Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(ступінь підготовки)

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

напрям підготовки (спеціальність) *125 Кібербезпека*
(код і назва напряму підготовки)

спеціалізація (освітня програма) *Кібербезпека*
(код і назва спеціальності)

ступінь підготовки *магістр*
(назва освітнього рівня)

кваліфікація *професіонал із організації інформаційної безпеки*
(код і назва кваліфікації)

на тему: ***Управління інцидентами кібербезпеки на малих комерційних підприємствах***

Виконавець: студент ***2*** **курсу, групи** ***125м-16-1***

(підпис) ***Твердохліб Ігор Сергійович*** (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
роботи	к.ф.-м.н., доц.. Гусєв О.Ю.		
розділів:			
спеціальний	ас. Ковальова Ю.В.		
економічний	к.е.н., доц. Волотковська Ю.О.		
Рецензент			
Нормоконтроль			

Дніпро
2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
д.т.н., проф. _____ Корнієнко В.І.

«_____»_____2018 року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту ***125м-16-1*** ***Твердохлібу Ігорю Сергійовичу***
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи ***Управління інцидентами кібербезпеки на малих комерційних підприємствах***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від «26» грудня 2017 р. № 2127-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *процес управління інцидентами кібербезпеки на малих комерційних підприємствах*

Предмет досліджень *протидія інцидентам кібербезпеки*

Мета НДР *забезпечити застосування послідовного і результативного підходу до управління інцидентами кібербезпеки, як до важливої складової системи менеджменту інформаційної безпеки на малих комерційних підприємствах*

Вихідні дані для проведення роботи *законодавство України та міжнародні стандарти у сфері кібербезпеки, наукові публікації вітчизняних та іноземних авторів, міжнародні статистичні дані з інцидентів та загроз кібербезпеки, показники діяльності підприємства*

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *полягає у розробці рекомендаційних методик щодо управління інцидентами кібербезпеки для малих комерційних підприємств*

Практична цінність *полягає у розробці на малих комерційних підприємствах послідовного і результативного підходу до вирішення питання управління інцидентами кібербезпеки*

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати роботи мають відповідати вимогам чинного законодавства України та міжнародним стандартам кібербезпеки, бути поданими у вигляді, що дозволяє безпосереднє використовування рекомендацій щодо управління інцидентами на малих комерційних підприємствах

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Аналіз стандартів і нормативно-правової бази з управління інцидентами кібербезпеки та міжнародної статистики з реалізації інцидентів. Аналіз актуальних проблем забезпечення кібербезпеки.	1 вересня 2017 р. – 25 вересня 2017 р.
Формування загальних вимог для процесів управління інцидентів кібербезпеки	26 вересня 2017 р. – 15 жовтня 2017 р.
Формування інформативної бази щодо планування системи управління інцидентами кібербезпеки	16 жовтня 2017 р. – 5 листопада 2017 р.
Розробка рекомендації щодо застосування системи управління інцидентами, аналізу обробки інцидентів, покращення системи управління інцидентами та складання рекомендаційних інструментів	6 листопада 2017 р. – 20 грудня 2017 р.
Визначення капітальних та експлуатаційних витрат на реалізацію запропонованих рекомендацій стосовно управління інцидентами кібербезпеки	21 грудня 2017 р. – 1 січня 2018 р.
Оформлення технічної документації	2 січня 2018 р. – 15 січня 2018 р.

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *від реалізації результатів роботи очікується позивтиним завдяки зниженню можливого збитку підприємства від інцидентів кібербезпеки через застосування запропонованих у дипломній роботі рекомендацій щодо процесів управління інцидентами кібербезпеки орієнтованих на малі комерційні підприємства*

Соціальний ефект *дипломної роботи, полягає у результативному і доцільному підході до управління інцидентами кібербезпеки, що зменшить можливість втрати важливої інформації,зменшить час відновлення системи після виникнення інциденту та підвищить впевненість власників, партнерів та клієнтів у надійності підприємства*

7 ДОДАТКОВІ ВИМОГИ

Відповідність оформлення пояснювальної записки:
ДСТУ 3008-95. «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення».
Бабенко Т.В. Методичні вимоги до підготовки та захисту дипломної роботи (проекту) для студентів галузей знань 1701 «Інформаційна безпека» та спеціальності 125 «Кібербезпека» / Бабенко Т.В., Корнєєв М.В., Кручінін О.В., Тимофєєв Д.С.; Нац. гірн. ун-т. – Д: НГУ, 2016. – 45 с.
Бабенко Т.В. Методичні вимоги до підготовки та захисту дипломної роботи

Завдання видав _____ О.Ю. Гусєв
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ І. С. Твердохліб
(підпис) (прізвище, ініціали)

Дата видачі завдання: 01.09.2017

Термін подання дипломної роботи до ДЕК 19.01.2018

РЕФЕРАТ

Пояснювальна записка: ___ с., __ рис., __табл., __ додатків, __ джерел.

Об’єкт дослідження: процес управління інцидентами кібербезпеки на малих комерційних підприємствах

Мета роботи: підготовка обґрунтованої рекомендаційної бази з управління інцидентами кібербезпеки для рядових співробітників і керівників малих комерційних підприємств.

Методи дослідження: порівняння, статистичний аналіз, моделювання.

У спеціальній частині досліджено теоретичну базу у сфері управління інформаційною безпекою та кібербезпекою в питаннях протидії інцидентам кібербезпеки. Проаналізовані актуальні проблеми кібербезпеки та розглянута характеристика інформаційного середовища малих комерційних підприємств. Проаналізовані міжнародні стандарти з управління інформаційною безпекою та на їх основі були сформовані загальні вимоги для управління інцидентами кібербезпеки.

У роботі розроблено рекомендаційну базу для управління інцидентами кібербезпеки. Для цього розроблено методичні вказівки для підвищення обізнаності персоналу у питаннях планування системи управління інцидентами, аналізу їх обробки, покращення системи. На прикладі підприємства було розглянуто управління типовими інцидентами.

В економічній частині проведено розрахунок вартості розробки, впровадження та підтримки рекомендованих методик і обґрунтовано їх економічну доцільність.

Практичне значення роботи полягає у розробці на малих комерційних підприємствах послідовного і результативного підходу до вирішення питання управління інцидентами кібербезпеки

Наукова новизна роботи полягає у розробці рекомендаційних методик щодо управління інцидентами кібербезпеки для малих комерційних підприємств

Ключові слова: ІНЦИДЕНТ КІБЕРБЕЗПЕКИ, ЗАГРОЗИ КІБЕРБЕЗПЕКИ, МАЛІ КОМЕРЦІЙНІ ПІДПРИЄМСТВА, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

РЕФЕРАТ

Объяснительная записка: ___ с., __ рис., __табл., __ приложений, __ источников.

Объект исследования: процесс управления инцидентами кибербезопасности на малых коммерческих предприятиях.

Цель работы: подготовка обоснованной рекомендательной базы по управлению инцидентами кибербезопасности для рядовых сотрудников и руководителей малых коммерческих предприятий.

Методы исследования: сравнение, статистический анализ, моделирование.

В специальной части исследовано теоретическую базу в области управления информационной безопасностью и кибербезопасностью в вопросах противодействия инцидентам кибербезопасности. Проанализированы актуальные проблемы кибербезопасности и рассмотрена характеристика информационной среды малых коммерческих предприятий. Проанализированы международные стандарты по управлению информационной безопасностью и на их основе были сформированы общие требования для управления инцидентами кибербезопасности.

В работе разработана рекомендательная база для управления инцидентами кибербезопасности. Для этого разработаны методические указания для повышения осведомленности персонала в вопросах планирования системы управления инцидентами, анализа их обработки, улучшение системы. На примере были рассмотрены управления типичными инцидентами.

В экономической части произведен расчет стоимости разработки, внедрения и поддержки рекомендованных методик и обосновано их экономическую целесообразность.

Практическое значение работы состоит в разработке на малых коммерческих предприятиях последовательного и результативного подхода к решению вопроса управления инцидентами кибербезопасности

Научная новизна работы заключается в разработке рекомендательных методик по управлению инцидентами кибербезопасности для малых коммерческих предприятий.

Ключевые слова: ИНЦИДЕНТ КИБЕРБЕЗОПАСНОСТИ, УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ, МАЛЫЕ КОММЕРЧЕСКИЕ ПРЕДПРИЯТИЯ, УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ.

ABSTRACT

Explanatory note: ___ p., __ fig., __ tables, __ sources.

Object of study: cybersecurity incident management process for small businesses.

The aim of research paper: to develop a justified methodology for managing cybersecurity incidents for ordinary employees and managers of small business enterprises.

Research methods: comparison, statistical analysis, modeling.

In the special part the theoretical basis in the field of information security and cybersecurity management in the issues of countering incidents of cybersecurity is researched. The actual problems of cybersecurity are analyzed and the characteristics of the information environment of small commercial enterprises are considered. The international standards for information security management were analyzed and on the basis of them were formed the general requirements for managing cybersecurity incidents.

The paper has developed a reference framework for managing cyber security incidents. To do this, methodological guidelines have been developed to raise awareness among staff in planning incident management systems, analyzing their processing, and improving the system. The example considered the management of typical incidents.

In the economic part, the calculation of the cost of development, implementation and support of the recommended methods is carried out and their economic feasibility is justified.

The practical value of the work consists in developing a consistent and effective approach to solving the problem of cybersecurity incidents management at small commercial enterprises.

The scientific novelty of the work is to develop advisory methods for managing cybersecurity incidents for small business enterprises.

Key words: INCIDENT OF CYBERSECURITY, THREATS OF CYBERSECURITY, SMALL BUSINESS ENTERPRISES, INFORMATION SECURITY MANAGEMENT

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ВПЗ – Відмітка про завершення;

ЗУ – Закон України;

ІБ – інформаційна безпека;

ІКТ – інформаційні і комунікаційні технології;

ІТ – інформаційні технології;

НД ТЗІ – нормативний документ технічного захисту інформації;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ПП – приватне підприємство;

УІІБ – управління інцидентами інформаційної безпеки;

СВВ – система виявлення вторгнень;

СУІІБ – система управління інцидентами інформаційної безпеки;

DoS – Denial of service;

DLP – Data Leak Prevention;

ISO/IEC – International Organization for Standardization/International Electrotechnical Commission;

MBR – Master boot record.

ЗМІСТ

ВСТУП

Актуальність. Питання забезпечення інформаційної безпеки на малих комерційних підприємствах актуальне в наш час, як ніколи раніше. Відповідно, і питання запобігання появи небажаних або несподіваних подій ІБ, інцидентів, з якими пов'язана значна вірогідність компрометації бізнес-операцій та створення загроз ІБ, теж актуальні. А виходячи з того, що значна частина існуючих організацій та підприємств складають малі приватні підприємства, даний питання стає особливо гострим і важливим, якому необхідно приділити належну увагу. В сучасному бізнесі інформаційні технології є невід’ємною частиною процесу управління бізнесом. Адже, всі підприємства функціонують в інформаційному середовищі. Для отримання комерційної вигоди підприємствам важливо зберігати цілісність, доступність і конфіденційність своїх інформаційних активів. Інформація може коштувати дуже багато в наші часи, тому для запобігання її витоку необхідно налагодити ефективний і раціональний процес управління інформаційною безпекою. Загроз кібербезпеці з кожним днем становиться все більше і більше, і зловмисники щодня збільшують досвід і вміння, їх технічний рівень дозволяє швидко і непомітно отримувати важливу їм інформацію незаконними шляхами. Частота виникнення і кількість інцидентів, пов'язаних з інформаційною безпекою, - один з наочних показників того, чи правильно функціонує система управління безпекою. Важливою складовою загальної стратегії забезпечення ІБ підприємства є структурований підхід до управління інцидентами інформаційної безпеки, в тому числі до управління інцидентами кібербезпеки. Метою такого підходу є побудова системи управління інцидентами ІБ, в рамках якої реалізується система управління інцидентами кібербезпеки.

Метою роботи є підготовка обґрунтованої рекомендаційної бази з управління інцидентами кібербезпеки для рядових співробітників і керівників малих комерційних підприємств.

У роботі були поставлені наступні завдання:

- аналіз нормативно-правової бази у сфері управління інформаційною безпекою;
- дослідження існуючих методів управління інцидентами кібербезпеки;
- планування системи управління інцидентами кібербезпеки;
- застосування системи управління інцидентами кібербезпеки;
- аналіз обробки інцидентів кібербезпеки;
- покращення системи управління інцидентами кібербезпеки;
- управління основними видами інцидентів на прикладі підприємства.

Об’єктом досліджень є процес управління інцидентами кібербезпеки.

Предметом досліджень є протидія інцидентам кібербезпеки.

Наукова новизна роботи полягає у розробці рекомендаційних методик щодо управління інцидентами кібербезпеки для малих комерційних підприємств.

Практична цінність полягає у розробці на малих комерційних підприємствах послідовного і результативного підходу до вирішення питання управління інцидентами кібербезпеки.

РОЗДІЛ 1
АНАЛІЗ ПРОЦЕСУ УПРАВЛІННЯ ІНЦИДЕНТАМИ В ПРОЦЕСІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

1.1 Характеристика інформаційного середовища малих комерційних підприємств

В сучасності інформація виступає як один з першорядних ресурсів, значення якого не менше, ніж значення матеріальних, сировинних і інших ресурсів. Використання останніх в значній мірі залежить саме від стану і використання інформації. На відміну від більшості ресурсів, які здатні виснажуватися, інформаційний потенціал може використаний багаторазово як колективами, так і індивідуальними працівниками. При цьому він постійно збільшується і збагачується.

У сучасних умовах важливим та гострим питанням стало питання інформаційного забезпечення, яке полягає в зборі та переробці інформації, необхідної для поняття обґрунтованих управлінських рішень. Передача інформації про стан і діяльність підприємства на вищий рівень управління і взаємний обмін інформацією між усіма взаємопов'язаними підприємства здійснюється на базі сучасної електронно-обчислювальної техніки та інших технічних засобів зв'язку.

Існує низка підходів до визначення поняття «інформаційне середовище»:

– інформаційне середовище – це сукупність технічних і програмних засобів зберігання, обробки і передачі інформації, а також політичні, економічні і культурні умови реалізації процесів інформатизації;

– інформаційне середовище – це світ інформації навколо людини і світ її інформаційної діяльності;

– інформаційне середовище – це сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням, споживанням інформації.

Підприємство – це стійка формальна соціальна структура, яка бере ресурси з навколишнього середовища і обробляє їх, щоб виробити продукцію.

Згідно до Господарського кодексу України, а саме до статті 55 [1], підприємства класифікуються за розміром як:

– мікропідприємства (не більше 10 співробітників, валовий дохід – менше 2млн. євро;

– малі підприємства (не більше 50 співробітників, валовий дохід – менше 10 млн. євро);

– середні підприємства (не більше 250 співробітників, валовий дохід – менше 50 млн. євро);

– великі підприємства (більше 250 співробітників, валовий дохід – більше 50 млн. євро).

Комерційне підприємство – це таке, яке здійснює операції та угоди з купівлі-продажу або перепродажу товарів. Це – різні торговельні підприємства. Основна функція - доведення товару до споживача.[2]

З врахуванням вищесказаного можна дати наступне визначення малому підприємству: це іманентний елемент системи економічних відносин в економіці ринкового типу, який забезпечує її інноваційну активність і підтримує конкурентне середовище.

Малі підприємства пронизані безліччю інформаційних потоків. Ці потоки можна визначити як зовнішню і внутрішню інформаційні середовища будь-якого підприємства.

Зовнішні інформаційні потоки відображають відносини між підприємством і економічними і політичними суб'єктами, діючими за його межами. Вони визначають взаємодію між підприємством, його реальними і потенційними клієнтами, конкурентами, тощо. Підприємство повинно постійно стежити за основними компонентами зовнішнього середовища, до яких відносяться економічні, технологічні, політико-правові, соціально-культурні та фізико-екологічні фактори.

Мале підприємство суттєво залежить від змін у зовнішньому середовищі. Аналіз сприятливих зовнішніх можливостей і загроз діяльності підприємства передбачає збір, обробку, оцінку значущості для підприємства найважливіших

змін у зовнішньому середовищі. Підсумком аналізу стану і тенденцій змін зовнішнього середовища підприємства є перелік загроз і відкриваються сприятливих можливостей для підприємства.

Внутрішнє середовище організації є джерелом її життєвої сили. Воно містить в собі той потенціал, який дає можливість організації функціонувати, а, отже, існувати і виживати в певному проміжку часу. Внутрішнє середовище - це сукупність характеристик організації і її внутрішніх суб'єктів (сил, слабкостей її елементів і зв'язків між ними), що впливають на стан і перспективи підприємства. Як було сказано вище, одним з основних ресурсів управлінської діяльності організацій є інформаційний ресурс.

Згідно до Закону України «Про інформацію» [3], інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Інформаційне середовище - це система, яка реалізує автоматизований збір, обробку, маніпулювання даними й включає технічні засоби обробки даних, програмне забезпечення та обслуговуючий персонал. Інакше кажучи, інформаційна система - це комплексне поєднання обладнання (комп'ютерів), програмного забезпечення, процедур, документації і персоналу, відповідального за введення, рух, управління і дистрибуцію даних і інформації. Інформація є основою управління. З її допомогою реалізуються зв'язки певних об'єктів, зв'язку між керуючою і керованою підсистемами, між управлінськими ланками.

Інформація – основа управління підприємством, сполучна ланка всіх управлінських процесів: планування, реалізації, координування, оцінки, контролю, коригування тощо. У будь-якій організації циркулює величезний масив інформації, в зв'язку з цим, питання її класифікації стає ключовим. Класифікація з великою часткою умовності може бути за формою планування:

- оперативна – термінова інформація, яка використовується в операційному плануванні;

- стратегічна – використовувана в середньостроковому і довгостроковому плануванні (відрізняється від оперативної глибиною і охопленим періодом).

За джерела формування:

- внутрішня – циркулююча між управлінським апаратом і об'єктом управління. Внутрішня інформація виникає в самій системі управління, формується в межах організації. Вона відображає різні часові інтервали розвитку об'єкта управління, містить відомості про ланцюгах, завданнях діяльності структурних підрозділів, про хід виробничого процесу. Характер, обсяг і ступінь деталізації цієї інформації різні. Така інформація, як правило, призначена для використання всередині самої компанії.
- зовнішня – інформація про зовнішнє середовище організації, під якою розуміються, як зазначалося раніше, економічні та політичні суб'єкти, що діють за межами компанії і відносини з ними. До зовнішньої також можна віднести інформацію, яка збирається і розробляється статистичними агентствами, різними державними і громадськими організаціями, інформацію, опубліковану в ЗМІ; інформацію рекламного та комерційного характеру інших фірм.

За мети використання:

- звітно-статистична – інформація, яка відображає результати фактичної діяльності підприємства для вищих органів управління, структур державної статистики, податкової інспекції;
- планові – для побудови тактичного і стратегічного плану діяльності організації;
- економічна – це інформація, яка виникає і функціонує в зв'язку з виробничо-господарською діяльністю людей, відображаючи об'єктивні закономірності
- виробничих відносин. Економічна інформація дозволяє провести економічний аналіз і оцінити результати виробничо-господарської і фінансової діяльності, прогнозувати економічний розвиток і вибрати його оптимальний

варіант, охоплює характеристику всіх економічних процесів і явищ на підприємстві. Економічна інформація може існувати і у вигляді економічних показників, що відображають кількісну характеристику економічних процесів і явищ.

