**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**
**імені ІГОРЯ СІКОРСЬКОГО»**
**ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**
**Кафедра інформаційної безпеки**

До захисту допущено
В.о. завідувача кафедри
**_____ Микола ГРАЙВОРОНСЬКИЙ**
(підпис)
“____”_____ 2021 р.

# Дипломна робота

**на здобуття ступеня бакалавра**
**за освітньо-професійною програмою «Системи, технології та математичні методи Кібербезпеки»**
**спеціальність: 125 «Кібербезпека»**

на тему: Ризик-аналіз атак несанкціонованого доступу до конфіденційних даних інтернет магазину

Виконав: здобувач вищої освіти IV курсу, групи ФБ-74
Каширін Євгеній Віталійович
Керівник Ткач Володимир Миколайович

Рецензент

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____

Київ 2021 р

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**
**імені ІГОРЯ СІКОРСЬКОГО»**
**ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**
**Кафедра інформаційної безпеки**

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Микола ГРАЙВОРОНСЬКИЙ
«__»_____2021 р
(підпис

# ЗАВДАННЯ

**на дипломну роботу здобувача вищої освіти**

Каширін Євгеній Віталійович
1. Тема роботи Ризик-аналіз атак несанкціонованого доступу до конфіденційних даних інтернет магазину
керівник роботи к.е.н, доц кафедри ІБ, Ткач Володимир Миколайович,
затверджені наказом по університету від «_____» _____ 2021 р. №

2. Термін подання здобувачем вищої освіти роботи 07 червня 2021 р.

3. Вихідні дані до роботи: Виконаний ризик-аналіз, який може бути використан при створенні системи управління ризиками та плану забезпечення безперервності та відновлення бізнесу.

4. Зміст роботи:

1. Аналіз параметрів ризику.
2. Методи аналізу параметрів ризику.
3. Аналіз типових загроз.
4. Ризик-аналіз доступу до конфіденційних даних інтернет магазину
5. Рекомендації щодо ліквідації типових загроз.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація, вміст якої - основні моменти виконаної роботи

6. Дата видачі завдання «06 » грудня 2020 р.

Календарний план

| № з/ | Назва етапів виконання дипломної роботи | Термін виконання етапів дипломної роботи | Примітка |
|---|---|---|---|
| 1 | Отримання завдання | 06.12.2020 | виконано |
| 2 | Загальний аналіз літературних джерел | 23.02.2021 | виконано |
| 3 | Аналіз актуальних загроз | 24.04.2021 | виконано |
| 4 | Аналіз методів ризик-аналізу | 13.05.2021 | виконано |
| 5 | Розробка ризик-аналізу на основі інтегрованого методу | 28.05.2021 | виконано |
| 6 | Розробка рекомендацій щодо ліквідації актуальних загроз | 31.05.2021 | виконано |

Здобувач вищої освіти _____ Євгеній КАШИРІН

Керівник роботи _____ Володимир ТКАЧ

# РЕФЕРАТ

Робота складається з 5 розділів, містить 6 таблиць, 7 рисунків, 12 літературних посилань, обсяг роботи – 47 сторінки.

**Мета дипломної роботи** полягає у виявленні актуальних кібер-загроз, модифікуванні аналітичного методу ризик-аналізу доступу до конфіденційних даних інтернет магазину, розробці методичних рекомендацій щодо забезпечення належного рівня безпеки компанії.

**Об'єктом дослідження** є процес ризик-аналізу доступу до конфіденційних даних інтернет магазину.

**Предметом дослідження** є актуальні кібер-загрози, та методи ризик-аналізу.

**Актуальність роботи** полягає в тому, що в сучасну епоху цифрових технологій все більше бізнес-процесів переходить в онлайн. Автоматизація процесів, спеціалізовані сервіси та інтернет таблиці значно підвищують зручність управління компанією. А можливість працювати віддалено стає особливо актуальною під час епідемії COVID-19. Проте ризики викрадення конфіденційних даних не зменшились. Підприємству, такому як інтернет магазин необхідно турбуватися забезпеченням належного рівня безпеки, адже від цього залежить не тільки гіпотетична компрометація комерційних даних самої компанії, але і особистих даних клієнтів. Виконаний ризик-аналіз загроз для інтернет магазину допоможе не тільки ліквідувати слабкі місця системи, а і заощадити ресурси для їх виявлення.

**Наукова новизна** зумовлюється тим, популярний метод оцінки ризиків був оптимізован для виявлення слабких місць в захисті компанії в інтернет-середовищі, а також в тому, що отриманий в роботі ризик-аналіз інформаційного ресурсу є готовим рішенням для усунення більшості популярних кібер-загроз.

**Практичне застосування** полягає в тому, що результатами ризик-аналізу можуть користуватися не лише інтернет магазини, а і інші компанії.

**Результати роботи** опубліковані на XIX Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики».

Ключові слова: ризик-аналіз, інтернет-магазин, інформаційна безпека

# ABSTRACT

The work consists of 5 sections, contains 6 tables, 7 figures, 12 references, volume of work - 47 pages.

The purpose of the thesis is to identify current cyber threats, modify the analytical method of risk analysis of access to confidential data of the online store, development of guidelines for ensuring the appropriate level of security of the company.

The object of the study is the process of risk analysis of access to confidential data of the online store.

The subject of the research is topical cyber threats and methods of risk analysis.

The relevance of the work is that in the modern age of digital technology, more and more business processes are moving online. Process automation, specialized services and Internet spreadsheets significantly increase the convenience of company management. And the ability to work remotely becomes especially relevant during the COVID-19 epidemic. However, the risks of theft of confidential data have not decreased. An enterprise such as an online store needs to worry about ensuring the appropriate level of security, because it depends not only on the hypothetical compromise of commercial data of the company itself, but also the personal data of customers. Performed risk analysis of threats to the online store will help not only to eliminate weaknesses in the system, but also save resources for their detection.

The scientific novelty is due to the fact that the popular method of risk assessment has been optimized to identify weaknesses in the protection of the company in the Internet environment, as well as the fact that the obtained risk analysis of information resources is a ready solution to eliminate most popular cyber threats.

The practical application is that the results of risk analysis can be used not only by online stores, but also by other companies.

The results were published at the XIX All-Ukrainian scientific-practical conference of students, graduate students and young scientists "Theoretical and applied problems of physics, mathematics and computer science."

Key words: risk analysis, online store, information security

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АОР – Аналіз та оцінка ризиків

ІР – Інформаційний ресурс

ЛЗ – Лінгвістична змінна

НЧ – нечітке число

ПЗ – Програмне забезпечення

ОС – Операційна система

# ВСТУП

**Актуальність роботи.** Стрімкий розвиток IT-інфраструктури підприємств незмінно тягне за собою неконтрольоване зростання кількості інформаційних загроз і вразливостей інформаційних ресурсів. Оцінка і аналіз інформаційних ризиків є необхідною умовою при створенні системи управління ризиками та плану забезпечення безперервності та відновлення бізнесу. На сьогоднішній день існує безліч інструментальних засобів, які об'єднуються в методики оцінки та аналізу ризику. Ці методики представляються в досить широкому спектрі, який починається нормативними документами (стандартами) і закінчується конкретними програмними продуктами. На практиці іноді необхідно здійснити оцінювання з комбінацією підходів інтерпретування суджень експерта та статистичних даних. Для вирішення такого завдання і спрощення розрахунків ризиків в роботі пропонується інтегрований метод аналізу і оцінювання ризиків, який на відміну від відомих дозволяє оперувати одночасно чіткими і нечіткими параметрами з можливістю трансформування термів лінгвістичних змінних

**Мета і завдання дослідження.** Мета роботи полягає у виявленні актуальних кібер-загроз, модифікуванні методу ризик-аналізу доступу до конфіденційних даних інтернет магазину, розробці методичних рекомендацій щодо забезпечення належного рівня безпеки компанії.

Завдання – розглянути методи ризик-аналізу доступу до конфіденційних даних інтернет магазину, розробити методичні рекомендацій щодо забезпечення належного рівня безпеки компанії

Об’єктом дослідження є поточна ситуація в інформаційній безпеці.

Предметом дослідження є актуальні кібер-загрози, методи ОАР.

**Методи дослідження.** Для аналізу кіберзагроз була використана аналітична база та статистичні дані компанії Cisco, статистичні дані в вільному доступі. Серед методів аналізу параметрів ризику розглянуто Статистичний метод, метод експертних оцінок та інтегрований метод.

Наукова новизна одержаних результатів. Був опрацьований и структурован великий объем статистичних даних, проведений ризик-аналіз може використовуватись для забезпечення інформаційної безпеки компаніями.

Практичне значення одержаних результатів. Оцінка і аналіз інформаційних ризиків є необхідною умовою при створенні системи управління ризиками та плану забезпечення безперервності та відновлення бізнесу. Висновки даної роботи використовуватись для забезпечення інформаційної безпеки структурам, яким це необхідно.

Апробація результатів роботи. Робота була оприлюднена на XIX Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики».

Публікації. Робота була опублікована на XIX Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики».

# 1 АНАЛІЗ ПАРАМЕТРІВ РИЗИКУ

## 1.1 Інтегроване поняття ризику

Методики аналізу та оцінки ризику інформаційної безпеки, що існують на даний момент в своїй основі розглядають певну кількість параметрів таких як частоту події, її ймовірність та небезпеку. Проте при побудові більшості систем менеджменту інформаційної безпеки та її аудиту на практиці доводится відображати ризик через більшу кількість параметрів: втрати, певні х-ки ситуації, витрати, відхилення від цілі і т.д.

Для полегшення задачі аналізу та оцінки ризику інформаційної безпеки пропонується розглянути інтегроване представлення параметрів ризику з відображенням на сферу ІБ та представити його у вигляді десятикомпонентного кортежу <E, A, S, C, P, D, M, F, L, V>, де E - подія, A - дія, M - міра ризику, C - характеристика ситуації, P - ймовірність, D - небезпека, S - ситуація вибору, F - частота, L - витрати і втрати (витрати), V - відхилення від мети.

