилення загальної ситуаційної обізнаності щодо інцидентів, вразливостей та загроз у середовищі державних установ, на об’єктах критичної інфраструктури, у громадському сегменті; запобігати вторгненням завдяки обміну інформацією та впровадженням контрзаходів, здатних зменшити поточні вразливості; захищати від повного спектру загроз шляхом підвищення контррозвідувальних та розвідувальних можливостей; зміцнити середовище кібербезпеки через освітянські, медійні громадські ініціативи; стимулювати та забезпечувати проведення кібернавчань, досліджень і розробок у сфері кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Vulnerability assessment in modern life, 2022 [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.reflectiz.com/blog/vulnerability-assessment-2022/.
2. Modern cybersecurity threats [Електронний ресурс] – Режим доступу до ресурсу: https://www.splunk.com/en_us/data-insider/what-are-modern-cybersecurity-threats.html.Як працюють нейронні мережі? [Електронний ресурс] – Режим доступу: http://apeps.kpi.ua/neural-networks/en
3. Digital transformation risks in modern businesses [Електронний ресурс] – Режим доступу до ресурсу: https://magenest.com/en/risk-in-digital-transformation/.
4. Security risks of digital transformation [Електронний ресурс] – Режим доступу до ресурсу: https://www.transputec.com/blogs/security-risks-of-digital-transformation/.
5. Digital Transformation Trends for 2022/2023 [Електронний ресурс] – Режим доступу до ресурсу: https://financesonline.com/digital-transformation-trends/.
6. Has mitigation steps for defending from digital transformation risks [Електронний ресурс] – Режим доступу до ресурсу: https://magenest.com/en/risk-in-digital-transformation/.
7. Six ways to defend against digital threats: [Електронний ресурс] – Режим доступу до ресурсу: https://www.themanufacturer.com/articles/six-ways-to-defend-against-digital-threats/.
8. Impact Of Digital Transformation, Vulnerability Management [Електронний ресурс] – Режим доступу до ресурсу: https://hitachi-systems-security.com/the-real-impact-of-digital-transformation-vulnerability-management-during-dx-part-4-of-4/.
9. Міністерство цифрової трансформації України [Електронний ресурс] – Режим доступу до ресурсу: https://thedigital.gov.ua/.

10.Міністерство цифрової трансформації України [Електронний ресурс] – Режим доступу до ресурсу: https://thedigital.gov.ua/.
11.ЦИФРОВА ТРАНСФОРМАЦІЯ ОСВІТИ І НАУКИ [Електронний ресурс] – Режим доступу до ресурсу: https://mon.gov.ua/ua/tag/cifrova-transformaciya-osviti-ta-nauki.
12.Потенціал цифрової трансформації у громадах України [Електронний ресурс] – Режим доступу до ресурсу: https://voxukraine.org/potentsial-tsyfrovoyi-transformatsiyi-u-gromadah-ukrayiny/.
13.Цифровізація України: до, під час та після повномасштабної війни [Електронний ресурс] – Режим доступу до ресурсу: https://www.vin.gov.ua/news/ostanni-novyny/47413-tsyfrovizatsiia-ukrainy-do-pid-chas-ta-pislia-povnomasshtabnoi-viiny.
14.Зміцнення ІТ-інфраструктури країни під час війни [Електронний ресурс] – Режим доступу до ресурсу: https://www.ukrinform.ua/rubric-presshall/3539383-zmicnenna-itinfrastrukturi-kraini-pid-cas-vijni.html.

Додаток А. Кількість кібератак та їх цілі за 2021 рік

Додаток Б. Принципи управління ризиками, щоб знайти певний прийнятний рівень ризику.

НАЙМЕНУВАННЯ	КРИТИЧНІСТЬ	КОНФІГУРАЦІЯ	ПОДІЇ	ЧАСТОТА	ПОВЕРХНЯ АТАКИ
Е-КОМЕРЦІЯ	Високий ризик	Прийнятний	Прийнятний	Прийнятний	Помірний
Інтернет фаервол	Середній ризик	Прийнятний	Помірний	Прийнятний	Прийнятний
Почтовий сервер	Високий ризик	Загрозливий	Помірний	Помірний	Помірний
База даних	Високий ризик	Загрозливий	Прийнятний	Помірний	Помірний
Серевр е-комерції	Високий ризик	Прийнятний	Прийнятний	Загрозливий	Прийнятний
Периметр фаерволу	Високий ризик	Прийнятний	Прийнятний	Прийнятний	Прийнятний
ПРОДАЖІ ТА МАРКЕТИНГ	Середній ризик	Помірний	Загрозливий	Прийнятний	Помірний
Робочі станції	Невизначено	Прийнятний	Загрозливий	Прийнятний	Помірний
Почтовий центр	Високий ризик	Прийнятний	Прийнятний	Загрозливий	Помірний
ІТ	Високий ризик	Прийнятний	Прийнятний	Загрозливий	Помірний

Додаток В. Перелік заумоважень нормоконтролера

Позначення документа	Сторінка	Зміст зауваження