- рекламна – для просування, стимулювання попиту на товари і послуги компанії;
- іміджева – для створення сприятливого образу компанії у широкої громадськості і її ключових груп;
- управлінська – для прийняття управлінських рішень, це потоки повідомлень (даних), що характеризують стан економічної системи і забезпечують управління у відповідності з обраними цілями

По місцю використання (призначенню):

- інформація для внутрішнього використання – найчастіше відображає фінансово-господарський стан організації. Наприклад, дані про чистий прибуток, витрати, методи збуту, техніках продажів, постачання і т.д .;
- інформація для зовнішнього використання – будь-яка інформація для поширення в ЗМІ, серед діючих і потенційних клієнтів, конкурентів, галузевого співтовариства і для широкої громадськості.

У розвитку організацій в даний час велику роль відіграє його інформатизація. У конкурентній боротьбі вирішальне значення набувають питання насичення виробництва потоками інформації і управління цими потоками. Щоб керівник мав можливість більш ефективно використовувати інформацію, він повинен отримувати її в меншому обсязі, більш концентрованою і відповідної тим завданням, які вирішуються на даному рівні управління. Зазвичай тільки незначна частина чинників має істотне значення при прийнятті рішень. Тому основну масу даних, які виникають при функціонуванні об'єктів, слід ретельно фільтрувати і тільки необхідні дані передавати в підсистеми управління для прийняття відповідних дій.

Важливою складовою інформаційного середовища є інформаційні технології. Згідно Закону України «Про Національну програму

інформатизації» [4], інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування.

Застосування інформаційних технологій дозволяє підприємству:

- швидко реагувати на зміну споживчих переваг і зовнішньої конкурентного середовища;
- скорочувати тривалість періоду розробки товару до його виведення на ринок;
- скорочувати терміни доставки;
- чітко виконувати замовлення;
- використовувати індивідуальний підхід до обслуговування споживачів;
- оперативно впроваджувати нові технології і розвивати творчість і інноваційний процес;
- оперативно реагувати на розвиток конкуренції.

Витрати на інформаційні та комунікаційні технології мають пряме відношення до витрат малого підприємництва. Закупівля обчислювальної техніки і програмного забезпечення, оплата послуг зв'язку, навчання співробітників розробці і застосуванню ІКТ, розробка програмних засобів власними силами та інші витрати на ПЗ, все це важлива складова успішного функціонування підприємства.

Важливою складовою роботи малого підприємництва з боку інформаційної системи стала необхідність обміну інформацією, виходу в мережу і автоматизація ведення бухгалтерського обліку. Даний функціонал веде до зменшення часу на додаткові узгодження між підрозділами, значно знизився рівень витрат підприємства.

Для плідного розвитку малим підприємствам необхідні інформаційні технології. Система передачі інформації не можлива без технічного

забезпечення і устаткування. Передача і обмін інформацією на підприємстві здійснюються на базі комп'ютерів та інших технічних засобах зв'язку.

Можна впевнено затвердити, що інформаційні технології в бізнесі в реаліях сучасності йдуть зовсім поряд. Щоб бізнес функціонував коректно і приносив прибуток від своєї діяльності безперервно, інформаційні активи підприємства мають бути захищені від кіберзагроз настільки, наскільки це є реальним. Це стає можливим, коли на підприємстві ефективно застосовується система управління інформаційною безпекою.

Відповідно до Закону України від 2007 року №12 «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [5], інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

Але це не єдине визначення терміну «інформаційна безпека». В Законі України «Про телекомунікації» від 2004 року №12 [6], визначення інформаційної безпеки стосується не стільки інформаційної безпеки України, як безпеки узагальненої технічної системи, якої є телекомунікаційна мережа, а саме: «інформаційна безпека телекомунікаційних мереж – це здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації ».

У Законі України «Про інформацію» [7], який є базовим по нормативному закріпленню інформаційної сфери держави, визначення інформаційної безпеки немає, а в Законі України «Про основи національної безпеки України», який є основним орієнтиром забезпечення безпеки нашої держави, системну сутність інформаційної безпеки представлені як невід'ємну складову національної безпеки України без точного визначення цього поняття. Крім того, в цьому

законі замість поняття «інформаційна безпека України» використовується поняття «національна безпека України в інформаційній сфері».

Для початку треба відрізнити два дуже схожих, але різних по змісту термінів кібербезпеки та інформаційної безпеки. Для цього зануримося в нормативно-правову базу, та витягнемо з Законів України ці поняття.

Відповідно до Закону України від 2017 року №45 «Про основні засади забезпечення кібербезпеки України»[8], кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

На перший погляд визначення термінів «кібербезпеки» і «інформаційної безпеки» дуже схоже. Так і є, але усе ж таки за своєю сутністю вони відрізняються. Намагаюсь пояснити це через наступний приклад.

Захищеність вашого сервера, веб-сайту, або домашнього комп’ютеру - це питання кібербезпеки, тому що це питання IT-систем, її обладнання та програмного забезпечення.

Захищеність ваших персональних даних, які можуть тягнути за собою розповсюдження комерційної тайни, або ж будь-якого іншого розповсюдження (аркуш з вашим логіном і паролем на робочому місці) - це питання інформаційної безпеки.

Різниця між цими двома термінами є також і в об’єктах діяльності. До об’єктів кібербезпеки відносяться::

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об’єкти критичної інфраструктури (при цьому формування переліку об'єктів критичної інфраструктури має бути затверджений Кабінетом Міністрів).

До об’єктів інформаційної безпеки відносяться:

- свідомість громадянина;
- психіка людей;
- інформаційні системи;
- особистість;
- колектив;
- суспільство;
- держава;
- світове товариство.

Таким чином, кібербезпека більш відповідає за інформаційний технологічний простір, а інформаційна безпека - за інформаційні соціальні питання.

Основними суб'єктами кібербезпеки і інформаційної безпеки є:

- Державна служба спеціального зв'язку та захисту інформації України;
- Національна поліція України;
- Служба безпеки України;
- Міністерство оборони України та Генеральний штаб Збройних Сил України;
- Розвідувальні органи;
- Національний банк України.

Сучасний бізнес тісно і безпосередньо пов'язаний з обробкою, передачею і зберіганням інформації. Малі комерційні підприємства існують в конкурентному середовищі, є безліч загроз, спрямованих на інформаційні

активи. Також, підприємство існує в загальному кіберпросторі, яке характеризується величезною кількістю загроз, пов’язаних з інформаційною безпекою.

Протидія цим загрозам – створення системного комплексу управління інформаційною безпекою з метою створення системи моделі управління кіберпростором. Однією з важливих складових цієї системи є система управління інцидентами кібербезпеки.

Інцидент кібербезпеки – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Технічний рівень кіберзлочинності у сучасності знаходиться на дійсно високому рівні, і не тільки України а й весь світ кожного дня терпить загрози кібербезпеки. Згідно З НД ТЗІ 1.1-003-99 [9], загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків інформаційно-телекомунікаційній системі.

1.2 Аналіз проблем інформаційної безпеки та кібербезпеки для малих комерційних підприємств

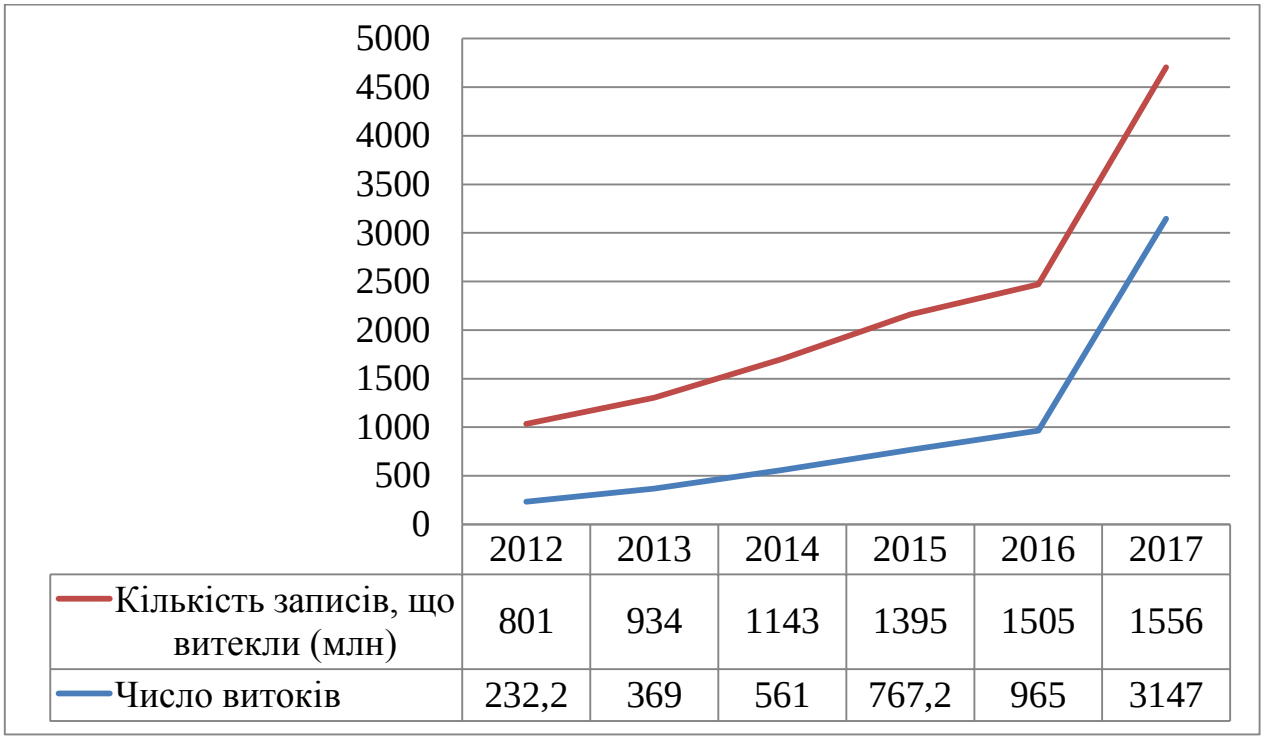
У сьогоденні питання забезпечення кібербезпеки не витрачає своєї актуальності. Сучасність не надає нам вибору, у наш час кожна людина в тій чи іншій мірі стикається з інформаційними технологіями. Зараз вони стрімко і повноцінно увійшли в наше життя. Будь які співробітники підприємств, якого б вони соціального рівня, кваліфікації не були, яку б посаду не займали, користуються Інтернетом, соціальними мережам, електронною поштою,

банкоматами, мобільними телефонами та іншими системами інформаційних технологій, що оброблюють інформацію.

Які б великі гроші не втрачалися на які б технічні засоби захисту не застосовувалися, завжди залишається одна потенційна загроза будь-якого підприємства: люди. Більшість випадків витоків інформації та виникнення інцидентів пов'язані з людським фактором.

Інша проблема пов'язана з професіоналами в області кібербезпеки. Існує їх дефіцит на ринку (46% організацій стверджують, що відчувають нестачу кваліфікованих фахівців з кібербезпеки), і часом вони перевантажені роботою, щоб виконувати свою роботу на належному рівні.

Далі, надані приклади, прибігаючи до статистичних даних декількох ресурсів. На період 2017 року за даними аналітичних центрів Cisco Cybersecurity Report [10] і InfoWatch [11] було зареєстровано 1556 випадків витоку конфіденційної інформації . В результаті витоків було скомпрометовано більш ніж 3,1 млрд. записів персональних даних.



	2012	2013	2014	2015	2016	2017
Кількість записів, що витекли (млн)	801	934	1143	1395	1505	1556
Число витоків	232,2	369	561	767,2	965	3147

Рисунок 1.1 – Число витоків інформації і обсяг персональних даних, скомпрометованих в результаті витоків 2012-2017 рр.

Кількісний ріст витоків в 2016 році сповільнилося. Якщо в 2016 році цей показник склав 7,9%, то в 2017 році число витоків виросло на 3,4%.

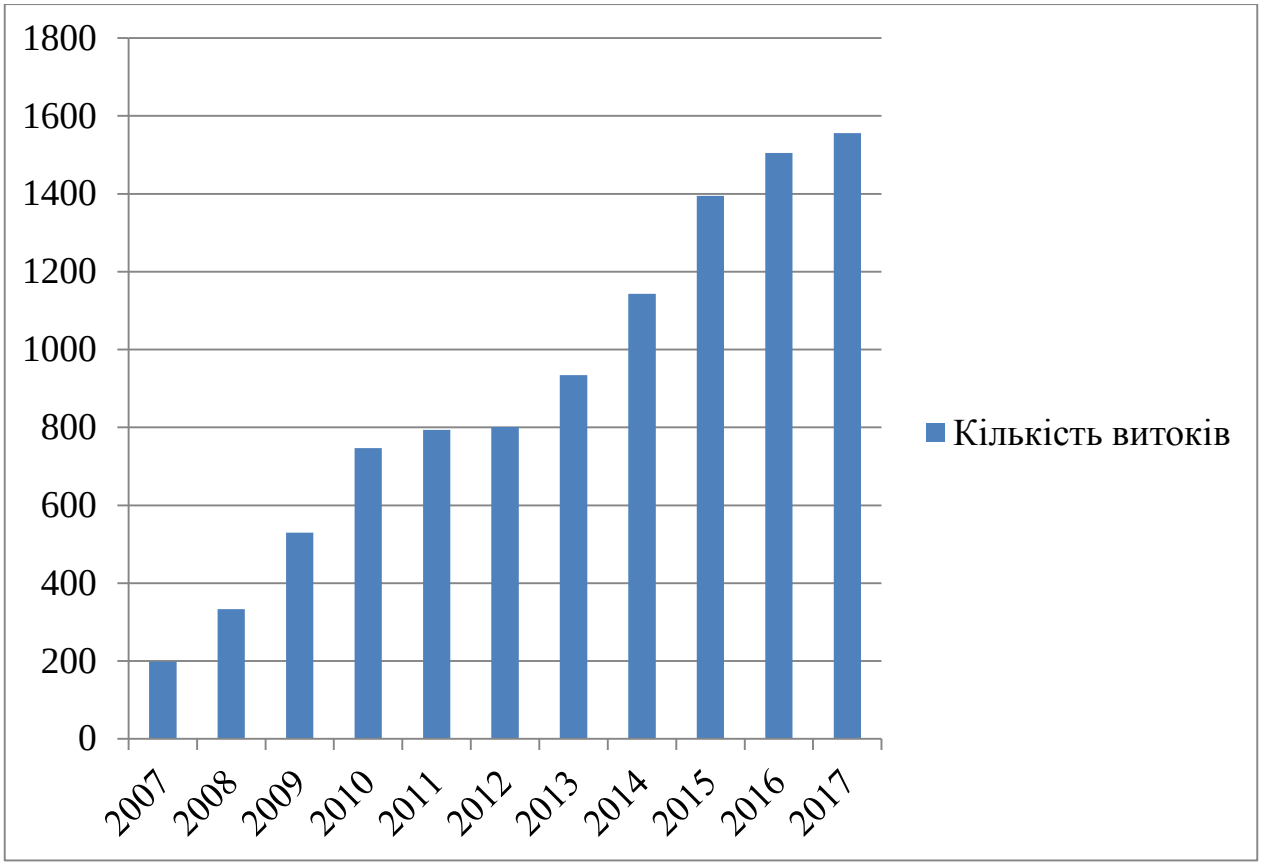


Рисунок 1.2 – Число зареєстрованих витоків інформації, 2007-2017 рр.

У 2017 році вперше за весь час спостережень було зафіксовано триразове збільшення обсягу даних, скомпрометованих в результаті витоків, і настільки ж суттєве зростання числа скомпрометованих записів персональних даних в розрахунку на один виток. Причому збільшення обсягів скомпрометованих даних не пов'язано тільки з однією або декількома великими витоками - в іншому випадку можна було б говорити про випадковий сплеск. На ділі ж було зафіксовано 79 витоків, в результаті кожної з яких скомпрометовано більш 1 млн. записів.

Таким чином, в 2017 році картина витоків зазнала суттєвих змін. Ми входимо в епоху масової компрометації даних. Основний фактор, що визначає сучасну картину – кількісний і якісний ріст витоків.

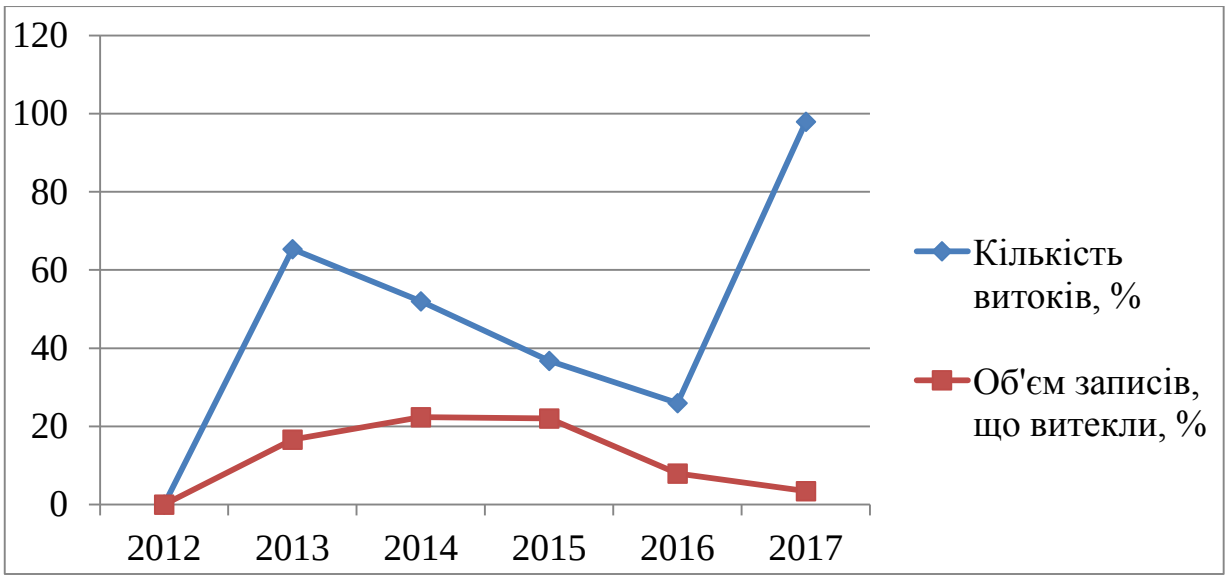


Рисунок 1.3 – Динаміка росту числа витоків і об’єму записів персональних даних

В 2017 році було зареєстровано 540 (38,2%) витоків інформації, наслідком котрих став зовнішній зловмисник. В 873 (61,8%) випадках виток інформації виник в наслідок внутрішнього порушника.