Перший розглядаємий компонент в кортежі є **ПОДІЯ (E).** Для зручності його представляють у вигляді символьної змінної, який може приймати одну із значень кінцевої множини ідентифікаторів $E \in \{E_1, E_2, ..., E_e\}$, де e - кількість розглядаємих ідентифікаторів подій). Так як класичними базовими характеристиками безпеки PIC є тріада CIA - конфіденційність, цілісність і доступність, то базові події прі e=7 можна інтерпретувати як:

$E_1$ = “Порушення конфіденційності (ПК)”,

$E_2$ = "Порушення цілісності (ПЦ)",

$E_3$ = "Порушення доступності (ПД)",

$E_4$ = "Порушення цілісності і конфіденційності (ПЦК)"

$E_5$ = "Порушення цілісності і доступності (ПЦД)"

$E_6$ = "Порушення конфіденційності та доступності (ПКД ) "

$E_7$ =" Порушення конфіденційності, цілісності та доступності (ПКЦД)

Другий розглядаємий компонент в кортежі - **Дія (А)**, яка стала причиною виникнення події Е. З боку ІБ **А** пов’язана з реалізацією потенційних загроз базовими характеристиками безпеки РІС, що стали причиною **Е**, що відображається одним з описаних вище ідентифікаторів$\{E_1, E_2, ..., E_e\}$. В такому разі **А** можна відобразити множиною ідентифікаторів $A \in \{A_1, A_2, ..., A_a\}$, де а - кінцева кількість ідентифікаторів загроз. Наприклад, на основі розглядаємих нижче найімовірніших загроз за 2020 рік:

$A_1$= “зараження програмами-шифрувальниками”,

$A_2$= “зараження Remote Access Trojans”,

$A_3$= “Несанкціонований доступ до корпоративної мережі”,

$A_4$= “Перехоплення інформації”,

$A_5$= “Соціальна інженерія”.

Задачу оцінювання та вимірювання ризиків ускладнює той факт, що для вимірювання останнього не існує стандартизованої природної шкали, тому оцінка проводиться на основі об'єктивних або суб'єктивних критеріїв.

Наприклад, об'єктивним критерієм може бути ймовірність поломки певного обладнання, таким як компьютер за певний проміжок часу, а суб'єктивним критерієм - оцінка власника інформаційного ресурсу ризику поломки компьютера, що базується на його професіональному досвіді. Для відображення такої оцінки розробляється якісна шкала, наприклад з такими градаціями як: низький, середній і високий рівні.

Для вимірювання ризику в сфері ІБ як правило використовуються якісні і кількісні шкали: грошові, лінгвістичні, імовірнісні, бінарні, а також можливі вимірювання за допомогою спеціальних коефіцієнтів. Таким чином, **компонент М**, можна відобразити трикомпонентною множиною $M \in \{Мкл, Мяк, Мі\}$, де Мкл - кількісна (наприклад, може характеризуватися чисельно), Мяк - якісна (наприклад, може характеризуватися лінгвістично) і Мі - інтегрована (наприклад, може характеризуватися чисельно і лінгвістично) заходи.

В роботі поняття ризику, в безлічі його тлумачень, розкривається так само через невизначеність. З точки зору ІБ базова ознака ризику невизначеність можна інтерпретувати, як характеристику ситуації при настанні певної події Е. В ІБ може наступити подія Е, до якого призвело дію А, яке раніше не відбувалося, наприклад, немає статистичних даних про конкретний вид інциденту порушення ІБ. Отже, розглядаючи компонент кортежу характеристики **ситуації (С)**, можна відобразити його як $C \in \{C_o, C_н\}$ де, $C_0$ - характеризує ситуацію як певну, а $C_н$ - як нечітку.

Четвертий розглядаємий компонент в кортежі - **ймовірність (Р)** появи події **Е** (наприклад, з ідентифікатором Е3). Часто імовірність поділяють на "фізичну або “об’єктивну” та "суб'єктивну". Фізична (об’єктивна) ймовірність розуміється як частота появи певної події в загальному обсязі здійснених спостережень або відношення кількості сприятливих результатів до їх загального числа. Вона, наприклад, формується при аналізі результатів великого числа спостережень. Під суб'єктивною ймовірністю розуміється міра впевненості особи або групи людей в тому, що дана подія відбудеться. Ця ймовірність може бути формально представлена різними способами, наприклад, імовірнісним розподілом або бінарним відношенням на множині подій, але найбільш часто вона являє собою вірогідну міру, отриману експертним шляхом. $\mathbf{P} = \sum_{i=1}^{p} P_i$ Слід зазначити, що коли виникають складнощі з отриманням статистичних даних, а так само для простоти інтерпретації величин, експерти $\mathbf{P} = \sum_{i=1}^{3} P_i$ використовуючи логіко-лінгвістичний підхід відображають цей компонент через лінгвістичну змінну (ЛЗ) "ЙМОВІРНІСТЬ" з базовою терм-множиною (р - кількість термів), для членів якого діє наступне відношення $P_1 < P_2 < ... < P_p$. Наприклад, при р = 3 для зазначеної ЛЗ можна сформувати множину термів = { "низька (Н)", "середня (С)", "висока (В)"}, відображаємих нечіткими числами Н, С, В, для яких визначаються відповідні функції приналежності. Також можуть бути введені й інші значення первинних термів такі як, наприклад, "дуже низька

(ДН)", "вище середнього (ВС)", "нижче середнього (НС)" та ін. Очевидно, що в цьому випадку Р відображається в лінгвістичної формі і при цьому логічно випливає, що М інтерпретується, як $М_{як}$.

Компонент **ситуація вибору (S)** в області ІБ можна інтерпретувати як величину, яка характеризує перевагу настання стану Е. На основі цього компонента зручно приймати рішення щодо організації заходів, наприклад, щодо зниження ризику, його прийняття, передачі третій особі і т.д. Компонент S, аналогічно ймовірності, можемо уявити через ЛЗ "СИТУАЦІЯ ВИБОРУ" з базовою терм-множиною ($S_1 < S_2 <... < S_s$), що дозволяє інтерпретувати вибір за допомогою s $\mathbf{S} = \overset{s}{\underset{i=1}{Y}} S_i$ варіантів. Наприклад, при s = 2 для зазначеної ЛЗ може бути $\mathbf{S} = \overset{2}{\underset{i=1}{Y}} S_i$ сформована наступним чином ={ "Менш приваблива (МП)", "більш приваблива (БП)"} або{ "менш надійна (МН) "," більш надійна (БН) "}, які відповідно відображаються нечіткими числами МП, БП або МН, БН .

Компонент кортежу **небезпека (D)** розглядається як величина яка характеризує небезпеку події, наприклад, $Е_1$ за допомогою $А_2$. За аналогією з Р компонент D може відображатися чисельно (наприклад, у відсотках) або за допомогою ЛЗ - "НЕБЕЗПЕКА" з базовою терм-множиною ($D_1 < D_2 <... < D_d$). Наприклад, при d = 3 $\mathbf{D} = \overset{d}{\underset{i=1}{Y}} D_i$ можемо визначини "Середня (С)", "висока (В)"}, а мірі ризику відповідає $М_{як}$

Наступний компонент кортежу **частота (F),** який в області ІБ можна пов'язати з частотою реалізації "загрози", що призвела до події Е. Такий компонент можна відображати чисельно або через ЛП - "ЧАСТОТА" наприклад, при f = 3 маємо { "низька (Н)", "середня (С)", "висока (В)"}.

Компонент витрати і втрати в області ІБ доцільно визначити через термін **витрати (L),** який за аналогією з попереднім можна представляти чисельно, наприклад, 1) 0 - $ 99; 2) $ 100 - $ 999.; 3) $ 1000 - $ 9999; 4) $ 10 000 - $ 99999, при цьому мірою відповідає $М_{кл}$. Також L можна представити за допомогою ЛП "ВИТРАТИ", наприклад, прі l = 5 маємо { "низькі (Н)", "нижчого за середній

(НС) "," середні (С) "," вище середнього (ВС) "," високі (В) "}, а М відповідає $М_{кл}$. На практиці зустрічається і інтегроване уявлення L, наприклад, 1) Negligible (менше $ 100); 2) Minor (менш $ 1000); 3) Moderate (менше $ 10 000); 4) Serious (Істотний негативний вплив на бізнес); 5) Critical (Катастрофічне вплив, можливе припинення діяльності підприємства), при цьому міра буде відображатися параметром $М_і$.

Відхилення від **мети (норми) (V)** - цей компонент, як і Р може відображатися чисельно (наприклад, як стандартне (квадратичне), ймовірне або допустиме відхилення), так і за допомогою застосування логіко-лінгвістичного підходу з допомогою ЛП "ВІДХИЛЕННЯ ВІД МЕТИ". Наприклад, при v = 3 сформуємо множину термів { "маленьке (М)", "середнє (С)", "велике(В) "}, що відображаються нечіткими числами М, С, Б.

Слід зазначити, що при поданні ризику, за допомогою кортежу, можна виділити компоненти, що його ідентифікують - **E, A, M, C** та оціночні компоненти **P, D, S, F, L і V.**

Компоненти, що ідентифікують кортеж виступають в якості інтегрованого ідентифікатора ризику і можуть відображаються за допомогою оціночних компонент за допомогою числових або лінгвістичних значень (показників), наприклад, для інформаційної системи компанії необхідно визначити ризик, пов'язаний з настанням події порушення ІБ, яке призвело до впливу на цілісність і доступність - це подія ідентифікується як $Е_5$ = "ПЦД", а дія, що призвела до нього, наприклад, $А_3$ = "Несанкціонований доступ до корпоративної мережі". Тут для відображення ризику можемо використовувати $М_{кл}$, $М_{як}$ або $М_і$, а для того щоб показати його значущі параметри слід скористатися оціночними компонентами кортежу, а саме, наприклад, визначити: ймовірність (Р) настання такої події, до якого привело цю дію; небезпека (D) від настання події; витрати (L), які будуть результатом настання події; частоту (F) настання даної події (дії); відхилення від мети (V) і нарешті, вибрати варіант прийняття рішень (S)

**Висновки до розділу 1**

У першому розділі провели аналіз поняття ризику з боку інформаційної безпеки. Визначили базові характеристики ризику з множини його тлумачень з усіх сфер для подальшої інтерпретації саме в інформаційній безпеці. Представили його у вигляді кортежу з описом найбільш популярних ідентифікуючих компонентів.