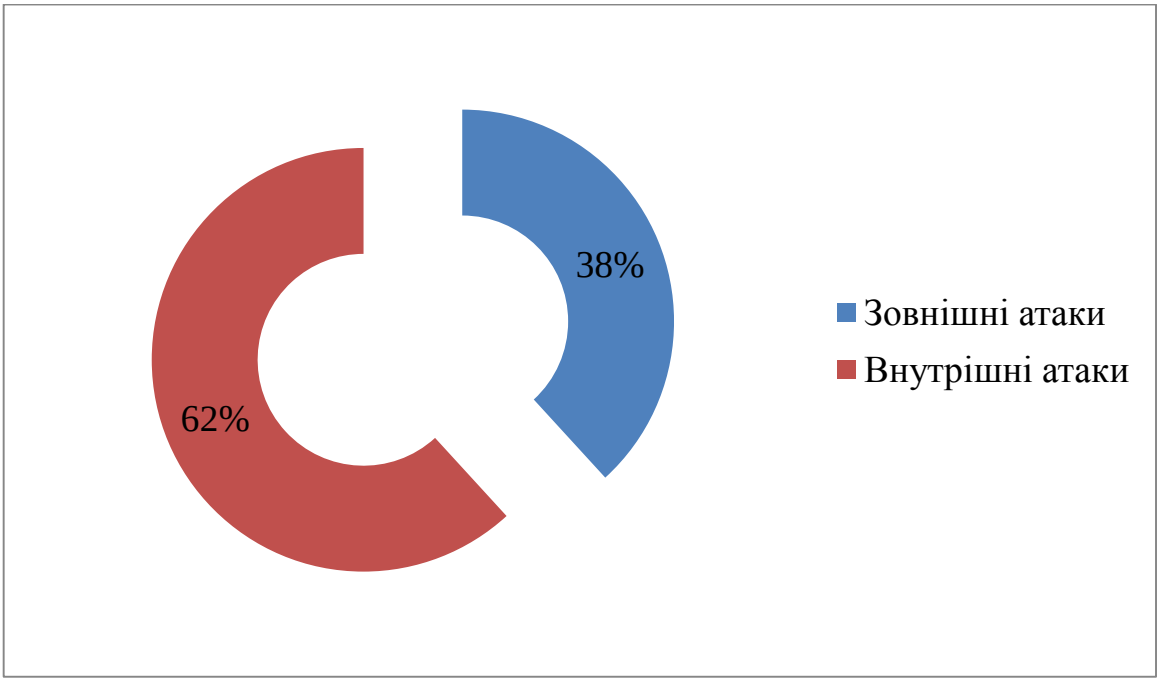


Рисунок 1.4 – Розподіл витоків по вектору впливу

Частка витоків під впливом зовнішніх атак виявилася більш за аналогічний показник 2016 року (тоді на частку витоків під впливом зовнішніх

атак припало 32% витоків). В результаті, в 2017 році з вини зовнішнього зловмисника було скомпрометовано 2,53 млрд. записів персональних даних - це становить 80% від сукупного обсягу скомпрометованих за рік запису. Виток даних під впливом зовнішніх атак відрізняються великим об'ємом компрометованих даних. В середньому, на один «зовнішній» виток доводиться 4,69 млн. скомпрометованих записів персональних даних. Для порівняння - в результаті витікання даних з вини або необережності внутрішнього порушника було скомпрометовано в середньому 0,56 млн. записів ПДН. Атаки «ззовні» мають ще одну характерну рису - зловмисники «виносять» з атакується периметра все, до чого можуть дотягнутися.

Якщо ефект «зовнішнього» витоку можна порівняти з килимовою бомбардуванням, то «внутрішній» виток ближче до точкового бомбометання - під загрозою опиняється критично важлива інформація, а розмір потенційного фінансового збитку практично не обмежений і може досягати вартості всього бізнесу постраждалої компанії.

У зв'язку з особливостями природи внутрішніх витоків необхідно звернути увагу на проблему «привілейованих» користувачів - топ-менеджменту, системних

адміністраторів, інших співробітників, чиї права доступу до інформації практично не обмежені, включаючи самих фахівців з інформаційної безпеки. Контролювати дії таких співробітників надзвичайно складно, а наслідки, до яких призводять помилки або зловмисна діяльність «високопоставлених» порушників, за масштабом можна порівняти зі стихійним лихом.

У 2016 році в 36% випадків винуватцями витоків інформації були справжні (33,9%) або колишні (2,1%) співробітники організацій. Більш ніж в 2% випадків була зафіксована вина керівників (топ-менеджмент, глави департаментів і відділів) і системних адміністраторів. Частка витоків, що трапилися на стороні підрядників, чий персонал мав легітимний доступ до охоронюваної інформації, склала 6%.

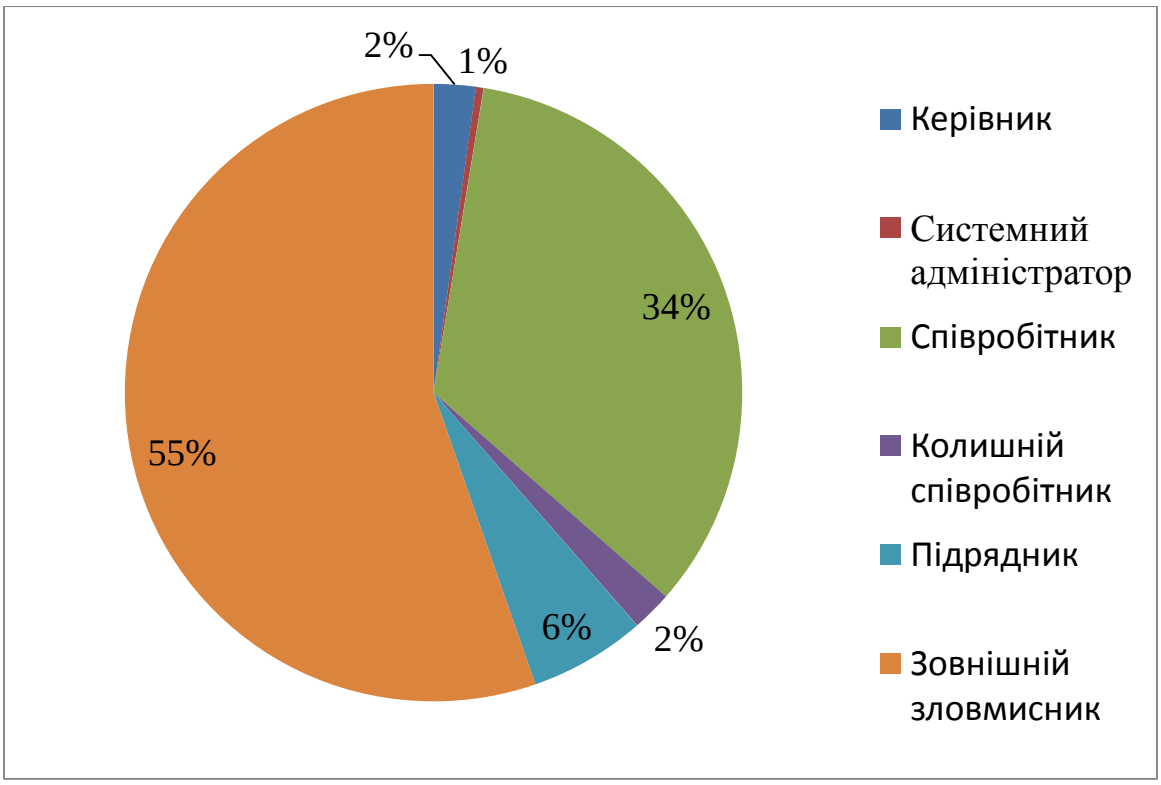


Рисунок 1.5 – Розподіл витоків по джерелу (винуватцю)

Частка витоків персональних і платежів в розподілі витоків за типом інформації залишилася на рівні попередніх років, склавши 93%.

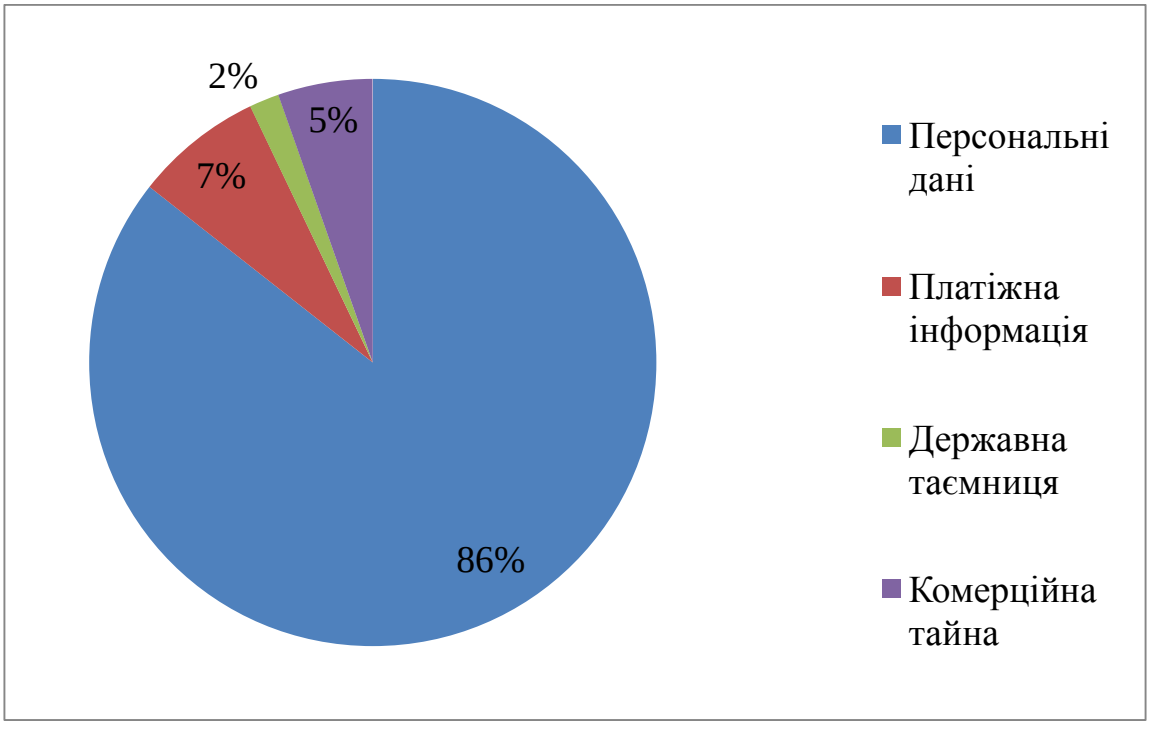


Рисунок 1.6 – Розподіл витоків за типами даних

У 2017 році частка витоків даних, пов'язаних з подальшим використанням скомпрометованої інформації з метою шахрайства знизилася до 7%.

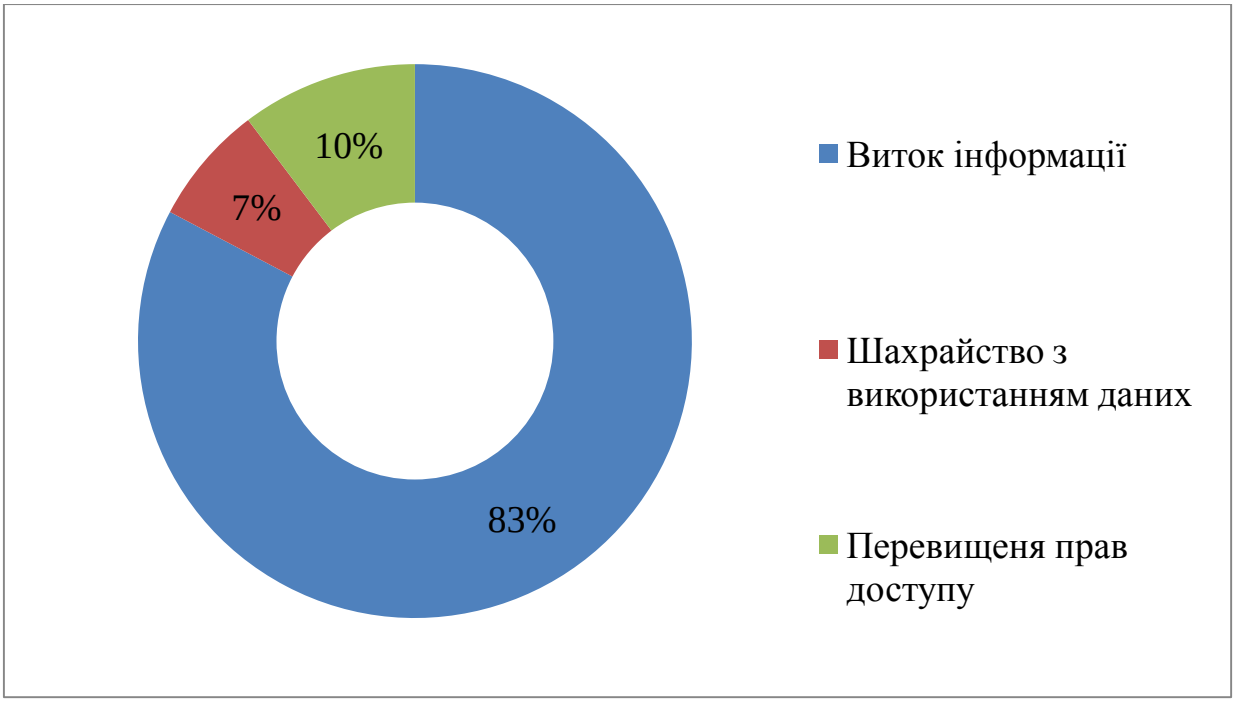


Рисунок 1.7 – Розподіл інцидентів по характеру

Триразове збільшення обсягу скомпрометованих даних свідчить про зростаючу з кожним днем цінності інформації в цифровому вигляді. Причому якщо кількісне зростання витоків прогнозувати складно - не виключено, що він просто зупиниться, то сценарій, при якому обсяг скомпрометованих даних зростає рік від року, слід вважати найбільш імовірним.

10% інцидентів класифіковані як порушення, пов'язані з отриманням несанкціонованого доступу до інформації.

У 2017 році скоротилася частка витоків в результаті втрати обладнання, а також за такими каналам, як «електронна пошта» і «паперові документи». Частки витоків через знімні носії, мобільні пристрої залишилися на рівні 2016 року. Частка «мережевого» каналу значно виросла.

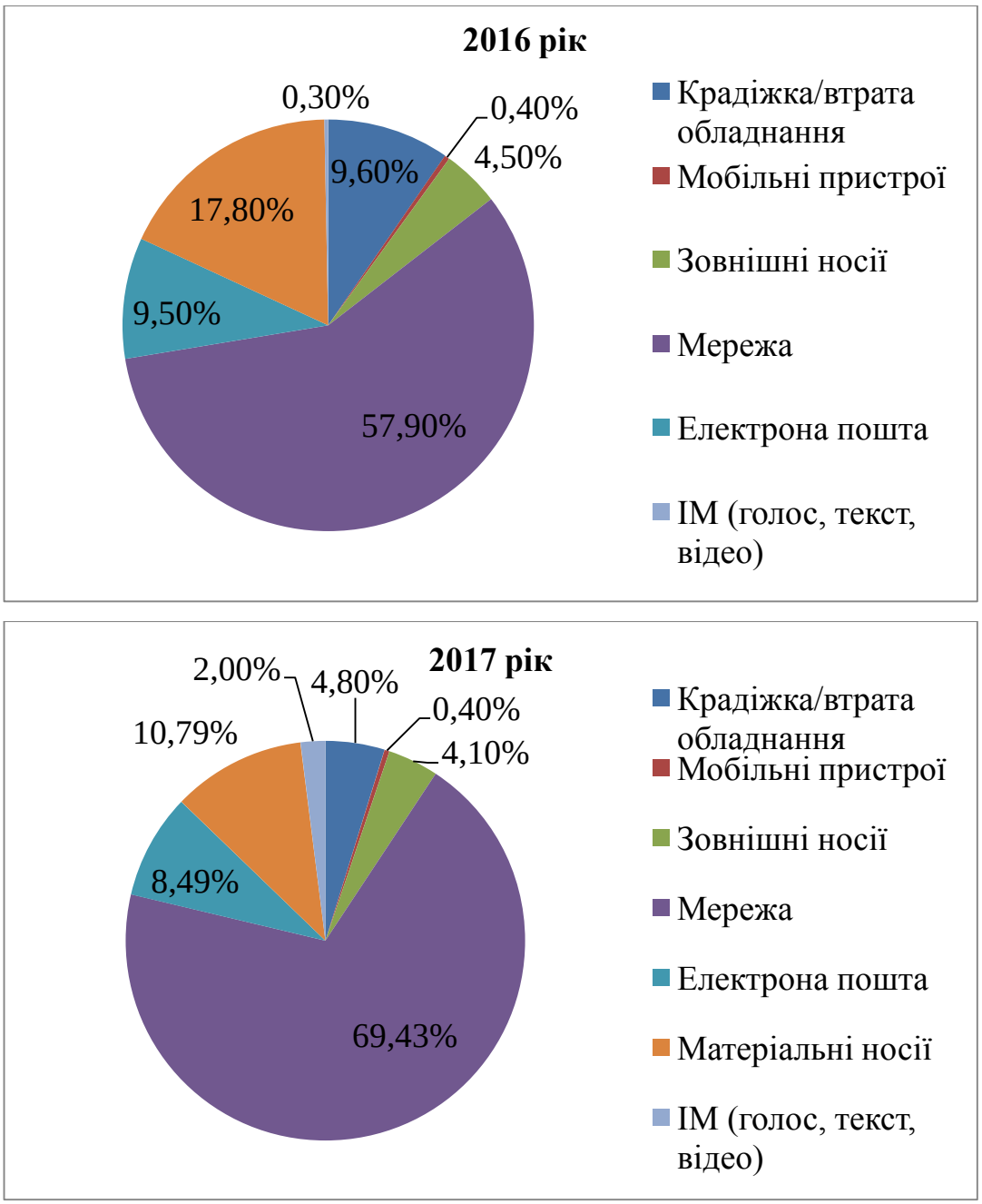


Рисунок 1.8 – Розподіл витоків по каналам у порівнянні 2016 і 2017 рр.

У розподілі витоків даних в результаті випадкових дій співробітників найбільш помітні витоку через електронну пошту - 23,7%, паперові носії - 16,2%, знімні носії - 6,7% і в результаті крадіжки або втрати обладнання - 5,3%. На мережевий канал доводиться 47,1% всіх зафіксованих випадкових витоків. Розподіл умисних витоків інформації характеризується переважанням мережевого каналу. Більше 90% випадків навмисної компрометації даних пов'язані з неправомірної передачею або розголошенням інформації з

використанням мережі Інтернет (в тому числі веб-сервісів, електронної пошти та інших інтернет-ресурсів).

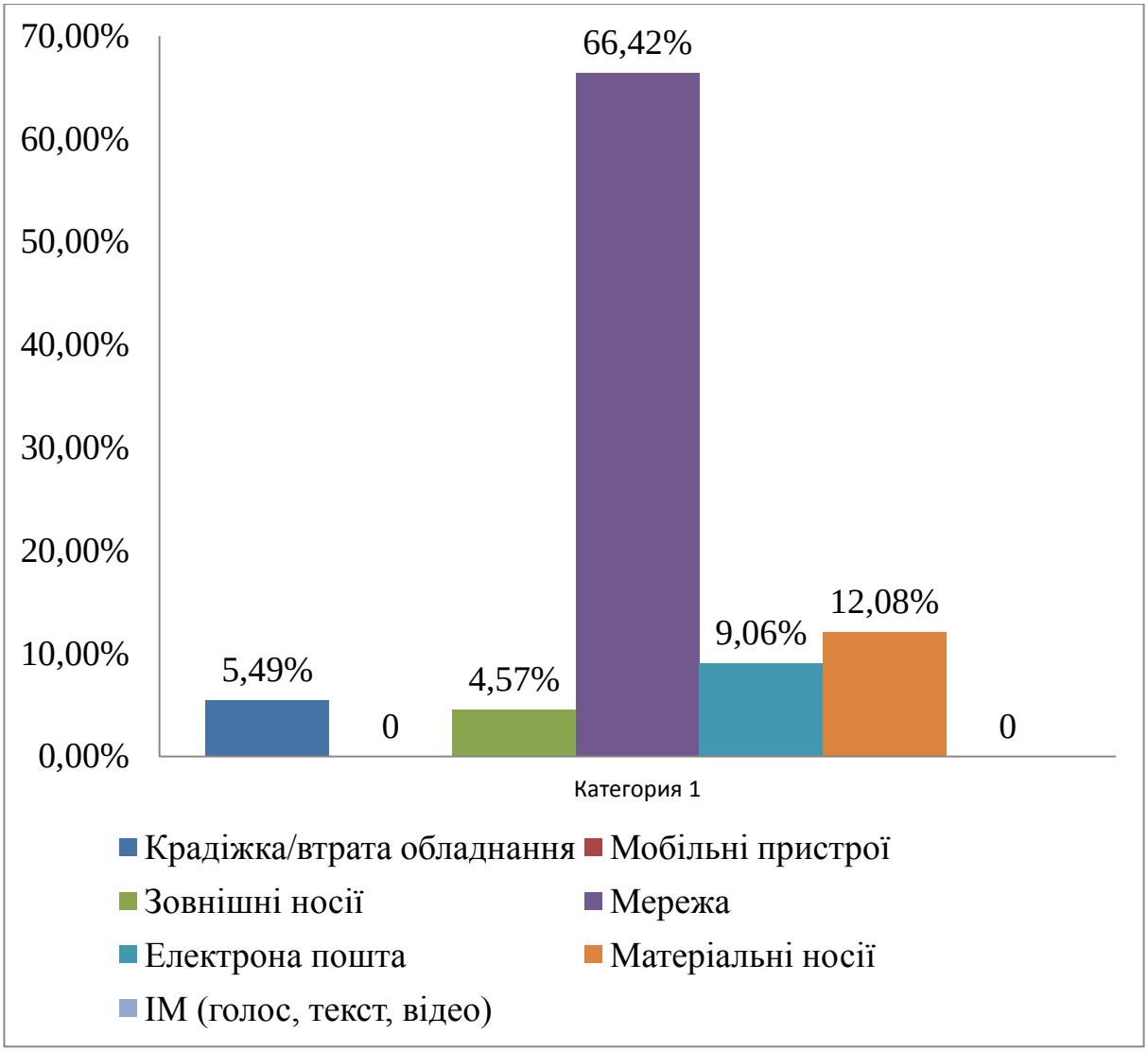


Рисунок 1.9 – Витоки персональних даних, розподіл по каналам

Мережевий канал виходить на перший план як за загальним обсягом скомпрометованих персональних даних, так і за кількістю витоків. Велика частина (> 66%) витоків персональних даних доводиться на мережу. У випадку з внутрішніми порушниками компанії мали справу з різноманітними сценаріями - збереженням конфіденційної інформації в хмарових сховищах, використанням безкоштовних поштових акаунтів (наприклад, веб-пошта).

Сценарії зовнішніх зломів менш варіативні. Хакери, як правило, не дуже добре знайомі зі структурою даних організації, наприклад, з тим, де зберігається найцінніша інформація і що вона собою являє, тому «беруть» все,

що представляє цінність. Мережевий канал слід визнати найбільш «популярним» стосовно і до випадкових, і до навмисних витоків. «Мережеві» витоки характеризує високий рівень критичності даних, величезні обсяги скомпрометованої інформації.

Невелика частка умисних витоків через мобільні пристрої, знімні носії, електронну пошту та паперові документи пояснюється тим, що зловмисники все менше використовують ці канали для здійснення протиправних дій. «Високий рівень» порушник обізнаний, що сучасні засоби контролю дозволяють успішно перехоплювати передачу конфіденційної інформації по цих каналах, і не ризикує даремно.

Домінування мережевого каналу в розподілі випадкових і навмисних витоків свідчить, по-перше, про зростаюче значення цього каналу для бізнесу. Число комунікаційних сервісів, «зав'язаних» на мережу, величезна. Кількість помилок співробітників, що працюють з цими сервісами, рік від року тільки збільшується. Як наслідок, зростає частка випадкових витоків при передачі інформації по мережі і публікації даних в Інтернеті. З іншого боку, зловмисники все рідше використовують завідомо контрольовані канали передачі інформації - електронну пошту, сервіси миттєвих повідомлень. У цьому сенсі мережа все ще залишається каналом передачі даних, де можливості систем контролю і захисту в цілому перевершують можливості зловмисників.

Галузева карта розподілу витоків за типом організації 2017 року у порівнянні з даними 2016 року не зазнало критичних змін.

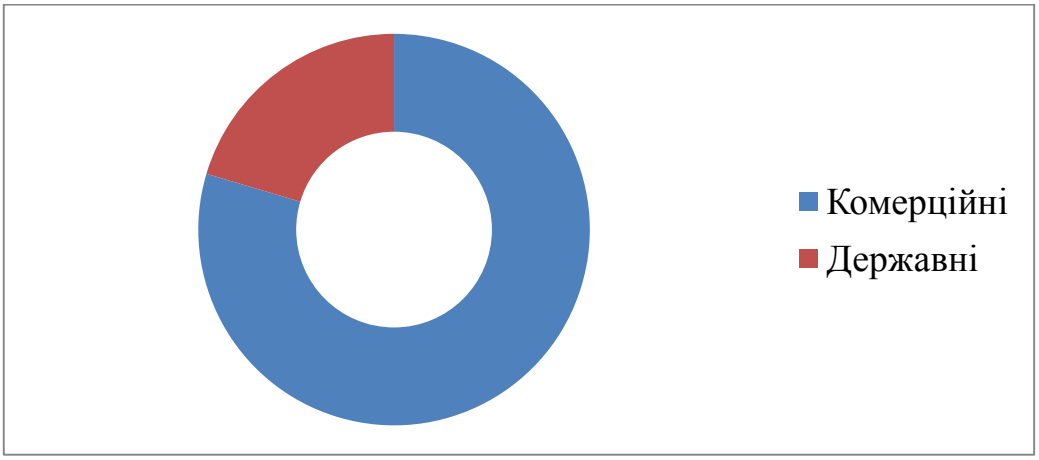


Рисунок 1.10 – Розподіл витоків по типу організації

Найчастіше фіксувалися витоку даних з медичних організацій (25,8%), рідше – у сфері промисловості і транспорту (3,9%). За об'ємом скомпрометованих записів пальма першості належить компаніям високотехнологічного сектора, перш за все великим інтернет-сервісам і торговим онлайн-майданчикам. На частку таких організацій припадає майже три чверті (73,6%) від усього обсягу скомпрометованих в 2017 році даних. помітна частка торгових компаній, готелів і ресторанів - 11,9%. На державні органи та муніципальні установи припадає 9,9% від усього обсягу скомпрометованих даних.

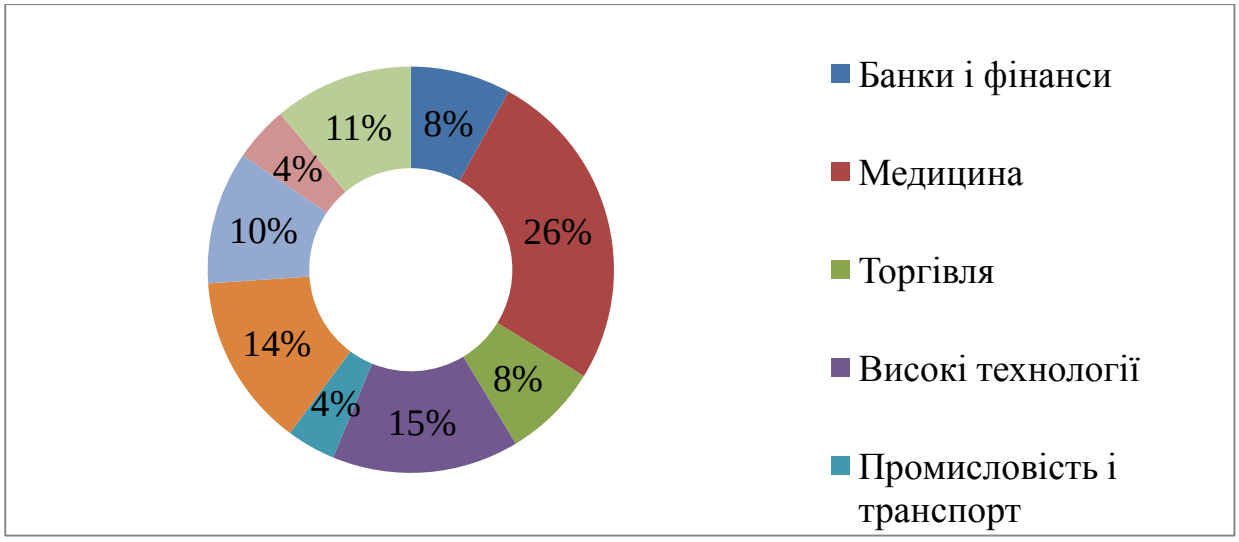


Рисунок 1.11 – Розподіл числа витоків даних по галузям

Наведені діаграми дають фактичну картину, загальне уявлення про витоках інформації та обсягах скомпрометованих даних в різних галузях. Важливіше з'ясувати, які сегменти зараз є найбільш «привабливими» для зловмисників. «Привабливість» галузі прямо обумовлена «ліквідністю» даних, які обробляють компанії цього сектора. Подання зловмисників про рівень захисту даних в галузі впливає на «привабливість» обернено пропорційно.

Показником «привабливості» можна вважати число умисних витоків в конкретної галузі. Галузеве розподілення умисних витоків одного типу дасть нам відповідь на питання, які сегменти найбільш «привабливі» для зловмисника (і найбільш уразливі). У 2017 році, як і роком раніше, найбільш

«привабливими» опинилися торгові, транспортні компанії, до яких додалися фінансові установи.

У цих галузях більше половини витоків, що супроводжувалися компрометацією персональних даних, мали умисний характер.

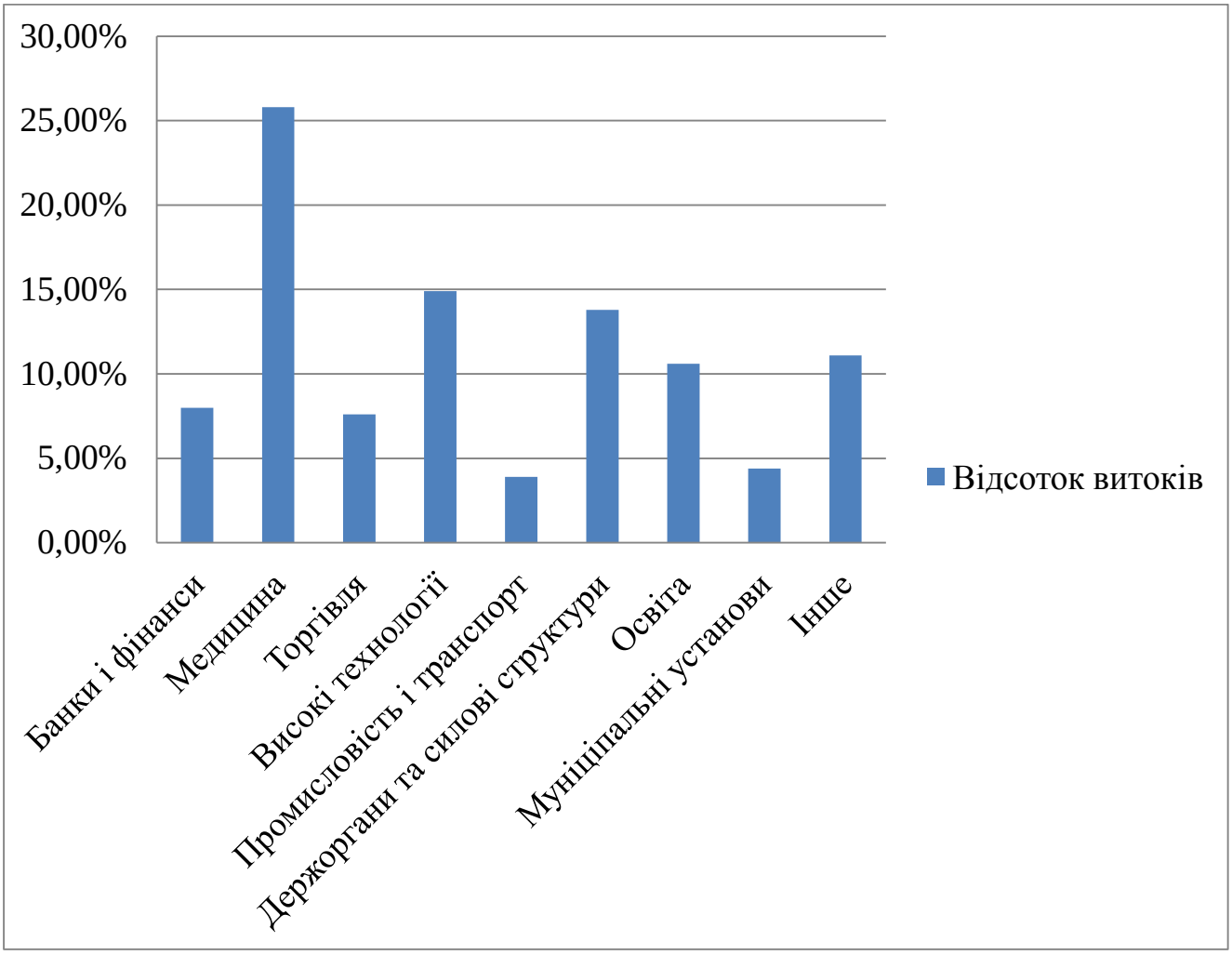


Рисунок 1.12 – Частка умисних витоків персональних даних від загальної кількості витоків персональних даних по галузям

Якщо перебудувати вже наведений розподіл в залежності від вектора атаки, можна отримати наочне уявлення про «привабливість» конкретної галузі для зовнішнього і внутрішнього зловмисника.

Рисунок 1.13 – Частка умисних витоків персональних даних під впливом внутрішнього і зовнішнього зловмисника від загального числа витоків персональних даних по галузям

Як видно з діаграми, високотехнологічні компанії, поряд з транспортним і банківським секторами, найчастіше ставали жертвами зовнішніх атак, спрямованих на розкрадання даних. Частка ПДН, вкрадених внутрішніми зловмисниками, в цих галузях незначна. З іншого боку, від зловмисних дій внутрішнього порушника найчастіше страждали медичні заклади і банки. Одна

з основних причин - надзвичайно висока ліквідність даних, з якими працює персонал медичних і фінансових установ.

Найбільший обсяг скомпрометованих персональних даних доводиться на високотехнологічні компанії (інтернет-сервіси, провайдери цифрових послуг, оператори стільникового зв'язку). Ці компанії можна назвати піонерами у використанні цифрових технологій обробки і зберігання даних. Лідерство за показником обсягу скомпрометованих даних - лише наслідок, плата за використання передових підходів до роботи з інформацією. У 2017 році розподіл витоків між середніми (до 500 ПК) і великими (більше 500 ПК) підприємствами вийшло приблизно однаковим як за кількістю витоків, так і за обсягом скомпрометованих даних.

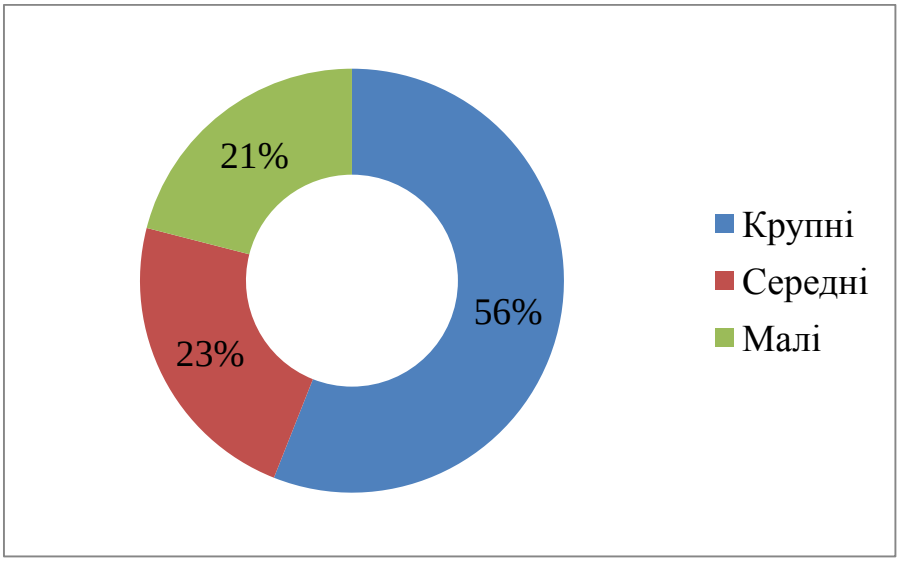


Рисунок 1.14 – Розподіл витоків по розміру підприємства

Великі компанії допускають трохи більше витоків в кількісному вираженні, при цьому обсяг втрачених даних в розрахунку на одну витік у них трохи нижче, ніж у компаній середнього розміру. Ймовірно, в зв'язку з цим слід зазначити недостатність фінансування, що виділяється на захист інформації від витоків в сегменті малого і середнього бізнесу.

Найближчим часом навряд чи слід очікувати якихось серйозних змін в галузевій картині витоків. Обидва ці чинники, так чи інакше впливають на динаміку витоків в розрізі конкретних галузей - це ліквідність і захищеність

даних, - відрізняє завидна стійкість. Уявлення про те, що банки, страхові компанії обробляють найбільш ліквідну інформацію, склалося дуже давно. Думка про надійності або слабкості систем захисту в тій чи іншій галузі теж не схильне особливим коливань. У підсумку ми маємо стабільну картину «привабливості» і, як результат, розуміння того, яка галузь нині найбільш вразлива.

Накладаючи дане розуміння на реальну динамічну картину витоків, можна з упевненістю прогнозувати зростання числа і потужності зовнішніх атак щодо високотехнологічних компаній, медичних установ і компаній, пов'язаних з медстрахуванням, а також фінансових організацій.