# 2 МЕТОДИ АНАЛІЗУ ПАРАМЕТРІВ РИЗИКУ

## 2.1 Інтегрований метод аналізу і оцінювання ризиків інформаційної безпеки

Процес аналізу і оцінювання ризиків (АОР) інформаційної безпеки (ІБ), часто в процесі АОР виникають ситуації, при яких експерт не завжди чітко може оцінити ту чи іншу загрозу ІБ.

Для вирішення такого роду завдань застосовуються детермінований або нечіткий метод АОР, що представлений нижче. На практиці бувають ситуації, коли необхідно провести оцінювання з комбінацією підходів інтерпретування суджень експерта, як щодо його можливостей чітко детермінувати значення отриманих оціночних параметрів, так і при його невпевненості щодо однозначності своїх пріоритетів.

Пропонований інтегрований метод містить 9 кроків. Розглянемо детально його роботу.

- **Крок 1 - Визначення множини загроз**

На першому кроці експертами згідно ідентифікованим інформаційним ресурсам (ІР) визначається множина можливих загроз. Для створення цієї множини в якості основи використовуємо модель параметрів інтегрованого уявлення ризиків, де $\mathbf{A} \in \{A_a\}(a = \overline{1,n})$множина дій елементи яких можуть призвести до безлічі подій порушення ІБ $\mathbf{E} \in \{E_e\}(e = \overline{1,7})$. Наприклад при e = 7 події можуть ідентифікуватися як, $E_1$ = "Порушення конфіденційності (ПК) ",

$E_2$ =" Порушення цілісності (ПЦ) ",

$E_3$ =" Порушення доступності (ПД) ",

$E_4$ =" Порушення цілісності і конфіденційності (ПЦК) "

$E_5$ = "Порушення цілісності і доступності (ПЦД)"

$E_6$ = "Порушення конфіденційності та доступності (ПКД) "

$E_7$ =" Порушення конфіденційності, цілісності та доступності

(ПКЦД) ", а при n = 5 експерти можуть ідентифікувати, такі **A** $\in \{A_a\}(a = \overline{1,5})$ $A_1$ = «Зараження програмами-шифрувальниками»;

$A_2$ = "Помилки користувача;

$A_3$ = «Порушення роботи сервісів системи»;

$A_4$ = «Порушення цілісності системи безпеки»;

$A_5$ = «Відмова в обслуговуванні».

- **Крок 2 - Визначення множини параметрів для оцінювання ризику**

Для відображення загального результату АОР скористаємося лінгвістичної змінною (ЛЗ) «ступінь ризику» (DR), яка визначається кортежем, де базові терм-множини задаються m термами $T_{DR} = \bigcup_{j=1}^{m} T_{DR_j}$ (наприклад, для m = 5 - $\bigcup_{j=1}^{5} T_{DR_j}$ = { «Незначний ризик порушення ІБ» (НР),

«Ступінь ризику порушення ІБ низька» (РН),

«Ступінь ризику порушення ІБ середня» (РС),

«Ступінь ризику порушення ІБ висока» (РВ),

«Граничний ризик порушення ІБ »(ГР)}, які можуть бути відображені на універсальній множині $X_{DR} \in \{0, max_{DR}\}$).

Для кожного з термів $T_{DR1}$, ..., $T_{DRj}$, ..., $T_{DRm}$ задається свій інтервал значень $[dr_{min}; dr_1$ [..., $[dr_j; dr_{j+1}$ [..., $[dr_m; dr_{max}]$

Далі для створення можливості експерту при оцінюванні використовувати більш широкий спектр величин, скористаємося вищевказаною моделлю параметрів і позначимо повну множину оціночних компонент $EK_{3Fh} \in \{EK_i\}$ = {P, L, F, D, S, V} (i=$\overline{1,g}$), де 3Fh - шістнадцятковий код, бінарне значення якого в такий спосіб відображає порядковий номер оціночного компонента в множині: P розташовується в розряді $2^5$, F в $2^4$, L - $2^3$, D - $2^2$, S -$2^1$, V-$2^0$

(наприклад, якщо експерти хочуть скористатися P, L, F то g = 3 (i=$\overline{1, 3}$), а EK $_{3C} \in$ {EK $_i$} = {EK $_1$, EK $_2$, EK $_3$} = {P, L, F}.

Також, на цьому кроці проводиться опис набору використовуваних оціночних компонент, які, як вважає експерт-аналітик, може впливати на оцінку ризику ІБ, а з іншого - оцінюють його різні за своєю природою боку, наприклад, що враховують особливості організації (банк, інтернет-магазин, силові відомства та ін.). Для цього експерт повинен визначити код, за яким з {EKi} обирають значення відповідних компонент, наприклад, при коді 2F - g = 3, EK $_{2F} \in$ {EK $_i$} = {EK $_1$, EK $_2$, EK $_3$} = {P, L, F}

Введемо ЛЗ «Рівень оціночного компонента EK $_i$» (KEK), яка задається кортежем <К $_{EK_i}$,Т$_{К_{EK_1}}$,Х$_{К_{EK_i}}$>, де базові терм-множини задаються m термами $T_{K_{EK_i}} = \bigcup_{j=1}^{m} T_{K_{EK_i j}}$ Наприклад, при m = 5 маємо {«Дуже низький» (ДН),

«низький» (Н), «середній» (С), «високий» (В),

«дуже високий» (ДВ)}, які в лінгвістичній формі характеризують рівень оціночного компонента

Оцінка значущості EK $_i$ здійснюється параметрами з множини LS $LS \in \{LS_i\}$ (i=1, g), а оцінка значення оціночного компонента - за допомогою множини ek $\in$ {ekj} (j = 1, g).

- **Крок 3 - Визначення кількості необхідних терм-множин для АОР**
- **Крок 4 - Оцінка рівня значущості оціночних компонент**

На цьому кроці кожному компоненту - EK $_i$ ставитися у відповідність рівень його значущості - LS $_i$.

Відзначимо, що якщо для всіх LS справедливо відношення порядку

$$\mathbf{LS}_i \geq \mathbf{LS}_{i+1} \qquad \textbf{(2.1)}$$

То значимість і-го компонента визначається за правилом Фішберна:

$$\boldsymbol{LS}_i = \frac{2(g-i+1)}{(g-1)g} \qquad \textbf{(2.2)}$$

Згідно з цим правилом у експерта відсутня інформація про значущість компонента і тоді вищевказана формула відображає максимум ентропії інформаційної невизначеності про об'єкт дослідження. Якщо ж все компоненти мають рівну значимість, то

$$\boldsymbol{LS}_{i} = 1/g \qquad \textbf{(2.3)}$$

- **Крок 5 - Визначення еталонних значень ступеня ризику**

На цьому кроці експертами визначаються еталонні значення для DR, тобто задається кількість термів в базовому терм-множині ЛЗ і ставитися їм у відповідність заданий інтервал значень, що лежить в діапазоні $[dr_{min};\ dr_{max}]$ (Див табл 1)

Таблиця 2.1 - Еталонні значення

| $\boldsymbol{EK_i}$ | НЧ $\underset{\sim}{X}_{K_{EK_{ij}}} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$ для $T_{K\,EK_i1} - T_{K\,EK_im}$ $(j=\overline{1,m})$ | | | | |
|---|---|---|---|---|---|
| | $T_{K\,EK_i1}$ | … | $T_{K\,EK_ij}$ | … | $T_{K\,EK_im}$ |
| $EK_1$ | $(a1_{min};\ b1_{1min};\ b1_{21};\ c1)$ | … | $(a1_j;\ b1_{1j};\ b1_{2j+1};\ c1_{j+1})$ | … | $(a1_m;\ b1_{1m};\ b1_{2max};\ c1_{max})$ |
| … | … | … | … | … | … |
| $EK_i$ | $(ai_{min};\ bi_{1min};\ bi_{21};\ ci)$ | … | $(ai_j;\ bi_{1j};\ bi_{2j+1};\ ci_{j+1})$ | … | $(ai_m;\ bi_{1m};\ bi_{2max};\ ci_{max})$ |
| … | … | … | … | … | … |
| $EK_g$ | $(ag_{min};\ bg_{1min};\ bg_{21};\ cg)$ | … | $(ag_j;\ bg_{1j};\ bg_{2j+1};\ cg_{j+1})$ | … | $(ag_m;\ bg_{1m};\ bg_{2max};\ cg_{max})$ |

- **Крок 6 - Оцінка поточних значень компонент**

На цьому кроці по кожному оціночному компоненту $\{EK_i\}$ = {P, S, F, D,L, V} (i=$\overline{1,\ g}$) експемрти відповідної предметної області визначають *ek* для всіх A при (a=$\overline{1,\ n}$)

Значення виставляються на підставі переваг експертів, статистичної інформації та інших даних.

- **Крок 7 - Класифікація поточних значень**

На цьому кроці за допомогою еталонних значень, сформульованих експертами, здійснюється визначення приналежності $ek_i^{A_a}$ заданому НЧ, за яким формується значення за допомогою виразу:

$$\lambda_{i1}^{(A_a)} = \begin{cases} 1 \; npu \; ek_i^{A_a} \in [bi_{11}, bi_{12}[ \\ 0 \; npu \; ek_i^{A_a} \notin [bi_{11}, ci_1[ \\ \mu_1(ek_i^{A_a}) \; npu \; ek_i^{A_a} \in [bi_{12}, ci_1[ \end{cases},$$

$$\dots$$

$$\lambda_{ij}^{(A_a)} = \begin{cases} \mu_j(ek_i^{A_a}) \; npu \; ek_i^{A_a} \in [ai_j, bi_{1j}[ \\ 1 \; npu \; ek_i^{A_a} \in [bi_{1j}, bi_{2j}[ \\ \mu_j(ek_i^{A_a}) \; npu \; ek_i^{A_a} \in [bi_{2j}, ci_j[ \\ 0 \; npu \; ek_i^{A_a} \notin [ai_j, ci_j[ \end{cases}, \quad \textbf{(2.4)}$$

$$\dots$$

$$\lambda_{im}^{(A_a)} = \begin{cases} \mu_m(ek_i^{A_a}) \; npu \; ek_i^{A_a} \in [ai_m, bi_{1m}[ \\ 1 \; npu \; ek_i^{A_a} \in [bi_{1m}, bi_{2m}[ \\ 0 \; npu \; ek_i^{A_a} \notin [ai_m, bi_{2m}[ \end{cases},$$

$$(j = \overline{2, m-1}).$$

- **Крок 8 - Оцінка ступеня ризику**

На цьому кроці проводиться обчислення показника ступеня ризику порушення ІБ $dr^{(A_a)}$ за формулою:

$$dr^{(A_a)} = \sum_{j=1}^{m} \left( dr_j \sum_{i=1}^{g} LS_i \lambda_{ij}^{(A_a)} \right), \quad \textbf{(2.5)}$$

- **Крок 9 - Формування структурованого параметра ризику**

На підставі обчисленого значення $dr^{(A_a)}$ і побудованих еталонів формуємо структурований параметр ступеня ризику SP за виразом:

$$SP^{(A_a)} = \begin{cases} (dr^{(A_a)}; T_{DR_j}) \; при \; \mu_j(dr) = 1 \\ (dr^{(A_a)}; T_{DR_j}(\mu_j(dr)); T_{DR_{j+1}}(\mu_{j+1}(dr))) \; при \; \mu_j(dr), \mu_{j+1}(dr) \neq 1 \end{cases}, \quad \textbf{(2.6)}$$

За допомогою SP можна отримати як числове значення ступеня ризику, так і лінгвістичну інтерпретацію, що враховує невпевненість експерта при формуванні поточних значень оціночних компонент з подальшою класифікацією за допомогою параметра $\lambda_{ij}^{(A_a)}$.