Наведені статистичні дані чітко показують, що існують проблеми майже на всіх рівнях забезпечення інформаційної безпеки. З цього можна зробити наступний висновок: країнам є над чим працювати, тобто вдосконалювати законодавчу базу, збільшувати контроль за мережевим трафіком, підвищувати інформаційну культуру серед громадян; підприємствам варто приділяти більше уваги до навчання і ознайомлення персоналу з інформаційною безпекою, щоб зменшити витоки інформації через необережність; користувачам потрібно приділити більше уваги за тим, з яких ресурсів вони завантажують інформацію, змінювати паролі, намагатися не завантажувати свої персональні дані з неперевіреного персонального комп’ютера (ПК).

Також слід звернути увагу на інформацію, що містить персональні дані, бо більшість зловмисників зацікавлення у збагачені, а крадіжка персональних даних – найлегший спосіб заробити і постачальниками такої інформації здебільшого є самі людей із-за своєї не обережності. Підводячи підсумки, зі статистичних даних ми бачимо, що кіберзлочинці націлені на персональні данні, використовують частіше усього примітивні засоби крадіжки інформації, а саме змінні носії, зловмисниками є сам персонал компанії у більшості випадків.

Зловмисники, в тому числі недобросовісні співробітники, підвищують ризики кібербезпеки компаній за рахунок існуючих і виникаючих загроз.

Кібербезпека – це процес, а не одноразове рішення, і проблема зловмисників, включаючи недобросовісних, а також неуважних і неінформованих співробітників, з часом вирішена не буде. Кожна нова або вдосконалена міра безпеки надійна до тих пір, поки не буде придуманий спосіб, як її обійти. Найкраще, що можуть зробити заходи по забезпеченню кібербезпеки - призупинити зловмисників і усунути виявлені проблеми. Однак, ситуація не безнадійна. Поки вирішуються існуючі проблеми, зловмисники розширюють свій арсенал новими загрозами.

Одним з останніх прикладів масової кібератаки, яка завдала величезної шкоди глобальних масштабів є вірус «Petya», який став самою крупною кібератакою в історії України. 27 червня 2017 року спочатку атакував Україну а потім й США, Російську Федерацію, Польшу, Францію, Італію, Індію, Германію, Великобританію, Іспанію, Естонію, Румунію. З цього списку, на Україну стало 75,2% заражень.

В результаті цієї вірусної атаки, в Україні була тимчасово заблокована діяльність наступних структур і сайтів.

Державні структури: Кабінет міністрів України, Міністерство внутрішніх справ, Міністерство культури, Міністерство фінансів, Національна поліція, Кіберполіція, Львівська міська рада, Міністерство енергії, Національний банк України.

Банки: Ощадбанк, Сбербанк, ТАСКомерцбанк, Укргазбанк, Банк Південний, ОТР банк, Кредобанк.

Транспорт: Аеропорт «Бориспіль», Київський метрополітен, Укрзалізниця

ЗМІ: Радіо «ЕРА-FM», Football.ua, СТБ, Інтер, Перший національний, Телеканал 24, Радіо «ЛЮКС», Радіо «Максимум», «КП в Україні», Телеканал АТР, «Кореспондент.нет».

Крупні підприємства: Нова Пошта, Київенерго, Нафтогаз України, Дніпренерго, Київводоканал, Новус, Епіцентр, Укртелеком, Укрпошта.

Мобільні оператори: Lifecell, Київстар, Vodafone.

Медицина: Фармак, клініка «Борис», корпорація «Артеріум».

Компанія Cyence [12], що займається оцінкою ризиків, підрахувала, що економічні втрати від атаки вірусу «Petya» можуть скласти близько $ 8 млрд. У цю суму компанія включила ще й шкоду, заподіяну травневої атакою схожого вірусу WannaCry, який вивів з ладу понад 200 тисяч комп'ютерів в 150 країнах світу.

Ще до масової атаки програми-вимагача WannaCry в середині травня у всьому світі стали все більше і серйозніше говорити про кібербезпеку. WannaCry тільки підкреслює, скільки роботи глобальної спільноти ще належить зробити, щоб знизити загрозу і наслідки майбутніх злочинних атак кіберзлочинців.

Оцінюючи втрати, які бізнес поніс через вірус можна говорити про недоотриманий компаніями прибутку. Деякі ритейлери були змушені зупинити роботу своїх магазинів, частина банківських відділень під час атаки працювала в "консультативному режимі" - це ті сфери, за якими вірус вдарив найбільш відчутно.

Оцінити скільки компаній постраждало і в якому обсязі дуже складно, оскільки деякі підприємства фактично припиняли свою роботу на день, а деякі, наприклад, тільки на кілька годин. Це один з наочних і актуальних прикладів глобальної кібератаки, яка принесла величезні втрати державі.

Можна зробити три ключових висновки на прикладі вірусних атак «Petya» і «WannaCry»:

- Уряди повинні своєчасно повідомляти про недоліки програмного забезпечення постачальникам і в тій мірі, в якій вони використовують ці недоліки, законодавчо закріплювати ці рішення для незалежного нагляду і обговорення. Тільки створюючи більшу прозорість відносно вразливостей, доступних для експлойтів, ми можемо сподіватися на мінімізацію їх виникнення і глобального впливу. Урядам слід також розробити і впровадити добре структурований і безперервний процес, який дозволить приймати засновані на ризики рішення щодо того, як звертатися і коли випускати інформацію про уразливість для розробників технологій та громадськості.

- Розробники технологій повинні мати відкриті механізми, засновані на оцінці ризиків, для отримання, обробки і розкриття інформації про наявність чи відсутність відомих вразливостей, виправлень, засобів їх усунення і обхідних рішень. Крім забезпечення безпеки протягом всього природного життєвого циклу продуктів, розробники технологій повинні повідомляти громадськості про те, коли, як, навіщо і чому необхідно контролювати уразливості. Крім того, вони повинні прагнути забезпечити більшу прозорість процесів спільної роботи. А також стежити за тим, що користувачі точно знають, кому потрібно повідомляти про уразливість, щоб про них стало відомо і вони були усунені.

- Лідери бізнесу повинні зробити забезпечення кібербезпеки першочерговим завданням. Керівники IT-служб в організаціях повинні використовувати всі можливості для інформування своїх керівників і ради директорів щодо ризиків, які представляють для бізнесу, його співробітників і клієнтів, а також для репутації бренду. Прийшов час, коли до цієї інформації треба прислухатися і почати діяти: лідери бізнесу повинні задати модель ставлення до кібербезпеки на вищому рівні і донести її важливість до всієї організації. Вони також повинні забезпечити актуальність і регулярне оновлення IT-інфраструктури, а також щоб цим заходам відводився відповідний бюджет. Повинна бути легітимна дискусія про те, як і коли уряд поширюють інформацію про уразливість в світовому масштабі. Але, як ми бачили на прикладі "Petya" і "WannaCry", уряд, який накопичує відомості про уразливість, створюють потенційну можливість витоку. Це, в свою чергу, створює величезні можливості як для національних гравців, так і кіберзлочинців.

Ми вже бачимо, як швидко працюють зловмисники. За даними аналітичного центру компанії Avast [13], яка є одним з лідерів ринку програмного антивірусного забезпечення, у 93% випадках для злому систем зловмисникам потрібно кілька хвилин або менше. У 28% на крадіжку інформації потрібно кілька хвилин, тоді як організаціям були потрібні тижні, щоб тільки виявити факт витоку. Для виявлення близько 70% витоків, пов'язаних зі зловживаннями співробітників, були потрібні місяці або роки.

Проте, вірусна атака – це одна з багатьох видів загроз, які можуть нанести шкоди інформаційній системі. За статистичними даними Global Security Intelligence Report [14] компанії Microsoft, майже всі витоки, загрози і різні інциденти відбуваються за чотирма стандартними сценаріями, які наведені в таблиці 1.1.

Таблиця 1.1 – Види найпопулярніших витоків та загроз і їх загальне відсоткове співвідношення

Види загроз та інцидентів	**Загальне відсоткове співвідношення**
Зловмисне ПЗ/Код (віруси, трояни, експлойти)	48,4%
Збір інформації (Робітники підприємств, конкуруючі фірми)	23,1%
Відмова в обслуговуванні (DoS)	16,6%
Несанкціонований/неавторизований доступ	11,9%

Зловмисне програмне забезпечення

Зловмисний код є програмою, приховано введену в іншу програму з наміром знищити дані, виконати руйнівні або «нав'язливі» програми або будь-яким іншим чином скомпрометувати безпеку або цілісність даних «жертви». В основному шкідливий код призначається для виконання даних непорядних функцій, при цьому немає необхідності знати користувача системи. Атаки, пов'язані з використанням шкідливого коду, можуть бути розділені на п'ять категорій: віруси, «троянські коні», «черв'яки» і мобільний код. Вірус має здатність до самокопіювання, створення власних копій і розповсюдження копій в інші файли, програми або комп'ютери. Віруси проникають у програми вузла і поширюються під час виконання інфікованої програми, зазвичай за участю користувача (наприклад, відкриття файлу, виконання програми. Клацання миші на файловому додатку).

«Троянські коні», названі так на згадку про дерев'яного коня з грецької міфології, є програмами, які справляють враження корисних, але в дійсності мають приховану шкідливу мету. Деякі «троянські коні» повністю змінюють існуючий файл в системі шкідливої версією, в той час як інші «троянські коні» представляються однією сутністю (наприклад, грою, доступною для завантаження), але реально є іншою (наприклад, грою і аналізатором пароля). «Троянські коні» найчастіше важкі для виявлення, оскільки здається, що вони виконують корисну функцію. «Троянських коней» можна віднести до однієї з трьох моделей:

- продовження виконання функції початкової програми і додаткове виконання самостійної шкідливої діяльності;
- продовження виконання функції початкової програми, але зміну цієї функції, щоб виконувати шкідливу діяльність (наприклад, версія «троянського коня» програми реєстрації входу, яка збирає паролі) або маскувати іншу шкідливу діяльність (наприклад, версія «троянського коня» програми відображення процесів, яка приховує певні процеси, які є шкідливими);
- виконання шкідливої функції, яка повністю заміняє функцію початкової програми.

Мета більшості «троянських коней» полягає в тому, щоб дати можливість віддаленому користувачеві отримати доступ і повний контроль над комп'ютером «жертви». Для виконання цього необхідно. щоб «троянські коні» складалися з компонента клієнта і компонента сервера. Клієнт завжди знаходиться на віддаленому комп'ютері порушника і намагається встановити з'єднання з сервером, який знаходиться на інфікованому вузлі. Коли встановлюється з'єднання між клієнтом і сервером, віддалений порушник може виконати команди на інфікованому комп'ютері і передати або модифікувати файли. Інша загальна мета «троянських коней» полягає в тому. щоб діяти як агенти DDoS.

Хробаки – це програми які копіюються самостійно, які є повністю

автономними, що означає, що їм не потрібно програма вузла, щоб інфікувати жертву. «Черви» поширюються самостійно; на відміну від вірусів, вони можуть створювати повністю функціональні копії і виконуватися самостійно без втручання користувача. Природа хробаків дозволяє їм швидко поширюватися. Особливістю «черв'яків» є те, що вони не несуть в собі ніякої шкідливої навантаження, крім самостійного розмноження, метою якого є засмічення пам'яті і, як наслідок, уповільнення роботи операційної системи.

Мобільний код є програмним забезпеченням, яке передається з віддаленої системи в локальну систему, а потім виконується на локальній системі без точних інструкцій користувачів. Мобільний код часто діє як механізм передачі вірусу - «хробака» або «троянського коня» - до робочої станції користувача.

Збір інформації

Інциденти збору інформації мають на увазі дії, пов'язані з визначенням потенційних цілей і отриманням уявлення про сервіси, що стосуються цих цілей. Інциденти збору інформації передбачають проведення «розвідки» з метою:

- визначення наявності мети, отримання уявлення про навколишню її мережевої топології і про те. з ким зазвичай ця мета пов'язана обміном інформації:
- визначення потенційних вразливостей мети або безпосередньо навколишнього її мережевий середовища, які можуть бути використані.

Прикладами атак збору інформації є:

- сканування DNS-сервера (системи доменних імен);
- відправка тестових запитів по випадковим мережевих адрес:
- зондування системи;
- сканування доступних мережевих портів в системі;
- сканування одного або декількох сервісів з відомими уразливими по діапазону мережевих адрес;
- пасивне прослуховування мережі.

У деяких випадках збір інформації розширюється і переходить в

неавторизований доступ, якщо, наприклад, порушник при пошуку уразливості системи намагається також отримати до неї доступі. Зазвичай це здійснюється автоматизованими інструментальними засобами злому, які не тільки виробляють пошук вразливостей. але і автоматично намагаються використовувати знайдені вразливі системи, сервіси та (або) мережі.

Відмова в обслуговуванні (DoS)

Інциденти відмови в обслуговуванні (DoS) призводять до нездатності систем, сервісів і мереж продовжувати функціонування з колишньою продуктивністю, найчастіше при повній відмові в доступі авторизованим користувачам, пов'язаному зі знищенням або виснаженням ресурсів. Цілями інциденту відмови в обслуговуванні можуть бути:

- зниження пропускної здатності мережі шляхом використання всієї доступної пропускної здатності мережі генерацією великих обсягів трафіку;
- виведення з ладу операційної системи передачею до сервера неправильно оформлених пакетів TCP IP;
- уповільнення роботи або блокування системи, сервісу, мережі за допомогою встановлення багатьох одночасних сеансів входу в систему, до сервісу, мережі;
- використання всього обсягу пам'яті систем шляхом створення численних, великих по об’єму файлів.

Несанкціонований доступ

Інцидент несанкціонованого доступу складається з неавторизованих спроб доступу в систему. Неавторизований доступ зазвичай реалізується через використання вразливостей операційної системи або додатків, використання імен користувачів і паролів або їх підбір. Цілями інциденту несанкціонованого доступу можуть бути:

- дистанційна компрометація поштового сервера;
- дискредитація Web-сервера;
- витяг файлів з паролями;
- перехоплення з'єднання або помилкове напрямок легітимних

мережевих з'єднань:

- перегляд конфіденційних даних, наприклад, записи платіжних відомостей та медичної інформації, без авторизації;
- запуск аналізаторів на робочої станції з метою захоплення імен користувачів і паролів;
- з'єднання з незахищеним модемом і отримання доступу до внутрішньої мережі;
- виконання ролі адміністратора, наприклад, переустановлення пароля e-mail і навчання новому паролю;
- використання не потребує постійного обслуговування зареєстрованої робочої станції без дозволу.

Те, безпосередньо чим буде проводитися атака, залежить від типу інформації, її розташування, способів доступу до неї і рівня захисту. Якщо атака буде розрахована на недосвідченість жертви, то можливе використання спам-розсилок. Оцінювати загрози інформаційної безпеки необхідно комплексно, при цьому методи оцінки будуть відрізнятися в кожному конкретному випадку. Наприклад, щоб виключити втрату даних через несправність обладнання, потрібно використовувати якісні комплектуючі, проводити регулярне технічне обслуговування, встановлювати стабілізатори напруги. Далі слід встановлювати і регулярно оновлювати програмне забезпечення. Окрему увагу потрібно приділити захисному ПО, бази якого повинні оновлюватися щодня

Навчання співробітників компанії основним поняттям інформаційної безпеки і принципам роботи різних шкідливих програм допоможе уникнути випадкових витоків даних, виключити випадкову установку потенційно небезпечних програм на комп'ютер. Також в якості запобіжного заходу від втрати інформації слід робити резервні копії. Для того щоб стежити за діяльністю співробітників на робочих місцях і мати можливість виявити зловмисника, слід використовувати DLP-системи.

1.3 Загальні вимоги для управління інцидентами кібербезпеки на підприємстві

Важливою складовою загальної стратегії забезпечення ІБ підприємства є структурований підхід до управління інцидентами інформаційної безпеки, в тому числі до управління інцидентами кібербезпеки.

Метою такого підходу є побудова системи управління інцидентами ІБ, в рамках якої реалізується система управління інцидентами кібербезпеки. Система управління інцидентами ІБ та кібербезпеки, незалежно від характеристик та виду діяльності підприємства, повинна забезпечувати наступне:

- події ІБ повинні бути виявлені і ефективно оброблені, зокрема визначені такими, що належать або не належать до інцидентів ІБ;
- ідентифіковані інциденти мають бути оцінені, і реагування на них повинно бути здійснено найбільш доцільним і результативним методом;
- негативний вплив інцидентів ІБ на підприємство і її бізнес-операції необхідно мінімізувати відповідними захисними заходами, які є частиною процесу реагування на інцидент;
- з інцидентів ІБ і управління ними необхідно вилучити уроки. Це збільшує шанси запобігання інцидентів ІБ в майбутньому, покращення застосування захисних заходів, покращення системи управління інцидентами ІБ.

Для досягнення вказаних цілей система управління інцидентами ІБ повинна містити чотири процеси (етапи обробки інцидентів):

1) планування і підготовка;
2) застосування;
3) аналіз;
4) покращення.

Зміст цих процесів показаний на наступній схемі:

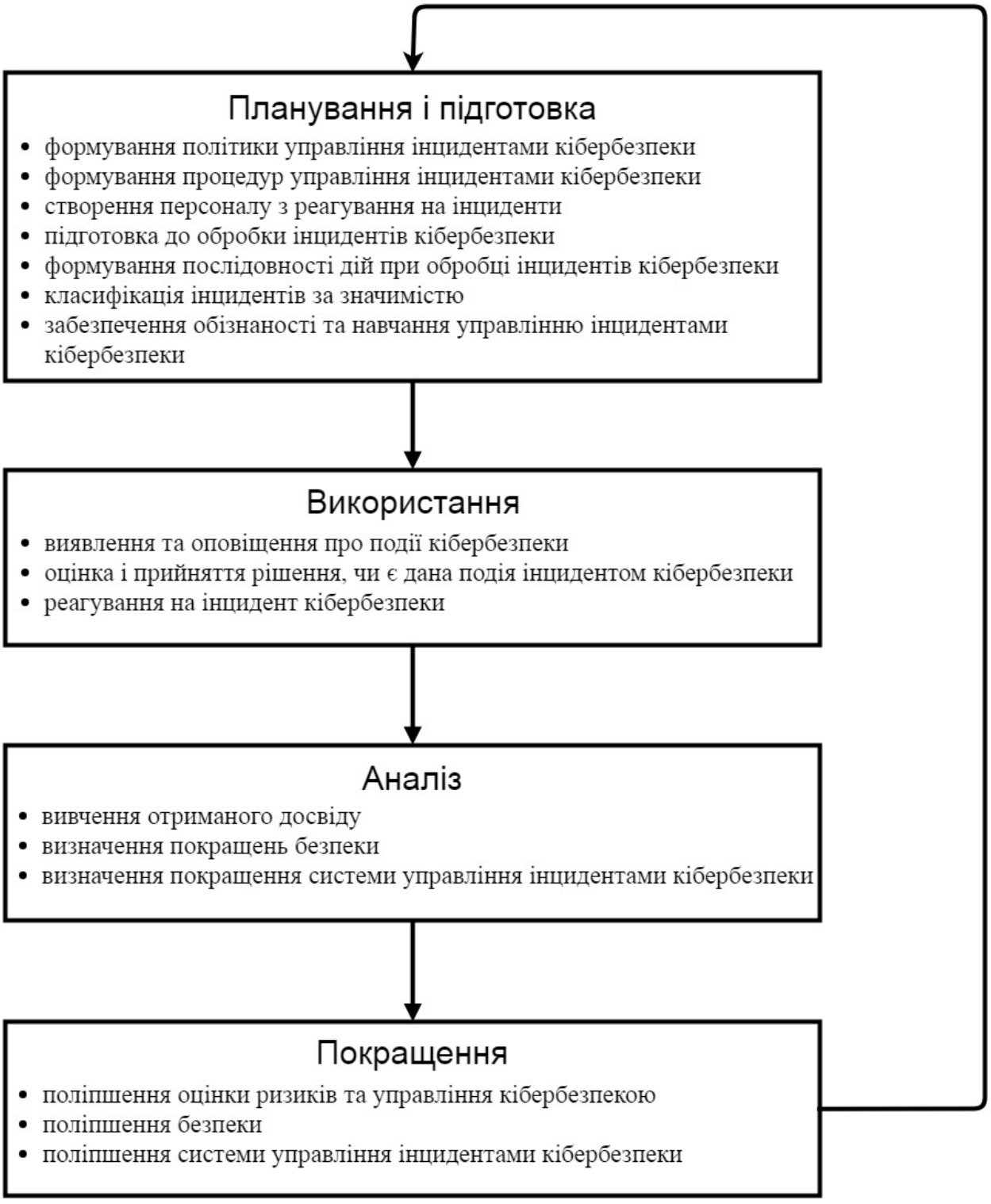


Рисунок 1.15 – Система управління інцидентами інформаційної безпеки

1.5 Висновки до першого розділу. Постановка задачі.

Проаналізувавши статистичні дані міжнародних компаній, ми ще раз впевнюємося в то, що будь яка інформація, яка має цінність, підпадає до сфери інтересів зловмисників. Тому, як сучасне законодавство, міжнародні стандарти так і науковці в інформаційній сфері прагнуть створити системи, процеси для безпечної обробку інформації користувачів, підприємств так і держави в цілому.

У першому розділі обґрунтована актуальність процесу управління інцидентами, яка підтверджується статистикою. Надані загальні вимоги система управління інцидентами інформаційної безпеки, їх схематична послідовність та описання процесів.

Показано, що кількість інцидентів з кожним роком збільшується їх різноманітність, також. Частка зловмисників, які націлених на ресурси України, в міжнародній статистиці, зросла. Це говорить про те, що потрібно вдосконалювати нормативну бузу, методики протидії реалізації інцидентів на основі вже існуючих і створювати нові. Грамотно розроблені процедури безпеки, методи і рішення можуть майже повністю зупинити зловмисників. Але для цього потрібні спільні зусилля фахівців, співробітників, партнерів і клієнтів підприємств, щоб зводити до мінімуму всі види атак і контролювати, щоб проблеми, які пов’язані з інцидентами управління кібербезпекою не переросли в катастрофу.

Постановка задачі: Складання рекомендаційної бази управління інцидентами кібербезпеки для рядових співробітників і керівників малих комерційних підприємств, що містить:

- планування системи управління інцидентами кібербезпеки;
- застосування системи управління інцидентами кібербезпеки;
- аналіз обробки інцидентів кібербезпеки;
- покращення системи управління інцидентами кібербезпеки;
- управління основними видами інцидентів на прикладі підприємства.

РОЗДІЛ 2
РЕКОМЕНДАЦІЇ ДЛЯ МАЛИХ КОМЕРЦІЙНИХ ПІДПРИЄМСТВ З УПРАВЛІННЯ ІНЦИДЕНАМИ КІБЕРБЕЗПЕКИ

2.1 Рекомендації щодо планування системи управління інцидентами кібербезпеки

Формування політики управління інцидентами кібербезпеки

Політика управління інцидентами ІБ призначена для персоналу, який має авторизований доступ до інформаційних систем підприємства та місцям їх розташування. Основні питання, які повинна включати політика управління інцидентами ІБ:

- огляд процедур виявлення подій, сповіщення (інформування) та збиранню відповідною інформації ІБ, і як ця інформація повинна використовуватися для визначення інцидентів ІБ. Цей огляд має містити перелік можливих подій ІБ, а також інформацію про те, як сповіщати про них, що сповіщати, коли і кому, а також як поводитися з новими подіями ІБ;
- огляд процесу оцінки інцидентів ІБ, включаючи перелік ролей, і подальші дії;
- короткий виклад дій після підтвердження того, що подія ІБ є інцидентом ІБ. Ці дії можуть бути такими:
- негайне реагування;
- сповіщення (інформування) відповідного персоналу та третіх сторін;
- установлення факту знаходження інциденту ІБ під контролем;
- подальше реагування;
- оголошення «кризової ситуації»;
- забезпечення безпечного зберігання свідоцтв в електронному вигляді на випадок судового розгляду або внутрішнього дисциплінарного розслідування;

- дії після вирішення інциденту ІБ, включаючи вилучення уроків та покращення управління інцидентами ІБ;
- опис діяльності співробітників на яких накладені обов’язки з реагування на інциденти ІБ, що включає наступні питання:
- організаційна структура співробітників з реагуванні на інциденти і основні ролі;
- цілі, сфера діяльності та повноваження цих осіб;
- зв'язок зі сторонніми організаціями;
- вимоги до програм забезпечення обізнаності та навчання управлінню інцидентами ІБ.

Формування процедур управління інцидентами кібербезпеки

Для створення системи управління інцидентами ІБ повинні бути розроблені детальні процедури для всіх етапів управління інцидентами ІБ.

Для етапу «Планування та підготовка» повинні бути сформовані процедури:

- підготовка до обробки інциденту ІБ;
- формування послідовності дій при обробці інцидентів ІБ;
- класифікація інцидентів ІБ за значимістю;

Для етапу «Застосування» повинні бути сформовані наступні процедури:

- виявлення і аналіз інциденту ІБ;
- стримування інциденту ІБ;
- усунення інциденту ІБ і відновлення після інциденту;
- збір доказів про інцидент ІБ.

Для етапу «Аналіз» повинні бути сформовані процедури:

- ідентифікація і документальне оформлення досвіду, видобутого з інцидентів ІБ;
- аналіз ефективності процедур реагування на інциденти ІБ і відновлення після інцидентів, а також ідентифікація покращення системи управління інцидентами ІБ в цілому (на основі видобутого досвіду);
- оновлення бази інцидентів ІБ.

Для етапу «Покращення» повинні бути сформовані наступні процедури:

- проведення оцінки ризиків по результатам обробки інцидентів;
- корегування захисних заходів по стримуванню, усуненню інцидентів ІБ і відновлення після них;
- корегування нормативних документів.

Накладення обов'язків реагування на інциденти кібербезпеки на діючих співробітників

Метою створення такого обов'язку є формування на підприємстві навченого і довіреного персоналу для управління інцидентами ІБ.

Структура, склад і кількість персоналу з реагування повинен відповідати розміру і структурі підприємства. Особи, на яких накладені обов'язки реагування на інциденти кібербезпеки повинні бути доступними для контакту так, щоб їх імена а також подробиці о контакті з ними були доступними на підприємстві.

Рівень повноважень таких співробітників повинен дозволяти підприємству необхідні дії, адекватні інциденту ІБ. Однак дії, що можуть вказати негативний вплив на діяльність підприємства, повинні бути узгоджені з вищим керівництвом.

Взаємодія осіб, на яких накладені обов'язки реагування на інциденти з підрозділами підприємства виконується по наступним напрямкам:

- співробітництво при обробці інциденту (якщо співробітництво необхідне);
- сповіщення і інформування про інцидент (за необхідністю);
- забезпечення обізнаності співробітників підприємства стосовно процесів і процедур системи управління інцидентами та їх змінах (поперед за все, про процедури виявлення і сповіщення про інциденти).

Підготовка до обробки інцидентів

При підготовці до обробки інциденту ІБ формуються:

- інфраструктура обробки інцидентів ІБ;
- база відомих інцидентів

При формуванні інфраструктури обробки інцидентів ІБ визначається інструментарій і ресурси, котрі можуть бути корисні у час обробки інциденту ІБ. До них відносяться: засоби зв'язку, комп'ютери, перелік критичних активів і т.п.

База відомих інцидентів ІБ формується на підставі всієї доступної інформації про інциденти, існуючі в різних джерелах, таких як: міжнародні і національні нормативні документи, присвячені обробці інцидентів ІБ, дані про результати обробки інцидентів ІБ організаціями-партнерами або іншими організаціями, а також інформація про інциденти ІБ з різних, але довірених джерел.

Відомості про інциденти ІБ повинні бути представлені в базі інцидентів у вигляді, зручному для використання і зрозумілими з точки зору їх розвитку: від подій, що визивають інцидент до можливих негативних наслідків інциденту.

Формування послідовності дій при обробці інцидентів

При плануванні обробки інцидентів формується послідовність дій при обробці, яка визначає початкову обробку інциденту ІБ, котра є загальною для всіх видів інциденту, і подальшу обробку інциденту ІБ, котра повинна бути адаптована до кожного конкретного типу інциденту.

Послідовність дій, яка представлена в таблиці [2.1], визначає основні кроки, які повинні бути виконані при початковій обробці інциденту. Після їх виконання, обробники інциденту повинні використовувати послідовність дій, які повинні бути адаптовані до кожного конкретного типу інциденту або загальну послідовність дій для некатегорованих інцидентів ІБ. В загальному вигляді така послідовність наведена в таблиці [2.2]

Таблиця 2.1 Послідовність дій при початковій обробці інциденту

Дія		ВПЗ
Виявлення та первісний аналіз інциденту		
1	Дія по виявленню інциденту	
1.1	Пошук і аналіз ознак інцидентів (провісників і покажчиків)	
1.2	Первісний аналіз небажаної події за допомогою бази відомих інцидентів	
2	Визначення реальності інциденту	
2.1	Збір і документування свідоцтв (доказів) небажаної події	
2.2	Визначення події помилковим інцидентом. Завершення обробки інциденту	
2.3	Визначення події реальним інцидентом. Продовження обробки інциденту	
3	Визначення інциденту по категорії (наприклад, відмова в обслуговуванні, зловмисний код, неавторизований доступ, збір інформації)	
4	Далі реалізується контрольний перелік дій по обробці інциденту певної категорії, якщо ж інцидент не підходить до прийнятих категорій, тоді реалізується загальний контрольний перелік дій по обробці некатегорованих інцидентів	

Послідовність дій забезпечує для обробників інцидентів керівництво по основним діям, які повинні бути виконані. Проте, вони не визначають обов'язкову послідовність кроків, яких треба дотримуватися завжди. Далі наведена послідовність дій при обробці некатегорованих інцидентів.

Таблиця 2.2 Загальна послідовність дій при обробці некатегорованих інцидентів

Дія		ВПЗ
Аналіз інциденту ІБ		
1	Збір та документування додаткових свідоцтв (доказів) інциденту для визначення його реальності та значущості	
2	Визначення значущості інциденту з точки зору впливу на бізнес	
2.1	Ідентифікація зачеплених активів і прогнозування, які активи будуть затронуті	
2.2	Оцінювання існуючого і потенціального впливу інциденту	
2.3	Визначення по матриці значущості інцидентів умов реагування на основі технічного впливу та зачеплених активів	
3	Повідомлення про інцидент відповідному внутрішньому персоналу і зовнішнім організаціям	
Стримування, усунення інциденту і відновлення після інциденту		
4	Отримання, документування, збереження і забезпечення безпеки і свідоцтв (доказів) інциденту	
5	Утримання інциденту	
6	Усунення інциденту	
6.1	Ідентифікація і мінімізація усіх уразливостей, котрі були застосовані	
6.2	Видалення компонентів інциденту (напр., зловмисного коду і т.д.)	
7	Відновлення після інциденту	
7.1	Відновлення зачеплених інцидентом систем до робочого стану	
7.2	Перевірка функціонування зачеплених систем	
8	Підготовка завершуючого звіту про інцидент	
Діяльність після інциденту		
9	Аналіз обробки інциденту	
10	Покращення системи управління інцидентами	

Класифікація інцидентів за значимістю

На підприємстві повинен бути сформований порядок обробки інцидентів ІБ, котрий полягає в тому, що обробка інцидентів ІБ здійснюється відповідно до їх значимості на основі двох факторів:

- існуючий і потенційний технічний вплив інциденту. Обробники інциденту повинні враховувати не тільки існуючий негативний технічний вплив інциденту (наприклад, неавторизований доступ на рівні користувача до даних), але також, можливо, майбутній технічний вплив інциденту, якщо він терміново не буде стриманий;
- критичність зачеплених активів. Активи, які зачеплені інцидентом (наприклад, Веб-сервери, зв'язність Інтернет, робочі станції користувача і додатки), мають різне значення для підприємства. Критичність активу заснована, головним чином, на його даних та послугах, взаємодії з іншими активами.

Критичність зачеплених активів та існуючий і потенційний технічний вплив інциденту визначають вплив інциденту ІБ на бізнес та значимість інциденту (критична - значимість 1, висока - значимість 2, середня - значимість 3, низька - значимість 4, несуттєва - значимість 5). Значимість інциденту вказує на пріоритетність його обробки, на ступінь його небезпеки. Наприклад, компрометація робочої станції користувача може привести до незначного збитку, пов'язаному з втратою цілісності або конфіденційності тільки інформаційних активів користувачів (Значимість 4). Доступ же на системному рівні може привести до серйозних порушень цілісності, конфіденційності і доступності критичних інформаційних активів, послуг та сервісів.

На підприємстві керівництво за значимістю інцидентів ІБ повинно бути задокументовано, наприклад, у вигляді матриці, що надана нижче в таблиці [2.3].

Таблиця 2.3 Примірна матриця для визначення значимості інцидентів ІБ

Існуючий вплив або ймовірний майбутній вплив інциденту	Критичність (важливість) активів, зачеплених в даний час або ті, котрі ймовірно будуть зачеплені інцидентом		
	Висока (пр. Веб-сервери, робочі станції системних адміністраторів)	Середня (пр. файлові сервери, сервери друку, поштовий сервер)	Низька (пр. робочі станції користувачів)
Доступ на системному рівні	Значимість 1	Значимість 2	Значимість 2
Неавторизована модифікація даних	Значимість 1	Значимість 2	Значимість 3
Неавторизований доступ до чутливих даних	Значимість 1	Значимість 2	Значимість 3
Неавторизований доступ на рівні користувача	Значимість 2	Значимість 3	Значимість 4
Недоступність послуг	Значимість 2	Значимість 3	Значимість 4
Роздратування (періодичне повідомлення на екрані, спливаючі картинки, що закривають екран і т.д)	Значимість 2	Значимість 5	Значимість 5

Забезпечення обізнаності та навчання управлінню інцидентами

Управління інцидентами кібербезпеки – це процес, котрий повинен підтримуватися персоналом, навченим діяльності по обробці інцидентів ІБ, і співробітниками підприємства, обізнаними у питаннях ІБ. Повинна існувати спеціальна програма навчання для персоналу, відповідального за ІБ і системних адміністраторів, та адміністраторів ІБ (якщо такі є на підприємстві).

Інструктажі зі співробітниками підприємства, що проводяться з метою забезпечення обізнаності, повинні містити:

- основи системи управління інцидентами ІБ, включаючи її сферу діяльності і послідовність дій по управлінню інцидентами ІБ;
- інформацію про процедури виявлення подій та інцидентів;
- інструкцію про те, як сповіщати про події і інциденти ІБ;
- інформацію про всі відомі інциденти і про результати управління інцидентами ІБ;

2.2 Рекомендації щодо застосування системи управління інцидентами кібербезпеки

Послідовність дій при обробці інциденту

Управління інцидентами ІБ на етапі використання системи управління інцидентами починається з виявлення події ІБ та завершується або виявленням хибності інциденту, або успішною обробкою інцидентом, або введенням антикризових дій. Послідовність дій при обробці подій або інцидентів ІБ на етапі використання системи управління інцидентами зображена на рисунку 2.1.

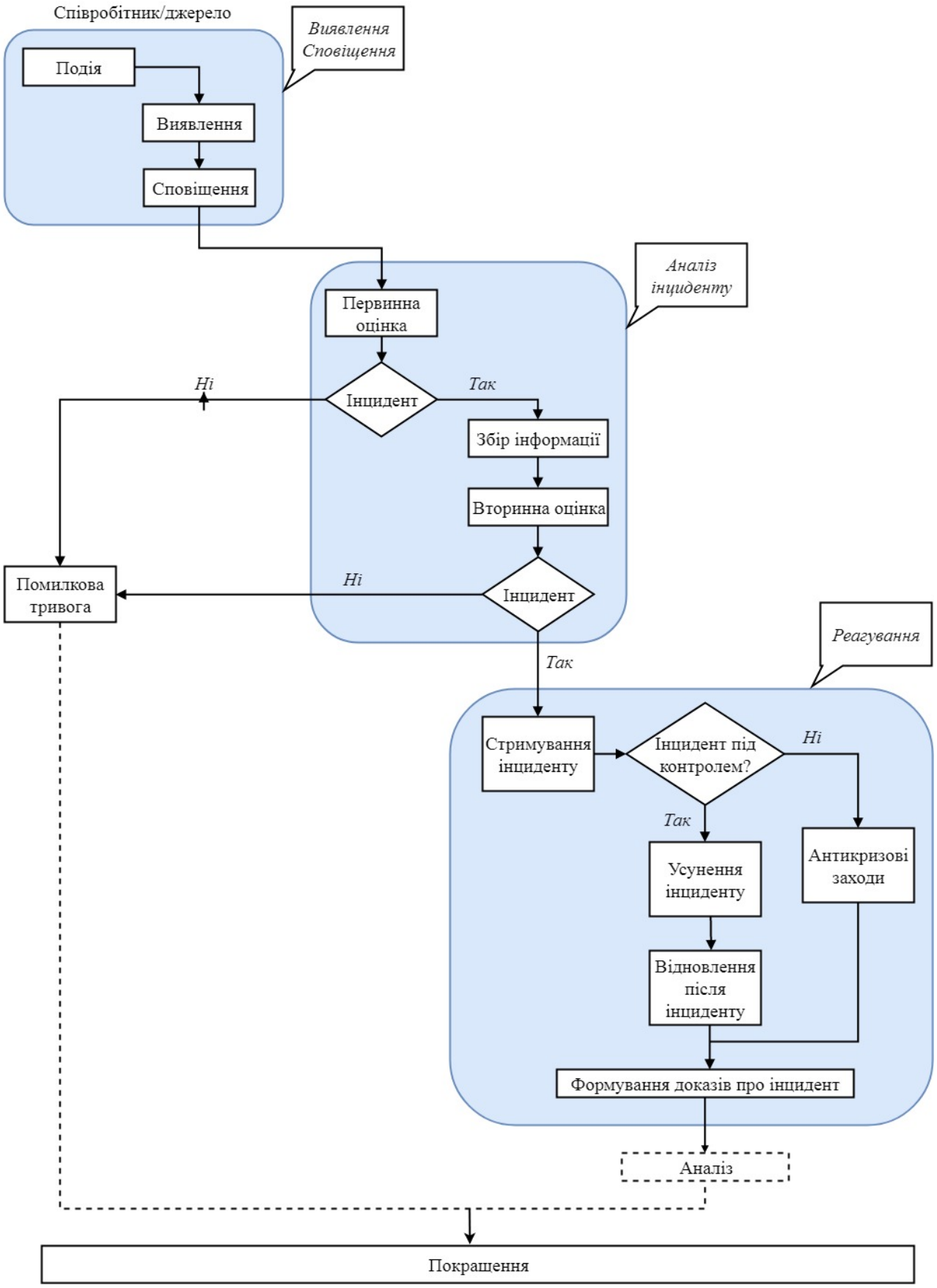


Рисунок 2.1 – Послідовність обробки подій та інцидентів ІБ на етапі використання системи управління інцидентами

Виявлення і аналіз інциденту

Виявлення інциденту ІБ здійснюється за допомогою систем виявлення вторгнень, антивірусного програмного забезпечення, записів моніторингу ІБ, співробітниками підприємства на основі ознак інцидентів ІБ. Ознаки інцидентів ІБ можна поділити на дві категорії: «вказівники» і «передвісники». «Передвісник» є ознакою того, що інцидент ІБ може трапитися у майбутньому. «Вказівник» - це ознака того, що інцидент ІБ, можливо, трапився або може трапитися зараз.