За виразом (3) можна обчислити середнє значення $dr^{(\text{ср})}$ по виразу:

$$dr^{(cp)} = (\sum_{a=1}^{m} dr^{(A_a)}) / m. \quad \textbf{(2.7)}$$

## 2.2 Статистичний метод аналізу ризиків

Статистичний метод аналізу ризиків застосовується в тому разі, коли експерт володіє достатньою кількістю аналітичних даних та статистичної інформації відносно об’єкта аналізу. Сутність цього методу полягає в тому, що для розрахунку ймовірності повторної кібератаки або потенційних збитків відбуває аналіз схожих атак і підрахунок збитків в минулому компанії.

Як перевагою так і недоліком даного методу аналізу ризиків є його варіативність фінального передбачення, адже в залежності від того, який напрям розвитку подій обере експерт, які фактори він врахує і залежить результат аналізу.Також, недоліком даного методу є необхідність в застосуванні імовірнісних характеристик.

### 2.3 Метод аналізу доцільності витрат

Метод аналізу доцільності витрат полягає в наступному: в процесі діяльності компанія витрачає різну кількість ресурсів для кожного напряму ІБ, а також ці витрати мають різний рівень ризику. Визначення рівня ризику даним методом орієнтовано на ідентифікацію потенційних зон ризику. А це, в свою чергу, дозволяє виявити слабкі місця з точки зору ризиків, а потім розробити шляхи їх ліквідації.

Також даний метод дозволяє визначити мінімальний критичний обсяг продажів, іншими словами - нижній граничний розмір реалізації продукції, при якому прибуток компанії дорівнює нулю. Якщо виробництво продукції буде меньше критичного, то компанія буде отримувати лише збитки.

Даний метод дозволить виявити напрями для негайної модернізації в рамках обмеженого бюджету.

### 2.4 Метод експертних оцінок

Метод визначення рівня ризику шляхом експертних оцінок , як не дивно, має більш суб'єктивний характер, якщо порівнювати його з описаними вище методами. Ця суб'єктивність передусім є наслідком того, що в залежності від професійних навичок групи експертів, їх доступу до аналітики і т.д. фінальне заключення щодо аналізу ризиків є висловлюванням власні суб'єктивні думки як про минулу ситуації (доконаний подію), так і про перспективи її розвитку.

Як правило, метод експертних оцінок застосовується при малому обсязі інформації або при визначенні рівня ризику за такими напрямками діяльності, у яких відсутні аналоги.

В цілому, компанія, що працює за цим методом виділяє групу ризиків і розглядає, як вони можуть вплинути на її діяльність. Як правило, розгляд зводиться до виставлення простих оцінок щодо ймовірності виникнення певного виду ризику, а також його ступеня впливу на діяльність компанії в цілому.

**Висновки до розділу 2**

Розглянули різні методи аналізу і оцінки інформаційних ризиків. Статистичний метод аналізу ризиків, метод аналізу доцільності витрат та метод експертних оцінок хоч і є продуктивними, проте їх суб'єктивність результатів змушує взяти за основу детермінований або нечіткий метод, який на відміну від відомих дозволяє оперувати одночасно чіткими і нечіткими параметрами з можливістю трансформування термів лінгвістичних змінних, для подальшого розвитку системи на його основі.

# 3 АНАЛІЗ ТИПОВИХ ЗАГРОЗ

Розглянемо типовий інтернет магазин з офісом, штатом з працівників, базою конфіденційних даних клієнтів для аналізу найвірогідніших загроз. Скористаємось аналітикою кібер-атак за минулий 2020 рік, з урахуванням наслідків всесвітньої епідемії COVID-19.

Основними цілями цілями атак зловмисників стали організації, а не фізичні особи. Це не дивно, адже атаки на юридичні компанії, які можуть бути чутливими до зупинення роботи, як володіють комерційною таємницею і зберігають великі об'єми персональних даних можуть віддати як викуп суму у декілька мільйонів. У той час, як атака на фізичну особу і близько не дасть таких результатів. Рисунок 3.1 демонструє різницю атак на фізичних і юридичних осіб.

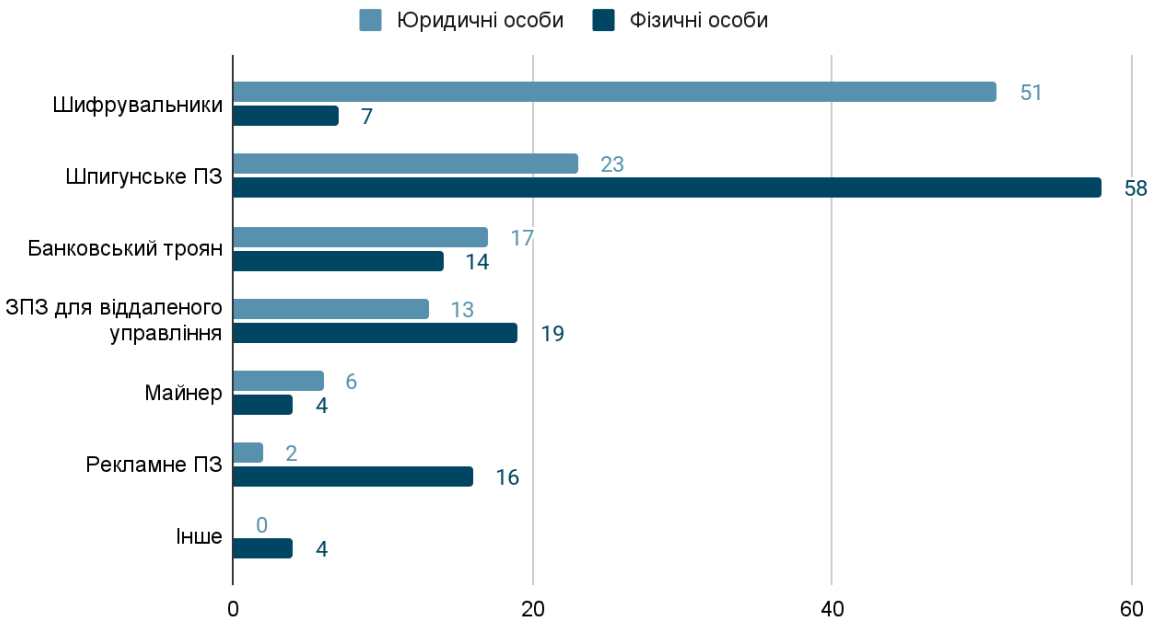


Рисунок 3.1 - Типи зловмисного ПЗ

## 3.1 Програми-шифрувальники

Через глобальну епідемію, кількість людей, що почали працювати онлайн значно зросла. Різноманітні бізнеси постали перед вибором - або перенести свою діяльність в інтернет, або зачинитись. Найбільш серйозною кібератакою за минулий рік є розповсюдження програм-шифрувальників. Якщо в кінці

минулого року вони становили 39% всіх атак, то на початку цього року їх частка збільшилася до 51%. Тобто, в кожна друга атака з поширенням зловмисного ПО була з використанням шифрувальників. З цього витікає наступний факт - частка атак, в яких зловмисник переслідує фінансову вигоду зросла на 42%. Рисунок 3.2 демонструє мотиви атак зловмисників.

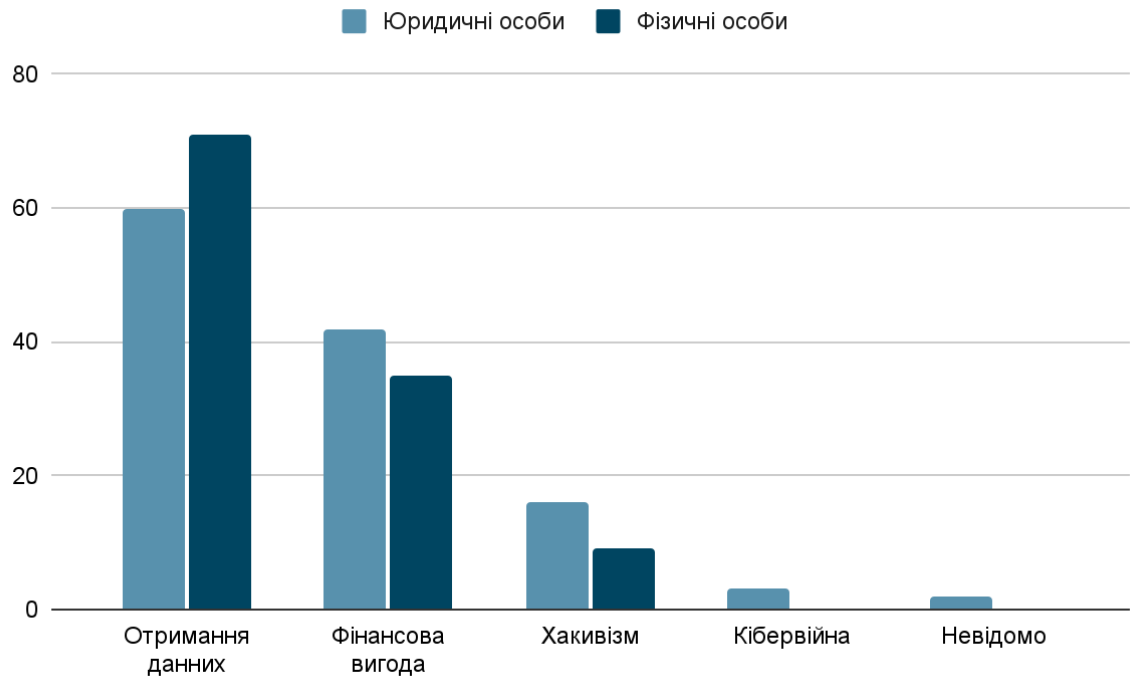


Рисунок 3.2 - Мотиви зловмисників

Як було вказано вище, зловмисники все рідше проводять масові атаки з викорстанням шифрувальників на фізичні особи, вони спеціально обіраюсть великі компанії, які можуть заплатити значний викуп, або організації та структури, для яких призупинення діяльності небезпечна, і наносять удар саме по ним. Через єпідемію в минулому році програми-вимагачі зробили акцен на промисловому секторі і медичних установах, що вказано на Рисунок 3.3