Приклади вказівників надані далі:

- антивірусне програмне забезпечення попереджає, що в системі з'явився вірус;
- користувачі скаржаться на повільний доступ до мережі Інтернет;
- системний адміністратор виявляє велику кількість поштових повідомлень з підозрілим змістом.

Приклади передвісників надані далі:

- публікація інформації про уразливості операційних систем чи ПЗ;
- загроза від групи хакерів, які заявляють що вони будуть атакувати підприємство.

Передвісники та вказівники інцидентів ІБ можуть бути виявлені співробітниками, які помітили ознаки нештатної ситуації. Співробітник, помітивши щось незвичайне або був проінформований про це автоматичними засобами, повинен сповісти групі реагування на інцидент, якщо така є на підприємстві, або особі, яка відповідальна за інциденти та події кібербезпеки.

Співробітник, який повідомив про подію ІБ, повинен заповнити звітну форму, установлену для системи управління інцидентів ІБ, так, щоб повідомити як можна більше інформації, що доступна йому в той момент. Переважно, щоб ця форма була в електронному вигляді.

Форма повідомлення «Звіт про подію ІБ» повинен містити наступну інформацію:

а) дата і час виявлення події;

б) дата і час сповіщення про подію;

в) інформація про особу, яка сповіла про подію ІБ;

г) опис події: що трапилося; як трапилося; чому трапилося; зачеплені інцидентом активи; виявленні уразливості.

Аналіз інцидентів ІБ починається з того що особи, на яких накладені обов'язки з реагування на інциденти повинні зафіксувати отримання заповненої звітної форми і проаналізувати її. Далі група реагування повинна тимчасово почати запис усіх фактів, що стосуються цієї події. Кожен документ, що стосується до інциденту, повинен бути з датою і підписаний обробником інциденту. Ця інформація і інші свідоцтва, що зібрані на цій стадії, можуть знадобитися у майбутньому для дисциплінарного або правового розслідування.

Якщо подія ІБ визначається як хибна, то форма «Звіт про подію ІБ» доповнюється інформацією про проведенні заходи, обґрунтуванням хибності події ІБ і записується в базу даних подій ІБ.

Якщо подія ІБ визначається як ймовірний інцидент, тоді заповнюється форма «Звіт про інцидент ІБ», в котрому повинно описуватися наступне:

а) дата і час виявлення події;

б) дата і час сповіщення про подію;

в) інформація про особу, яка сповіла про подію ІБ;

г) опис події: що трапилося; як трапилося; чому трапилося; реальний чи потенційний вплив інциденту ІБ на бізнес організації; зачеплені інцидентом активи; виявленні уразливості; передбачувана значимість інциденту ІБ.

Якщо інцидент був вирішений, тоді звіт повинен містити також інформацію стосовно здійснених захисних заходів і будь-якому отриманому досліді. Після заповнення звітної форми, вона повинна бути введена в базу даних інцидентів ІБ.

Якщо інцидент ІБ визначається як хибний, то форма «Звіт про інцидент ІБ» доповнюється інформацією про проведені заходи, обґрунтуванням хибності інциденту ІБ і записується в базу даних інцидентів ІБ.

Далі наведений приклад форми звіту про інцидент кібербезпеки:

Таблиця 2.4 – Приклад форми звіту про інцидент кібербезпеки

Потенційна спроба проведення атаки на вузол контрольованої інфраструктури					
Дата реєстрації:	01.01.2018	**Статус:**	Новий	**Тривалість впливу:**	2 дні
Уражені активи:	Персональний комп'ютер ПК-User (ip:10.420.424., mac:07:03:3323)	**Симптоми/ ознаки інциденту:**	Помітне сповільнення роботи ПК, погіршення швидкості Інтернету, періодично мерехтливий екран	**Дата початку інциденту:**	01.01.2018
Автор звіту	Іванов Іван Іванович	**Значимість**	Середня	**Дата завершення інциденту**	-
Сповіщенні про інцидент особи:	Петров Василь Сергійович, Шевченко Олег Олегович	**Дата і час сповіщення про інцидент:**	01.01.2018, 12:38:43	**Дата закриття інциденту**	-

Якщо інцидент ІБ визначається як реальний, то особи, що реагують на інциденти кібербезпеки визначає сферу діяльності інциденту, а саме: які мережі, комп'ютери або програмне забезпечення були зачеплені; хто або що стало джерелом; на що він вплинув або міг вплинути. Уточнюється значимість інциденту (за шкалою, прийнятою в організації) і визначається реальний або потенційний вплив інциденту ІБ на бізнес організації, виходячи з наступних можливих наслідків:

- фінансові втрати/переривання бізнес-діяльності;

- збиток комерційним або економічним інтересам;

- збиток інформації, що містить персональні дані;

- порушення правових і нормативних вимог;

- шкоди престижу організації.

Проведений аналіз повинен забезпечити персонал з реагування інцидентами інформацією, достатньою для визначення наступних дій, пов’язаних з реагуванням на інцидент, таких як стримування, усунення інциденту. При сумніві у виборі наступних дій, обробники інциденту повинні передбачати гірший розвиток ситуації, доки додатковий аналіз не вкаже на зворотне.

Реагування на інциденти

Стримування інциденту

Коли інцидент ІБ був виявлений і проаналізований, необхідне забезпечити стримування інциденту ІБ до того, як може бути завдані збитки активам системи.

При стримуванні інциденту важливо прийняти рішення про стратегії стримування (наприклад, відключення системи від кабельної або бездротової мережі, блокування окремих функцій). Для прийняття таких рішень необхідно, щоб стратегія і процедури для стримування інциденту були зумовлені. Підприємство повинно визначити прийнятні ризики і розробити супутні стратегії стримування.

У певних випадках стримування інциденту може бути відкладено на деякий час, для того щоб провести моніторинг активності атакуючого для збору додаткових показань. Проте ризик при цьому збільшується, так як стратегія відкладного стримування є небезпечною, оскільки атакуючий може встигнути задати шкоду.

При обробці інциденту власники системі зазвичай прагнуть ідентифікувати атакуючого. Хоча ця інформація є важливою, але обробники інциденту повинні перш за все вирішити задачу стримування, усунення і відновлення. Ідентифікація атакуючого може бути тривалим і марним

процесом, котрий може відвернути увагу персоналу з реагування на інциденти від досягнення їх головної мети – мінімізації впливу на бізнес.

Для ідентифікації атакуючого необхідно виконати наступні дії:

- визначення IP-адреса атакуючого. Задача полягає в визначенні реальності цієї адреси, наприклад, за допомогою тестування і трасування підозрілого вузла (трасування — покрокове виконання програми з зупинками на кожній стрічці або команді);

- сканування системи атакуючого. Щоб перевірити адрес атакуючого і зібрати більше інформації по атакуючому, застосовують, наприклад, сканери вразливостей;

- моніторинг можливих каналів зв'язку атакуючого.

По завершенні процедури стримування необхідно оцінити, чи знаходиться інцидент ІБ під контролем. Якщо підтверджується, що інцидент ІБ знаходиться під контролем, то персонал з реагування повинен перейти до наступних дій по реагуванню, направлених на усунення інциденту ІБ і відновлення нормальної роботи системи після інциденту.

Якщо не підтверджується, що інцидент ІБ знаходиться під контролем, то персонал з реагування інцидентами кібербезпеки повинен ініціювати «антикризові» дії.

Усунення інциденту і відновлення після інциденту

Дії по усуненню інциденту і відновленню після інциденту полягають в тому, що після того, як інцидент був стриманий, може знадобиться усунути елементи інциденту, такі як ліквідація зловмисного коду, блокування зламаних облікових записів або паролів користувача. Для деяких інцидентів усунення або не є необхідним, або виконується в час відновленням. При відновленні, персонал з реагування і системний адміністратор підготовлюють системи до нормального стану.

При відновленні можуть бути реалізовані наступні дії: відновлення програмних засобів з резервних копій, запуск компонентів систем з довіреного стану, заміна скомпрометованих файлів довіреними версіями, зміна паролів.

Якщо внаслідок знищення журналів реєстрація інцидентів ІБ стає невідомим повний об’єм інформації про інцидент, тоді може знадобиться повна перестройка системи, сервісу або мережі.

«Антикризові» дії

Якщо по завершенні процедур стримування персонал з реагування інцидентами визначив, що інцидент знаходиться не під контролем, то вони мають вжити «антикризові» дії для обробки інциденту. Для цього використовується, наприклад, попередньо розроблений план безперервності бізнесу.

Обробка всіх можливих інцидентів ІБ, які можуть вплинути на доступність, цілісність або руйнування системи, повинна бути визначена в плані безперервності бізнесу організації. Ці варіанти обробки інцидентів повинні бути безпосередньо пов’язані з пріоритетами бізнесу організації і супутніми часовими рамками відновлення і, відповідно, з максимально прийнятим часом простою систем і їх компонентів.

В плані необхідно визначити:

- попередження і підтримуючі заходи забезпечення безперервності бізнесу;

- організаційну структуру і відповідальність, яка пов’язана з управлінням безперервності бізнесу;

- основні положення безперервності бізнесу.

Формування та зберігання свідоцтв інцидентів

Після усунення інцидентів ІБ і відновлення після них необхідно сформувати заключний звіт по кожному інциденту. Звіт забезпечує довідкові дані, котрі можуть бути використані при обробці подібних інцидентів. Створення хронології подій є важливим зі сторони юридичних причин, так як дає можливість визначити оцінку збитку, викликаного інцидентом, в термінах будь-якої втрати програмного забезпечення і файлів, шкоди апаратним засобам і затрат персоналу (включаючи послуги по відновленню).

Для формування такого звіту, по-перше, оновлюється інформація в звіті «Звіт про інцидент ІБ»:

- що представляє собою інцидент ІБ;

- що стало його причиною, чим або ким він був викликаний;

- на що він вплинув або міг вплинути;

- реальний або потенційний вплив інциденту ІБ на бізнес організації;

- значимість інциденту ІБ (за шкалою небезпеки, прийнятою на підприємстві);

- дії, вжиті для розрішення інциденту.

Вивчення характеристик інциденту може вказати на вразливості та загрози ІБ. Ці данні можуть бути використані в процесі оцінки ризику.

По-друге, збираються статистичні дані про інциденти, які включають:

- кількість оброблених інцидентів. Слід виробляти роздільні підрахунки інцидентів для кожної категорії;

- час, затрачений на інцидент. Для кожного інциденту час може бути виміряний декількома способами: загальний час, затрачений на обробку інциденту (в тому числі підготовка); час від началу інциденту до його рішення; час для кожного етапу обробки інциденту (наприклад, стримування, відновлення).

На підприємстві повинно бути визначено, як довго повинні зберігатися свідоцтва (докази) інциденту. При цьому повинні бути враховані наступні фактори:

- судове переслідування. Якщо передбачається, що атакуючий буде переслідуватися по закону, то може стати необхідним зберігати свідоцтва інциденту, доки не будуть завершені всі юридичні дії;

- зберігання даних. Підприємство може мати політику, положення зберігання даних, які встановлюють, як довго можуть зберігатися визначені типи даних;

- витрати. Якщо підприємство зберігає багато компонентів інцидентів (наприклад, накопичувачі) і на протязі багатьох років, то витрати можуть бути суттєвими.

2.3 Рекомендації щодо аналізу обробки інцидентів

Вивчення отриманого досвіду

Після закінчення інциденту ІБ важливо вилучити уроки з його обробки, щоб в наступний раз цей інцидент ІБ можна було швидко виявити і вжити заходи. Отриманий досвід розглядається з точки зору:

- нових або змінених вимог до захисних заходів ІБ. Це можуть бути технічні або нетехнічні захисні заходи. В залежності від отриманих уроків вимоги можуть включати необхідність вдосконалення захисних заходів і проведення інструктажу для співробітників з метою забезпечення обізнаності у питаннях безпеки, а також необхідність перегляду або розробки нормативних документів з ІБ;

- змін в системі управління інцидентами ІБ і її процесах, формах звіту і базі даних подій і інцидентів ІБ;

Окрім того, необхідно проаналізувати послідовність інцидентів ІБ на наявність небезпечних тенденцій, що можуть бути застосовано для визначення потреби в захисних заходах або зміни підходів до обробки інцидентів ІБ.

В процесі аналізу, проведеного після вирішення інциденту ІБ, можуть бути визначені нові захисні заходи або зміни для існуючих як необхідні. Рекомендації і відповідні вимоги до захисних заходів можуть виявитися такими, що їх неможливо буде реалізувати негайно або по фінансовим або по експлуатаційним причинам. У такому випадку вони повинні бути передбачені у довгострокових цілях підприємства.

Після розрішення інциденту персонал з реагування на інциденти повинен проаналізувати все те, що сталося, з метою оцінки та визначення ступеню результативності реагування на інцидент ІБ. Цей аналіз призначений для

виявлення успішно задіяних елементів системи управління інцидентами ІБ і виявлення необхідності в будь-яких покращеннях.

Якщо значимість інциденту висока, то після розрішення інциденту необхідно провести нараду всіх заінтересованих сторін. На цій нараді повинні розглядатися наступні питання:

1 Чи працювали належним чином процедури, прийняті в системі управління інцидентами ІБ?

2 Чи застосовувалися процедури або методи, які сприяли виявленню інцидентів?

3 Чи були застосовані процедури або інструменти, які використовувались для стримування і усунення інциденту?

4 Чи були застосовані процедури, що допомагають відновленню інформаційних систем після інциденту?

Результати наради повинні бути задокументовані і за цими результатами повинні бути здійснені заходи по покращенню системи управління інцидентами.

2.4. Рекомендації щодо покращення системи управління інцидентами

В залежності від значимості обробленого інциденту ІБ при оцінці ризиків і управлінні ІБ може знадобитися враховувати нові загрози та уразливості. В результаті оцінки ризиків і управління ІБ може виникнути необхідність внесення змін в існуючі захисні заходи або застосування нових.

Організація повинна реалізовувати прийняті рішення по покращенню ІБ відповідно до виявлених в результаті аналізу потреб в реалізації оновлених або нових захисних заходів.

Безпосередньо після завершення інциденту ІБ повинні бути оновленні, якщо потребується, політики і процедури ІБ, для того щоб врахувати будь-які проблемні питання, ідентифіковані в процесі управління інцидентами ІБ. Важливою метою керівництва і персоналу з реагування на інциденти є

розповсюдження відомостей про оновлення політик і процедур ІБ серед усіх причетних співробітників підприємства. Ця мета може бути досягнута за допомогою включення інформації про прийняті зміни в програму інформування співробітників у питаннях безпеки.

Обґрунтовані та затверджені за результатами аналізу обробки інциденті ІБ зміни, що призначені для покращення областей системи управління інцидентами ІБ, повинні бути внесені в оновлені документи системи управління інцидентами ІБ.

Зміни в процесах, процедурах і звітних формах системи управління інцидентами ІБ повинні бути ретельно перевірені і протестовані до введення в експлуатацію.

2.5 Управління типовими інцидентами кібербезпеки на прикладі підприємства

Управління інцидентами, що найчастіше зустрічаються на малих комерційних підприємствах буде розглянуто на прикладі приватного підприємства (ПП) «H2O». Це комерційне підприємство займається продажем питної води на території міста Дніпро. Процес забезпечення управління інформаційною безпекою – одне із головних питань підприємства, тому що будь-які проблеми, пов’язані з ІБ та кібербезпекою можуть завдати великої матеріальної втрати та втрати репутації. Тому, питання захисту інформаційних активів актуальне і потребує своєчасного вирішення. Інформація стосовно даних про клієнтів зберігається у базі даних на внутрішніх та зовнішніх серверах компанії. Менеджери з продажу здійснюють дзвінки шляхом інтернет-телефонії на своїх робочих станціях.

Основні інциденти, які потребують більш детального розгляду виходячи з тонкощів і характеристик підприємства, це інциденти, що задані:

- несанкціонованим доступом;
- зловмисним ПЗ;
- збором інформації;

- відмовою в обслуговуванні.

Далі надані детальні рекомендації стосовно основних процесів управління цими інцидентами на прикладі. Були розглянуті питання:

- підготовки до обробки інциденту;
- вибору захисних заходів;
- послідовності дій і порядку обробки інциденту;
- виявлення і аналізу інциденту;
- стримування і усунення інциденту;
- відновлення після інциденту;
- збору і обробки свідоцтв інциденту.

НЕСАНЦІОНОВАНИЙ ДОСТУП

1. Підготовка до обробки інциденту

При підготовці до обробки інциденту необхідно побудувати можливі сценарію відомих інцидентів несанкціонованого доступу.

Сценарії розвитку інциденту будуються на основі критичних подій, які призводять до інциденту, і попередніх їм небажаних подій. У табл. 2.5 наведені критичні події їм передували небажані події інциденту несанкціонованого доступу.

Таблиця 2.5 – Небажані події інциденту відмови в обслуговуванні

Критична дія	Небажана подія
Неавторизоване використання вузла	Використання вузла для атаки інших систем. Створення нових облікових записів на адміністративному рівні. Порушення працездатності вузла. Модифікація або доповнення процесів / послуг. Модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації. Отримання привілейованого доступу до вузла
Неавторизована модифікація даних	Видалення або модифікація вмісту Web-сервера. Видалення або модифікація вмісту FTP-сервера.