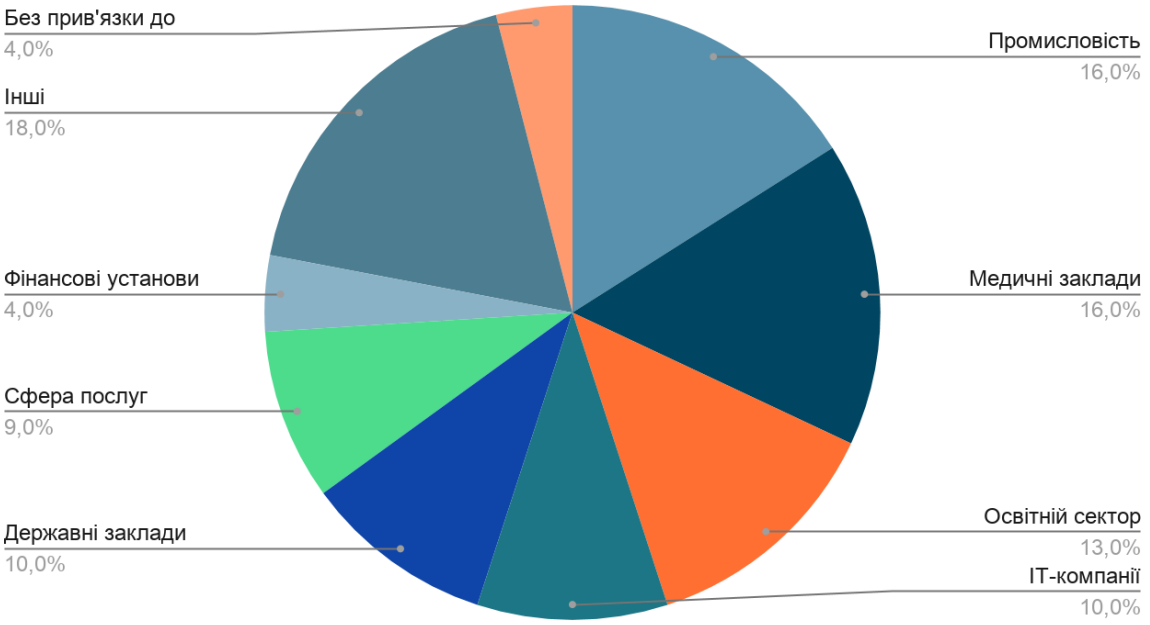


Рисунок 3.3 - Атаки програм-вимагачів по галузям

### 3.2 Способи потрапляння шкідливого ПЗ у внутрішню мережу компанії

Отже, основною загрозою для інтернет магазину є атака з використанням програм шифрувальників. Основним способом потрапляння у внутрішню мережу компанії шкідливого ПЗ є електронна пошта. Проте можна спостерігати тенденцію збільшення кількості атак, в яких шкідливе ПЗ розповсюджується шляхом експлуатації певних вразливостей софта, що використовує компанія. Наприклад, оператори програми-вимагача Netwalker до квітня 2020 року розповсюджували свій шкідливий код за допомогою фішингових листів, а вже починаючи з квітня експлуатують вразливості в неоновленних VPN-рішеннях, займаються підбором паролів для віддаленого доступу по протоколу RDP і шукають уразливості в веб-додатках.

Пандемія багато в чому посприяла цьому тренду: компанії, в тому числі великі інтернет магазини в терміновому порядку виводили на периметр сервіси, які до пандемії були доступні тільки з локальної мережі. Через це периметр швидко змінювався, приділяти достатньо уваги безпеці цих сервісів ресурсів не вистачає, тому багато хто не встигав або не мав можливості забезпечити їх надійний захист. Більша частина компаній все ще працюють у віддаленому режимі, тому питання контролювання доступних ззовні ресурсів і розробка

ефективного процесу управління вразливостями для них стоять особливо гостро. Рисунок 3.4 відображає способи розповсюдження зловмисного ПЗ в атаках на юридичні особи.

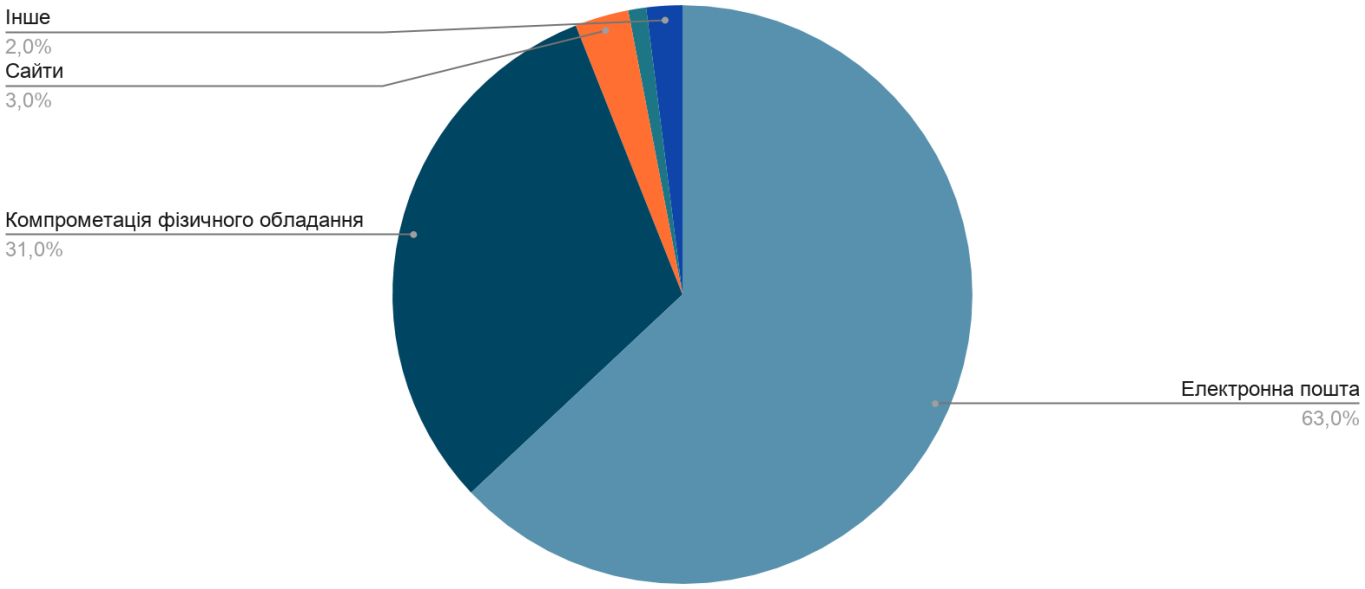


Рисунок 3.4 - Способи розповсюдження зловмисного ПЗ

### 3.3 Зростання кількості атак

Задача ризик-аналізу і прогнозування атак ускладнюється тим, що винахідливість зловмисників зростає, вони вигадують нові методи приховування атак, Наприклад, нещодавно хакери розробили спеціальний плагін для офісного програмного забезпечення для того, щоб проникнути в корпоративну мережу компанії. Ціллю зловмисників були знімки робочого столу ПК, конфіденційні дані, файли з певним розширенням. Особливість розглянутого хакерського плагіну полягає в тому, що він автоматично перевіряє чи запущений  диспетчер задач або схожий софт в системі. У разі виявлення такої активності шкідливий код нічого не робить. Завдяки цьому він залишається непоміченим набагато довше. Подібна модифікація шкідливого ПЗ а також приховування атак самими компаніями-жертвами(з огляду на репутаційну складову) робить неможливими збирання точної статистики, що нас цікавить. Однак на основі відкритих даних і звітів атакованих компаній можна побудувати Рисунок 3.5, що представлена нижче.

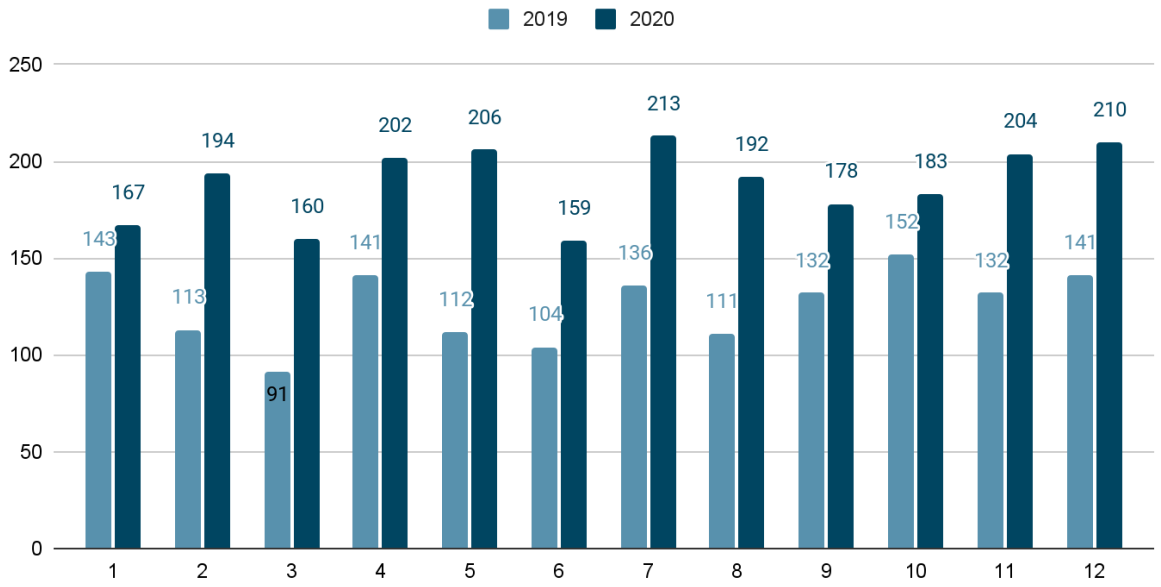


Рисунок 3.5 - Кількість атак в 2019 та 2020 роках

### 3.4 Соціальна інженерія

Більша частина методів соціальної інженерії, що використовують зловмисники не вимагають поглиблених технічних або практичних знань, тому їх актуальність і розповсюдженість в 2020 року тільки зросла. Хакери, що працюють поодинці або злочинні угрупування - будь-хто зможе використовувати писані нижче методи.

Не дивлячись на те, що існує велика кількість методик, які підпадають під таке поняття як “соціальна інженерія” в області кібербезпеки розглядати ми будемо лише найпопулярніші - фішинг та спам.

**Фішинг** - це метод кібератаки, суть якого полягає у тому, що злочинець з ціллю отримання конфіденційної інформації, в тому числі комерційної таємниці або особистих даних клієнтів намагається завоювати довіру у атакованої людини - менеджера, оператора колл-центру, будь-якого іншого працівника компанії. Для підвищення ймовірності отримання даних злочинці можуть створювати відчуття терміновості або навіть залякують жертву.

В нашому випадку особливу увагу слід приділити тим фішинговим

кампаніям, які беруть за свою ціль корпорації або компанії, такі як інтернет магазин.

**Спам** - це специфічна атака, яка відзначається масовою розсилкою небажаних листів. Як ми бачимо з таблиці 4, у більшості випадків спам - це особливий лист електронної пошти, який відправляється на велику кількість адрес. Проте воно може бути доставлено через соціальні мережі, СМС і т.п. Не дивлячись на те, що спам не є соціальною інженерією, однак зловмисники можуть використовувати його види:

- spearphishing,
- vishing,
- smishing,
- поширення шкідливих вкладень та посилань.

За 2020 рік 44% компаній з кількістю працівників 250-500 повідомили, що у них відбувався витік інформації через атаки з використанням соціальної інженерії. Варто звернути увагу на те, що 88% компаній-представників малого бізнесу, таких як наш інтернет магазин вважають, що їх дані є «ймовірною» метою для кіберзлочинців, а 46% - «дуже ймовірною» метою. Так, за 2020 рік в результаті кібератак компанії в США втратили більше 2,700,000,000 доларів.

**Висновки до розділу 3**

Проаналізували основні загрози 2020 року, такі як зорстання числа програм-шифрувальників, Remote Access Trojans, погіршення ситуації з випадками атак з використанням соціальної інженерії.

Взяли до уваги той факт, що найпопулярнішим способом потрапляння зловмисного ПЗ є електронна пошта.

З урахуванням того факту, що кількість загроз і атак в цілому зросла (причиною є як суцільний перехід на віддалену роботу, так і ріст IT-індустрії взагалі), зібрали усі необхідні дані для побудови ризик-аналізу доступу до конфіденційних даних інтернет магазину.

# 4 РИЗИК-АНАЛІЗ ДОСТУПУ ДО КОНФІДЕНЦІЙНИХ ДАНИХ ІНТЕРНЕТ МАГАЗИНУ

На основі 3 розділу можемо виділити основні дії (А) і загрози, з якими стикається типовий інтернет-магазин. Здійснемо їх аналіз за допомогою інтегрованого методу, статистичного методу, побудуємо таблицю ризиків.

## 4.1 Статистичний метод аналізу ризиків для інтернет магазину

Спираючись на статистичні дані атак за 2020 рік, опубліковані в мережі інтернет судження експертів та аналітиків та звітів компаній можемо побудувати наступний графік:

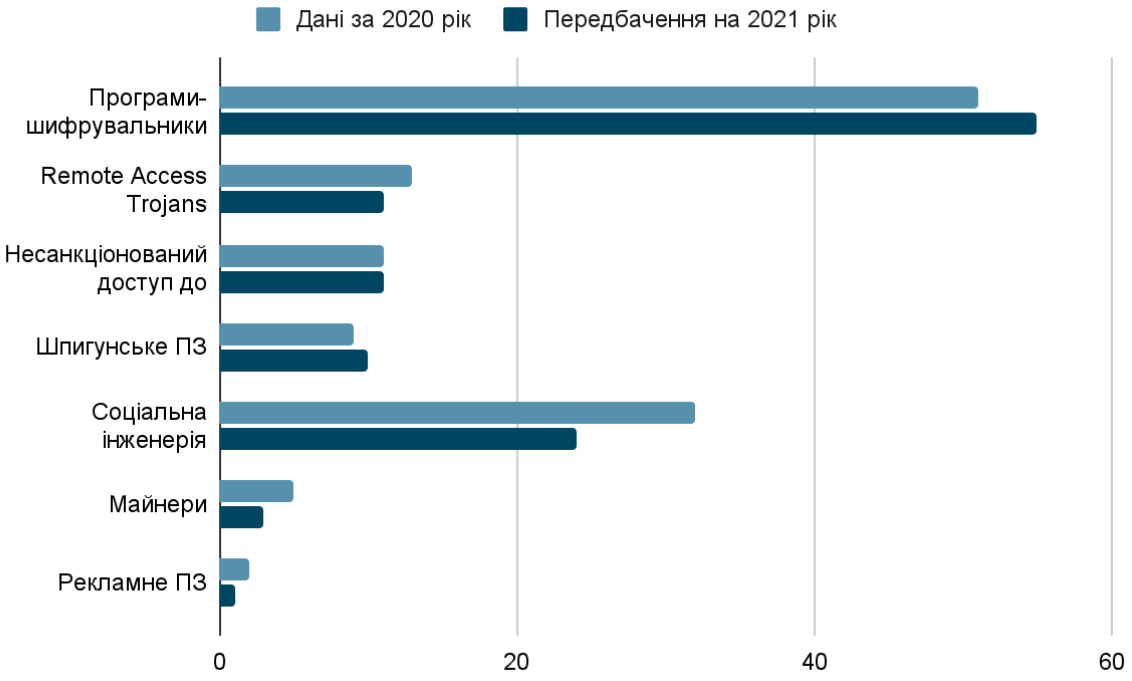


Рисунок 4.1 - Випадки атак за 2020 рік

Як бачимо з діаграми кількість атак, що прогнозують експерти тільки зросте. Також, на основі статистичних даних можна зробити висновки щодо областей, які є найбільш потенційно небезпечними.

### 4.2 Інтегрований метод АОР в інтернет магазині

Розглянемо на прикладі інтернет магазину роботу інтегрованого методу АОР. Нехай експерти визначили ІР для АОР $IP_1$ = “інтернет магазин”

- **Крок 1**. На основі статистичних даних за 2020 рік цьому інформаційному ресурсі були визначені наступні загрози **A** $\in \{A_a\}(a = \overline{1,7})$:

  $A_1$ = «Програми-шифрувальники»;

  $A_2$ = «Remote Access Trojans»;

  $A_3$ = «Несанкціонований доступ до корпоративної мережі»;

  $A_4$ = «Шпигунське ПЗ»;

  $A_5$ = «Соціальна інженерія».

  $A_6$ = «Майнери»;

  $A_7$ = «Рекламне ПЗ».

- **Крок 2.** Для оцінки ризику визначено такі множини: **DR**, $\mathbf{EK}_i$, скористаємося множиною оціночних компонент з кодом 2F, тоді $EK_{2F} \in \{EK_i\} = \{EK_1, EK_2, EK_3, EK_4\} = \{D, P, L, F\}$

Тобто, для кожної загрози будемо оцінювати її ймовірність, небезпеку, частоту та витрати.

- **Крок 3.** Визначимо кількості необхідних терм-множин для АОР, нехай m = 5.
- **Крок 4.** Оцінку **LS** здійснимо за формулою

  $1 / i\ LS_i = 1/ g = 0{,}25\ (i = \overline{1,4})$.

- **Крок 5**. Розглянемо випадок, коли експерти визначили для оцінювання базові терм-множини для m = 5 - $\bigcup_{j=1}^{5} T_{DR_J}$ ={

❖ «Незначний ризик порушення ІБ »(НР),
❖ «Ступінь ризику порушення ІБ низька »(РН),

- « Ступінь ризику порушення ІБ середня »(РС),
- « Ступінь ризику порушення ІБ висока »(РВ),
- « Граничний ризик порушення ІБ »(ПР)}

і $\bigcup_{j=1}^{5} T_{K_{EK_i\ J}}$ = {«Дуже низький» (ОН),

«низький» (Н),

«середній» (З),

«високий» (В),

«дуже високий» (ОВ)}.

Таблиця 4.1 - Приклад значень інтервалів

| **Интервали** | **Терми** | $\mu_j(dr)$ |
|---|---|---|
| [0; 10] | $T_{DR1}$ | 1 |
| [10; 20] | $T_{DR1}$ | $\mu_1(dr)$= (20-dr)/10 |
| | $T_{DR2}$ | $\mu_{j2}(dr)$= 1 -$\mu_1(dr)$ |
| [20; 30] | $T_{DR2}$ | 1 |
| [30; 40] | $T_{DR2}$ | $\mu_2(dr)$= (40-dr)/10 |
| | $T_{DR3}$ | $\mu_3(dr)$= 1 -$\mu_2(dr)$ |
| [40; 50] | $T_{DR3}$ | 1 |
| [50; 60] | $T_{DR3}$ | $\mu_3(dr)$= (60-dr)/10 |
| | $T_{DR4}$ | $\mu_4(dr)$= 1 -$\mu_3(dr)$ |
| [60; 70] | $T_{DR4}$ | 1 |
| [70; 80] | $T_{DR4}$ | $\mu_4(dr)$= (80-dr)/10 |
| | $T_{DR5}$ | $\mu_5(dr)$= 1 -$\mu_4(dr)$ |
| [80; 100] | $T_{DR5}$ | 1 |

- **Крок 6.** Поточний стан ІБ $IP_1$ характеризується значеннями оціночних компонент ek по кожному A, які визначаються на основі експертних суджень. Для здійснення подальших розрахунків будуть використовуватися дані представлені в Таблиці 4.2.

Таблиця 4.2 - Класифікація поточних значень компонент

| $EK_i$ | $ek_i^{A_1}$ | $ek_i^{A_2}$ | $ek_i^{A_3}$ | $ek_i^{A_4}$ | $ek_i^{A_5}$ | $ek_i^{A_6}$ | $ek_i^{A_7}$ |
|---|---|---|---|---|---|---|---|
| **P** | 90 | 60 | 43 | 56 | 57 | 21 | 9 |
| **L** | 0,4 | 0,35 | 0,39 | 0,31 | 0,25 | 0,12 | 0,05 |
| **D** | 7 | 7 | 6 | 5 | 5 | 2 | 1 |
| **F** | 0,80 | 0,73 | 0,43 | 0,37 | 0,54 | 0,3 | 0,2 |

- **Крок 7**. Далі проводиться класифікація поточних значень $ek_i^A$ за формулою (2.4), а результати заносяться в Таблицю 4.3.

Таблиця 4.3 - Приклад значень інтервалів

| $EK_i$ | | **P** | **L** | **D** | **F** |
|---|---|---|---|---|---|
| Значення $\lambda$ дл $\in \{A_a\}(a = \overline{1,7})$ | $\lambda_{ij}^{(A_1)}$ для $T_{K_{EKim}}$ $(i = \overline{1,4}), (j = \overline{1,5})$ | 0 | 0 | 0 | 0 |
| | | 0 | 0 | 0 | 0 |
| | | 0 | 0 | 0 | 0 |
| | | 0 | **0,6** | **1** | 0 |
| | | **1** | **0,4** | 0 | **1** |

| | | | | | |
|---|---|---|---|---|---|
| | $\lambda_{ij}^{(A_2)}$ для $T_{K_{EKim}}$ $(i = \overline{1,4}), (j = \overline{1,5})$ | 0 | 0 | 0 | 0 |
| | | 0 | 0 | 0 | 0 |
| | | **0,6** | 0 | 0 | 0 |
| | | **0,4** | **1** | **1** | **1** |
| | | 0 | 0 | 0 | 0 |
| | $\lambda_{ij}^{(A_3)}$ для $T_{K_{EKim}}$ $(i = \overline{1,4}), (j = \overline{1,5})$ | 0 | 0 | 0 | 0 |
| | | **0,6** | 0 | 0 | 0 |
| | | **0,4** | **0,6** | **0,5** | **1** |
| | | 0 | **0,4** | **0,5** | 0 |
| | | 0 | 0 | 0 | 0 |
| | $\lambda_{ij}^{(A_4)}$ для $T_{K_{EKim}}$ $(i = \overline{1,4}), (j = \overline{1,5})$ | 0 | 0 | 0 | 0 |
| | | 0 | 0 | **0,6** | **1** |
| | | **1** | **1** | **0,4** | 0 |
| | | 0 | 0 | 0 | 0 |
| | | 0 | 0 | 0 | 0 |
| | $\lambda_{ij}^{(A_5)}$ для $T_{K_{EKim}}$ $(i = \overline{1,4}), (j = \overline{1,5})$ | 0 | 0 | 0 | 0 |
| | | 0 | **0,6** | **0,6** | 0 |
| | | **1** | **0,4** | **0,4** | **0,6** |
| | | 0 | 0 | 0 | **0,4** |
| | | 0 | 0 | 0 | 0 |

Кінець таблиці 4.3

| | | | | | |
|---|---|---|---|---|---|
| | $\lambda_{ij}^{(A_6)}$ для $T_{K_{EKim}}$ $(i = \overline{1,4}), (j = \overline{1,5})$ | **0,4** | **1** | **1** | 0 |
| | | **0,6** | 0 | 0 | **1** |
| | | 0 | 0 | 0 | 0 |
| | | 0 | 0 | 0 | 0 |
| | | 0 | 0 | 0 | 0 |
| | $\lambda_{ij}^{(A_7)}$ для $T_{K_{EKim}}$ $(i = \overline{1,4}), (j = \overline{1,5})$ | **1** | 1 | 1 | **0,6** |
| | | 0 | 0 | 0 | **0,4** |
| | | 0 | 0 | 0 | 0 |
| | | 0 | 0 | 0 | 0 |
| | | 0 | 0 | 0 | 0 |

- **Крок 8.** Зробимо обчислення показника ступеня ризику порушення ІБ за формулою (2.6), де m = 5, j =$\overline{1,5}$, i =$\overline{1,4}$, a =$\overline{1,7}$, $dr_1 = 10$, $dr_2 = 30$, $dr_3 = 50$, $dr_4 = 70$, $dr_5 = 90$, тоді

$$dr^{(A_1)} = 91,$$
$$dr^{(A_2)} = 83,$$
$$dr^{(A_3)} = 79,$$
$$dr^{(A_4)} = 64,$$
$$dr^{(A_5)} = 57{,}5,$$
$$dr^{(A_6)} = 23,$$
$$dr^{(A_7)} = 13.$$

- **Крок 9**. Формуємо $SP^{(A_a)}$:

$$SP^{(A_1)}=(dr^{(A_1)};T_{DR_4}) = (91; \text{КР}),$$

$$SP^{(A_2)}= (dr^{(A_2)};T_{DR_4}) = (83; \text{КР}),$$

$$SP^{(A_3)}= (dr^{(A_3)};T_{DR_4}) = (79; \text{ВС}),$$

$$SP^{(A_4)}= (dr^{(A_4)};T_{DR_4}) = (64; \text{ВР}),$$

$$SP^{(A_5)}= (dr^{(A_5)};T_{DR_4}) = (57{,}5; \text{СР}),$$

$$SP^{(A_6)}= (dr^{(A_6)};T_{DR_4}) = (23; \text{РН}),$$

$$SP^{(A_7)}= (dr^{(A_7)};T_{DR_4}) = (13; \text{НР}).$$

Також для даного ІР на основі виразу (2.7), можна обчислити середнє значення ступеня ризику:

$$dr^{(\text{ср})}= (91+83+79+64+57{,}5+23+13)/7 = 58{,}5$$

$$SP^{(\text{ср})}= (58{,}5; \text{СР})$$

Отже, для обраної інформаційної системи оцінка ризику складає 58,5.

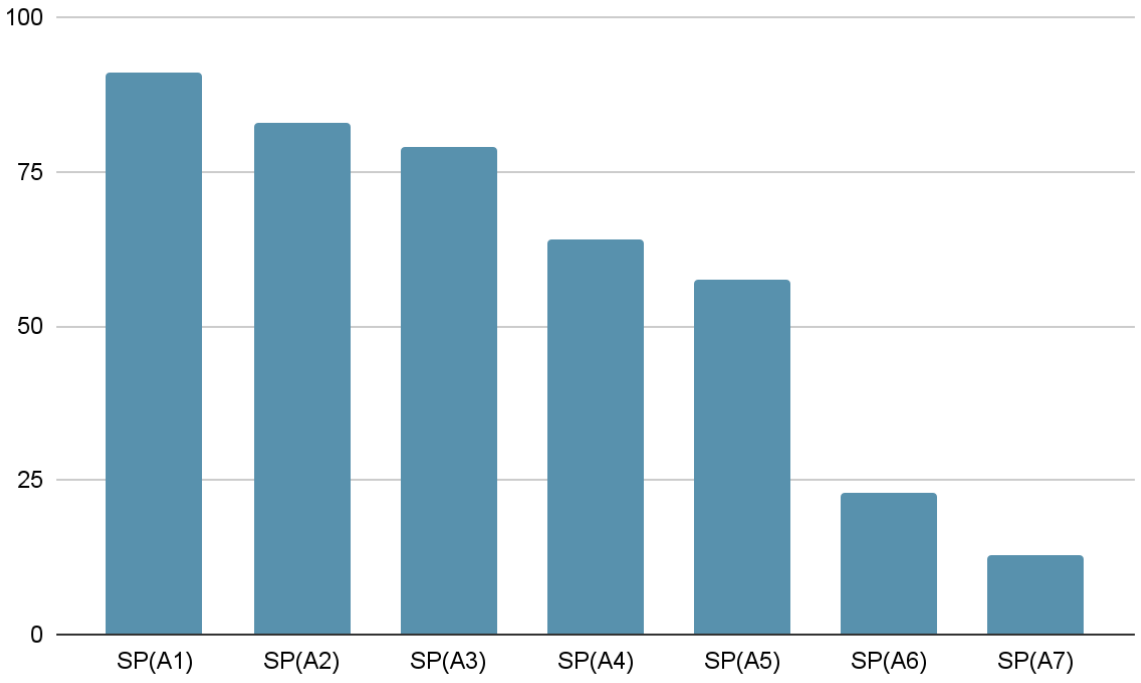


Рисунок 4.1 - Висновки інтегрованого методу аналізу ризиків

На основі отриманих вище даних можемо побудувати таблицю з висновками.

Таблиця 4.4 - Типові загрози

| № | Назва загрози | Причини виникнення | Наслідки | Дії для попередження загро |
|---|---|---|---|---|
| 1. | Програми-шифрувальники (Sodinokibi, Phobos,Netwalker т інші) | відсутність антивірусного софу в системі; відсутність знань основ кібербезпеки персоналу | можливе призупинення роботи працівників, як наслідок - магазину в цілому | інструктажі серед персоналу, встановлення антивірусного софту, фаєрволів |
| 2. | Remote Access Trojans (RAT) | відсутність специфічного софу в системі; відсутність знань основ кібербезпеки персоналу | можливий витік/модифікація персональних даних, повна втрата даних | інструктажі серед персоналу, встановлення специфічного софту, фаєрволів |
| 3. | Шпигунське ПЗ | відсутність специфічного софу в системі; відсутність знань основ кібербезпеки персоналу | можливий витік/модифікація персональних даних | інструктажі серед персоналу, встановлення антивірусного софту, фаєрволів |
| 4. | Несанкціонований доступ до корпоративної мережі | недосконалість механізмів автентифікації та ідентифікації | можливий витік/модифікація персональних даних | покращити механізми аутентифікації та ідентифікації |
| 5. | Майнери | ігнорування контролю трафіку | можливий витік персональних даних | Встановлення відповідного ПЗ |
| 6. | Рекламне ПЗ | відсутність відповідних правил | можливий витік/модифікація персональних даних | Встановлення відповідного ПЗ |
| 7. | Соціальна інженерія | відсутність знань основ кібербезпеки персоналу | можливий витік персональних даних | інструктажі серед персоналу |

Отже, через глобальну епідемію, кількість людей, що почали працювати онлайн значно зросла. Різноманітні бізнеси постали перед вибором - або перенести свою діяльність в інтернет, або зачинитись. Як висновок - стрімкий ріст атак типу Remote Access Trojans (RAT); Phobos, Netwalker і т.п. Найбільш серйозною кібератакою за минулий рік є розповсюдження програм-шифрувальників. 51% компаній зіткнулися з цією загрозою.

Ризики перехоплення інформації, атак за допомогою соціальної інженерії також залишаються на достатньо високому рівні.

**Висновки до розділу 4**

Провели ризик-аналіз для типового інтернет магазину на основі найпопулярніших загроз за 2020 рік. Отримані дані можна використовувати при створенні системи управління ризиками та плану забезпечення безперервності та відновлення діяльності не тільки інтернет магазину, а й іншим компаніям, що працюють в мережі інтернет.

Таблиця 4.5 - Таблиця ризиків

| № | Назва загрози | Вплив загрози на систему | Ймовірність реалізації атаки | Загальний рівень |
|---|---|---|---|---|
| 1. | Програми-шифрувальники | Високий вплив | Дуже висока | Високий рівень |
| 2. | Remote Access Trojans | Високий вплив | Висока | Високий рівень |
| 3. | Несанкціонований доступ до корпоративної мережі | Високий вплив | Висока | Високий рівень |
| 4. | Шпигунське ПЗ | Високий вплив | Середня | Високий рівень |
| 5. | Соціальна інженерія | Середній вплив | Середня | Високий рівень |
| 6. | Майнери | Середній вплив | Низька | Середній рівень |
| 7. | Рекламне ПЗ | Дуже низький вплив | Дуже низька | Середній рівень |

# 5 РЕКОМЕНДАЦІЇ ЩОДО ЛІКВІДАЦІЇ ТИПОВИХ ЗАГРОЗ

На основі отриманих вище даних можна виділити наступні рекомендації.

## 5.1 Використання ефективних технічних засобів захисту

- Створення систем централізованого управління оновленнями для використовуваного ПЗ. Необхідно брати до уваги актуальну аналітику щодо ситуації в кібер-просторі для правильної приоритизации планів по оновленю ПЗ.
- Налаштуванн автоматизовуваних засобів аналізу захищеності і виявлення вразливостей в ПЗ.
- Створення систем антивірусного захисту з вбудованим ізольованим середовищем для динамічної перевірки файлів, які здатні виявляти і блокувати шкідливі файли в корпоративній електронній пошті до моменту їх відкриття співробітниками. Найбільш ефективним буде використання антивірусного ПЗ, побудованого на рішеннях одночасно декількох виробників, здатного виявляти приховану присутність шкідливих програм і дозволяє виявляти і блокувати шкідливу активність в різних потоках даних - в поштовому, мережевому і веб-трафіку, в файлових сховищах, на веб-порталах. Важливо, щоб обране рішення дозволяло перевіряти файли не тільки в реальному часі, а й автоматично аналізувало вже перевірені раніше, це дозволить виявити упущені раніше загрози при оновленні баз сигнатур.
- Автоматизувати засоби аналізу захищеності і виявлення вразливостей в ПО.
- Використовувати системи глибокого аналізу мережевого трафіку - для виявлення складних цільових атак як в реальному часі, так і в збережених копіях трафіку. Застосування такого рішення дозволить не тільки побачити не виявлені раніше факти злому, але і в режимі реального часу

відслідковувати мережеві атаки, в тому числі запуск шкідливого ПЗ і хакерських інструментів та атаки на контролер домену. Такий підхід дозволить істотно знизити час прихованої присутності порушника в інфраструктурі, і тим самим мінімізувати ризики витоку важливих даних і порушення роботи бізнес-систем, знизити можливі фінансові втрати від присутності зловмисників.

### 5.2 Захист даних

- Не треба зберігати важливу інформацію у відкритому вигляді або у відкритому доступі;
- регулярно створювати резервні копії систем і зберігати їх на виділених серверах окремо від мережевих сегментів робочих систем;
- мінімізуйте, наскільки це можливо, привілеї користувачів і служб;
- використовуйте різні облікові записи і паролі для доступу до різних ресурсів;
- застосовуйте двухфакторную аутентифікацію там, де це можливо, наприклад для захисту привілейованих облікових записів.

### 5.3 Контроль якості паролів

- Створити спеціальну “парольну політику”, яка передбачає суворі вимоги щодо мінімальної довжині паролів, її складності та наявності спеціальних символів;
- Розробити обмежений термін дії використання паролів (не більше 30;60;тощо днів).

### 5.4 Контроль безпеки систем:

- Постійне оновлення ПЗ;
- Постійна перевірка знань співробітників. Проведення тренінгів, лекцій для підвищення обізнаності співробітників в питаннях інформаційної безпеки;

- Контроль появи небезпечних ресурсів на периметрі мережі. Регулярна інвентаризація мережевих ресурсів, доступних для підключення. Аналіз публікацій про нові вразливості: це дозволяє оперативно виявляти такі уразливості в ресурсах компанії і своєчасно їх усувати;
- Ефективний фільтр трафіку для мінімізації доступних зловмисникові інтерфейсів мережевих служб; особливу увагу варто приділяти інтерфейсам віддаленого управління серверами і мережевим обладнанням;
- Регулярне тестування на проникнення для своєчасного виявлення нових векторів атак на внутрішню інфраструктуру і оцінки ефективності вжитих заходів щодо захисту;
- Регулярний аналіз захищеності веб-додатків, включаючи аналіз вихідного коду, з метою виявлення та усунення вразливостей, що дозволяють проводити атаки, в тому числі на клієнтів додатки;
- Відстежування кількості запитів до ресурсів в секунду, налаштвання конфігурацій серверів і мережевих пристроїв таким чином, щоб нейтралізувати типові сценарії атаки (наприклад, TCP- і UDP-флуд або множинні запити до БД).

### 5.5 Безпека клієнтів

- Регулярне підвищення обізнаності клієнтів в питаннях ІБ;
- Регулярне нагадування клієнтам про правила безпечної роботи в інтернеті, пояснення методів атак і способів захисту;
- Застереження клієнтів від введення облікових даних на підозрілих веб-ресурсах і тим більше від повідомлення такої інформації третім особам по електронній пошті або під час телефонної розмови;
- Пояснення клієнтам порядок дій в разі підозр про шахрайство;

### Висновки до розділу 5

Відзначався масовий сплеск числа загроз, причинами якого могли стати як прискорення цифровий трансформації у всіх індустріях, так і

повсюдний перехід на віддалену роботу. Протягом року кількість кібератак росло, підвищувалася їх складність, протистояти їм ставало все важче.

Розробили рекомендації щодо ліквідації найпоширініших і найнебезпечніших загроз з боку ПЗ, технічної і соціальної складової.

# ВИСНОВКИ

В результаті роботи проаналізували ризики атак несанкціонованого доступу до конфіденційних даних інтернет магазину. Проаналізували ситуацію з кібер-атаками за минулий рік, ознайомились з їх аналітикою.

Побудували таблиці ризиків для ліпшого оцінювання вразливих місць в системі, а запропонований метод на відміну від відомих надає можливість оперувати одночасно чіткими і нечіткими параметрами з вибором необхідної кількості терм-множин, що спрощує процес АОР.

Прийшли до висновку, що найбільш небезпечними є загрози, після реалізації яких зловмисник отримує повний контроль над системою, в тому числі доступ до конфіденційних даних. Необхідно слідкувати за всіма аспектами безпеки, починаючи від надання інструктажів працівникам, закінчуючи постійним оновленням ПЗ.

Все більше і більше різноманітних бізнесів і підприємств будуть переходити в онлайн режим, тому аналіз можливих ризиків є важливою складовою забезпечення кібербезпеки.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

- Корченко А.Г. Методы анализа и оценки рисков потерь государственных информационных ре- сурсов / А.Г. Корченко, В.П. Щербина, С.В. Казмирчук // Защита информации – 2012. – No1. – С. 126-139
- Казмирчук С.В. Анализ и оценивание рисков информационных ресурсов / С.В. Казмирчук // Защита информации – 2013. – Том 15 No1 (58). – С. 37-46.
- Казмирчук С.В. Анализа и оценивания рисков информационных ресурсов в нечетких условиях / С.В. Казмирчук // Защита информации – 2013. – Том 15 No2 (59). – С. 133-140.
- Корченко А.Г. Интегрированное представление параметров риска / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2011. – No1 (50). – С. 96 – 101
- “Cisco Cybersecurity Reports” [Електронний ресурс] - https://www.cisco.com/c/en/us/products/security/cybersecurity-reports.html#~get-the-report
- “Positive Technologies 2021” [Електронний ресурс] - https://www.ptsecurity.com/ru-ru/research/analytics/positive-research-2021/
- “Positive Technologies 2020” [Електронний ресурс] - https://www.ptsecurity.com/ru-ru/research/analytics/positive-research-2020/
- “Управление рисками кибербезопасности” [Електронний ресурс] - https://www.securityvision.ru/modules/upravlenie-riskami-kiberbezopasnosti/
- “Кибербезопасность: стратегии атак и обороны”/Юрий Диогенес, Эрдаль Озкайя// 2020
- Симонов С. С. Технологии и инструментарий для управления рисками / Симонов С. С. // Информационный бюллетень Jet Info. – 2003. – No 2 (117)/2003.
- Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А.Г. – К. : “МК-Пресс”, 2006.

- Монте-Карло для аналитиков. Как грамотно моделировать и измерять риски. [Электронный ресурс] / Андрей Лукашов // Риск-менеджмент. – 2007. – No3. – Режим доступа: http://www.ecsocman.edu.ru/images/pubs/2007/04/27/0000307302/72-77-praktikum_-_lukashev_SCR.pdf