	Порушення працездатності вузла. Недоступність послуг, сервісів.
Неавторизоване використання облікового запису користувача	Модифікація або доповнення процесів / послуг. Модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації. Недоступність послуг, сервісів. Отримання привілейованого доступу до вузла. Блокування облікових записів користувачів. Завантаження інструментарію зловмисника
Неавторизований доступ до бази даних	Несанкціоноване копіювання або модифікація даних. Несанкціонований доступ до файлів паролів

Інцидент несанкціонованого доступу може призвести до розкриття конфіденційної інформації, що спричинить за собою грошові втрати і шкоди репутації. Також інцидент несанкціонованого доступу може призвести до переривання одного або декількох бізнес-процесів і втрати даних, що в свою чергу викличе втрату продуктивності, внаслідок чого організації буде завдано матеріальних збитків і шкоди репутації.

На рис. 2.2 представлені приклади сценаріїв розвитку інциденту несанкціонованого доступу.

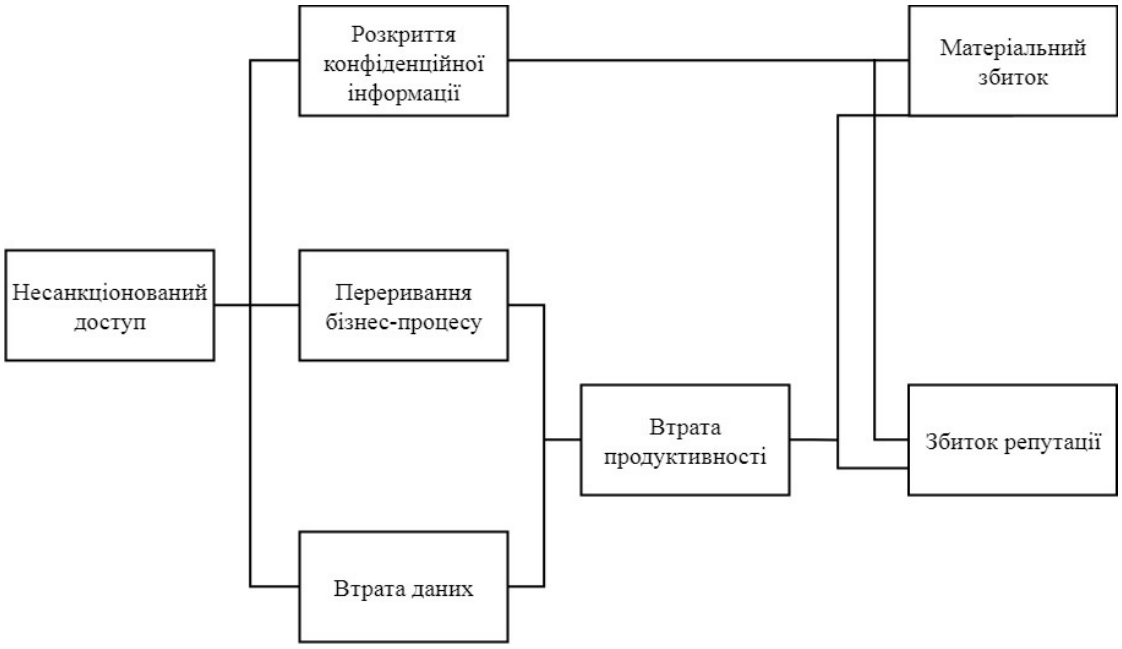


Рисунок 2.2 – Приклад сценарію розвитку інциденту несанкціонованого доступу

2. Вибір захисних заходів

Захисні заходи по управлінню доступом до систем, обрані на основі результатів оцінки ризиків, націлені на протидію реалізації виявлених загроз і зниження можливості використання вразливостей, пов'язаних з управлінням доступом. Такими захисними мірами, наприклад можуть бути:

- управління доступом користувачів до системи:
    1) процедури реєстрації та зняття з реєстрації користувачів щодо доступу до систем і сервісів;
    2) надання та контроль привілеїв і прав доступу користувачам до певних систем, програмного забезпечення, операційної системи і т.д.;
    3) парольний захист;
- управління мережевим доступом:
    1) визначення переліку дозволених мережевих послуг;
    2) заходи і процедури щодо захисту від несанкціонованого підключення до мережевих сервісів;
    3) аутентифікація віддалених користувачів;
    4) аутентифікація віддалених вузлів;
    5) управління маршрутизацією мережі;
    6) контроль мережевих з’єднань;
- управління доступом до операційної системи:
    1) процедури ідентифікації і аутентифікації вузла;
    2) процедури ідентифікації і аутентифікації користувачів;
- управління доступом до додатків:
    1) надання та контроль прав доступу користувачів до додатків;
    2) ізоляція систем, що обробляють важливу інформацію;
    3) моніторинг доступу і використання систем.

Крім того, за результатами оцінки ризиків можуть бути обрані захисні заходи, що дозволяють виявляти небажані події. що ведуть до інциденту

несанкціонованого доступу. До таких захисних заходів, наприклад, можуть належати:

- мережева і вузлова системи виявлення вторгнень (СОВ);
- міжмережевий екран.

Однак зважаючи на наявність залишкового ризику, появи нових загроз і вразливостей обраних захисних заходів може бути недостатньо, і інциденти кібербезпеки відбуватимуться. Необхідна своєчасна і оперативна обробка інцидентів кібербезпеки. щоб знизити можливі збитки від них.

На основі аналізу сценаріїв інциденту повинні бути визначені захисні заходи щодо стримування, усунення інциденту і відновленню після нього. Ці заходи вибираються і реалізуються персоналом з реагування на інциденти відповідно до сценарію розвитку інциденту.

До захисних заходів, стримуючим інцидент несанкціонованого доступу, відносяться:

- ізолювання вузлів і систем, які зазнали інциденту;
- блокування послуг, які зазнали інциденту:
- блокування маршрутів атакуючого;
- блокування облікових записів користувачів, які могли бути використані при інциденті.

Заходами щодо усунення інциденту і відновленню після інциденту несанкціонованого доступу можуть бути:

- відновлення з резервної копни атакований ОС або ПЗ;
- зміна всіх паролів у всіх системах, які мали відносини з атакований системою, а також перегляд процедур пральний захисту;
- ідентифікація всіх вразливостей, які були використані. і визначення стратегії для їх зменшення.

3. Послідовність дій і порядок обробки інциденту

Для забезпечення ефективного реагування на інцидент в підприємстві повинна бути сформована послідовність дій при обробці інцидентів несанкціонованого доступу. Ця послідовність приводиться в табл. 2.6.

Послідовність дій може змінюватися в залежності від особливостей інцидентів і стратегій щодо стримування інциденту, обраних конкретною організацією.

В організації повинен бути визначений порядок обробки інцидентів несанкціонованого доступу в залежності від їх значимості. Орієнтовна матриця визначення значущості інцидентів неавторизованого доступу показана в табл. 2.7.

Заголовки стовпців показують різну ступінь критичності активів, а заголовки рядків – різні категорії технічного впливу. Рівень значущості інциденту в матриці визначає пріоритетність його обробки.

Таблиця 2.6 – Послідовній дій при обробці інциденту відмови несанкціонованого доступу

Дія		Завершено
Аналіз інциденту		
1	Збір і документування додаткових свідчень (доказів) інциденту для визначення його реальності і значимості	
2	Визначення значущості інциденту з точки зору його впливу на бізнес	
2.1	Ідентифікація порушених активів і прогнозування, які активи можуть бути порушені	
2.2	Оцінювання існуючих і потенційних впливів інциденту	
2.3	Визначення по матриці значущості інцидентів умов реагування на основі технічного впливу і порушених активів	
3	Повідомлення про інцидент відповідному внутрішньому персоналу і зовнішнім організаціям	
Стримування, усунення інциденту і відновлення після інциденту		
4	Виконання початкового стримування інциденту (наприклад, блокування облікових записів користувача, які могли бути використані при атаці)	
5	Отримання. документування, збереження і забезпечення безпеки свідоцтв (доказів) інциденту	
6	Необхідність упевнитися в стримуванні інциденту	
6.1	Аналіз інциденту і визначення, чи достатньо було стримування (включаючи перевірку інших систем на ознаки вторгнення)	
6.2	Реалізація додаткових заходів стримування при необхідності	
7	Усунення інциденту	
7.1	Ідентифікація та мінімізація всіх вразливостей, які були використані	
7.2	Видалення компонентів інциденту	
8	Відновлення після інциденту	
8.1	Відновлення порушених інцидентом систем до робочого стану	
8.2	Перевірка функціонування порушених систем	
9	Підготовка завершального звіту про інцидент	
Діяльність після інциденту		

Таблиця 2.7 Примірна матриця визначення значимості інцидентів відмови в обслуговуванні

Існуючий вплив або ймовірний майбутній вплив інциденту	Критичність (важливість) активів, котрі зачеплені в даний час або які, цілком ймовірно, будуть порушені інцидентом		
	Висока (наприклад. Зв'язність з Internet. Web-сервери. робочі станції системних адміністраторів)	Середня (наприклад, сервери файлів, сервери друку, поштовий сервер)	Низька (наприклад, робочі станції користувачів)
Неавторизований доступ на системному рівні	Значимість 1	Значимість 2	Значимість 3
Неавторизований доступ до чутливих даних	Значимість 1	Значимість 3	Значимість 3
Неавторизований доступ на рівні користувача	Значимість 2	Значимість 3	Значимість 4
Роздратування (приставання)	Значимість 2	Значимість 5	Значимість 5

4. Виявлення і аналіз інциденту

Виявлення та аналіз інцидентів несанкціонованого доступу може відбуватися з допомогою різних передвісників і покажчиків інциденту. У табл. 2.8 перераховуються можливі передвісники інциденту несанкціонованого доступу і наводяться дії, які можуть запобігти появі інциденту.

Таблиця 2.8 – Передвісники інциденту несанкціонованого доступу і дії по їх запобіганню

Передвісники	Дії по запобіганню
Розвідувальна діяльність з метою упорядкування структури вузлів і послуг та ідентифікації вразливостей. Активність може включати перегляди портів, вразливостей, тести по методу запит-відповідь, трасування маршрутів і захоплення заголовків, банерів. Така активність виявляється, головним чином, за допомогою СВВ і за допомогою аналізу журналів моніторингу ІБ	Обробники інцидентів повинні виявити особливі зміни при зондуванні, наприклад, несподіваний інтерес до конкретного номеру порту або вузла. Якщо ця активність вказує на вразливість, яка може бути використана, організація може мати час заблокувати майбутні атаки шляхом зменшення цієї уразливості (наприклад, блокування послуги, зміну правил мережевого екрану)
Про можливості несанкціонованого доступу повідомляється публічно, і це становить значну загрозу для підприємства	Організація повинна розслідувати можливості несанкціонованого доступу і. якщо можливо, змінити засоби управління ІБ. щоб мінімізувати потенційний вплив цього інциденту на організацію

Покажчики інциденту - це ознаки небажаних подій, які можуть бути виявлені за допомогою:

- повідомленні мережевих і вузлових СВВ;
- перегляду журналів моніторингу ІБ;
- перегляду статистики мережевого екрану;
- повідомлення користувачів про відхилення в роботі систем.

Вказівники небажаних подій інциденту несанкціонованого доступу наведені в табл. 2.9.

Таблиця 2.9 – Вказівники небажаних подій інциденту впровадження зловмисного коду

Можливі вказівники	Небажані події
Незвичайний трафік до вузла і від вузла	Використання вузла для атаки інших систем
Зміни в конфігурації систем, що включають: – несподівані відкриті порти; зміни в стані систем (повторні старти, закриття); – зміни в політиках журналу реєстрації і даних; – новий обліковий запис користувача або групи на адміністративному рівні.	Модифікація або доповнення процесів/послуг. Модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації. Недоступність послуг, сервісів. Порушення працездатності вузла. Отримання привілейованого доступу до вузла. Блокування облікових записів користувачів. Завантаження інструментарію зловмисника
Надмірна активність в мережі	Модифікація або доповнення процесів/послуг. Порушення працездатності вузла. Недоступність послуг, сервісів. Завантаження інструментарію зловмисника
Повідомлення користувачів про недоступність послуг, серверів	Використання вузла для атаки інших систем. Модифікація або доповнення процесів / послуг. Модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації. Недоступність послуг, сервісів. Порушення працездатності вузла. Блокування облікових записів користувачів. Завантаження інструментарію зловмисника. Видалення або модифікація вмісту Web-сервера. Видалення або модифікація вмісту FTP-сервера
Повідомлення користувачів про модифікацію даних (наприклад, спотворений Web-сайт, Web-сторінка)	Видалення або модифікація вмісту Web-сервера. Видалення або модифікація вмісту FTP-сервера.
Повідомлення про виявлення вторгнень в мережу або до вузла	Використання вузла для атаки інших систем. Порушення працездатності вузла. Видалення або модифікація вмісту Web-сервера. Видалення або модифікація вмісту FTP-сервера. Порушення працездатності вузла. Недоступність послуг, сервісів. Завантаження інструментарію зловмисника. Несанкціоноване копіювання або модифікація даних. Несанкціонований доступ до файлів паролів
Нові файли або каталоги з незвичайними іменами (наприклад, виконавчі символи, пробіли, крапки)	Несанкціоноване копіювання або модифікація даних. Модифікація або доповнення процесів/послуг. Модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації. Завантаження інструментарію зловмисника. Видалення або модифікація вмісту FTP-сервера

Продовження таблиці 2.9 – Вказівники небажаних подій інциденту впровадження зловмисного коду

Можливі вказівники	Небажані події
Незвичайні повідомлення журналів операційної системи і ПЗ	Використання вузла для атаки інших систем. Модифікація або доповнення процесів/послуг. Модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації
Спроби доступу до критичних файлів	Модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації. Отримання привілейованого доступу до вузла. Несанкціоноване копіювання або модифікація даних. Несанкціонований доступ до файлів паролів
Збільшення використання ресурсів	Використання вузла для атаки інших систем. Модифікація або доповнення процесів/послуг. Порушення працездатності вузла. Недоступність послуг, сервісів. Завантаження інструментарію зловмисника.
Неправильне використання облікових записів (наприклад, застосовується невживаний обліковий запис, обліковий запис використовується багатьма користувачами, велике число заблокованих облікових записів)	Використання вузла для атаки інших систем. Створення нових облікових записів або групи на адміністративному рівні. Отримання привілейованого доступу до вузла. Блокування облікових записів користувачів. Завантаження інструментарію зловмисника. Несанкціоноване копіювання або модифікація даних. Несанкціонований доступ до файлів паролів
Записи журналу rгоху-сервера. показують завантаження інструментарію зловмисника	Отримання привілейованого доступу до вузла. Завантаження інструментарію зловмисника

Інциденти неавторизованого доступу відрізняються від інших типів інцидентів тим, що вони можуть; відбуватися в кілька етапів. Зазвичай атакуючі виконують множинні розвідувальні дії, щоб визначити внутрішню структуру мереж: ідентифікувати вузли; визначити, які операційна система, послуги і програми встановлені на кожному вузлі. Розвідувальні дії повинні контролюватися, щоб усвідомити можливий ризик.

Після завершення розвідувальних дій атакуючі починають вживати дії щодо здійснення несанкціонованого доступу до систем. Деякі уразливості дозволяють привілейований доступ отримати відразу, в один етап, в той час як інші уразливості забезпечують тільки доступ на рівні користувача. Більшість атакуючих шукають доступ до систем на рівні адміністратора. Вони прагнуть

визначити уразливості, які можуть надати привілейований доступ. Якщо така вразливість не розпізнається або не може бути використана, атакуючі можуть намагатися знайти і використовувати уразливості, які забезпечать доступ на рівні користувача, і потім проводити додаткові атаки, щоб підвищити рівень доступу. Через те, що цей процес може зайняти значний час, ця атака може бути виявлена на проміжному етапі, коли деякий доступ був отриманий, але пошук доступу триває. Група реагування на інциденти повинна спробувати виявити і почати обробку таких інцидентів до того, як буде отримано повний доступ на рівні адміністратора.

Під час інцидентів неавторизованого доступу важко відрізнити звичайну активність від зловмисної активності. Такі покажчики, як відключення компонентів систем, зміни конфігурації моніторингу, цілком ймовірно є авторизованої діяльністю, а не атаками. Ключем до визначення джерела активності є процес управління змінами інформаційної сфери в організації. Якщо заплановано обслуговування системи, як. наприклад, оновлення операційної системи, ця інформація повинна доводитись персоналу7, який спостерігає і аналізує провісники і покажчики. Тоді при виявленні підозрілих покажчиків аналітик може визначити, що вони викликані планової активністю обслуговування.

При встановленні ступеня небезпеки інциденту несанкціонованого доступу визначення існуючого і потенційного технічного впливу інциденту може бути дуже важким. Через те, що атакуючі хочуть підняти привілеї доступу на рівні користувача до доступу на рівні адміністратора, поточні інциденти слід потенційно ідентифікувати як доступ на системному рівні. Поточне вплив інциденту може бути важко визначити, поки не проведено розширений аналіз. Однак часто необхідно, щоб небезпека інциденту побуту визначена до того, як завершиться аналіз. Цьому, ґрунтуючись на оцінці поточного впливу, краще допустити, що інцидент неавторизованого доступу призведе до більш небезпечних наслідків, тобто підвищити його.

5. Стримування і усунення інциденту та відновлення після нього

Час реагування на інцидент є критичним при стримуванні інциденту несанкціонованого доступу. Щоб визначити точно, що сталося, може знадобитися розширений аналіз ; в разі активної атаки стан системи може швидко змінюватися. У більшості випадків після виконання початкового аналізу інциденту і встановлення ступеня небезпеки цього інциденту доцільно реалізувати початкові заходи стримування і потім виконати подальший аналіз, щоб визначити, чи достатні були заходи стримування. Наприклад, може бути не очевидно, скопіював чи атакуючий системний файл паролів. Процедура відключення вузла від мережі, поки обробники інциденту визначають, чи був скомпрометований файл паролів, має перешкоджати атакуючому використовувати ці паролі. У більшості середовищ, проте, це не так. Через довірених відносин між системами і користувачами, що забезпечують одні й ті ж паролі або паролі для багатьох систем, вкрадені паролі часто використовуються для доступу до інших систем. Інцидент може швидко розширитися від одного вузла до багатьох вузлів за короткий час.

Обробникам інцидентів складно вибрати стратегії стримування. так як якщо вони допускають найгірше, то стратегія стримування може заблокувати всі мережі і системи. Обробники інцидентів повинні розглянути більш помірні рішення, які спрямовані на зменшення ризику до прийнятного рівня, ніж блокування всіх мереж і систем (якщо звичайно, ступінь зловмисної активності не так велика). Послідовність вживаються захисних заходів при стримуванні інциденту несанкціонованого доступу може бути такою:

– ізолювання порушених вузлів і систем. Це найпростіший прийом зі стримування інциденту несанкціонованого доступу - від'єднати кожну порушену систему і вузол. Це охороняє системи від подальшої компрометації. Однак проблемою може бути ідентифікація всіх порушених систем. Атакуючі часто використовують одну скомпрометовану систему як джерело атак проти інших внутрішніх систем. Обробники повинні досліджувати інші системи з точки зору ознак успішних атак;

– блокування порушених послуг. Якщо атакуючий використовує конкретну послугу, щоб отримати неавторизований доступ, то стримування може являти собою тимчасове або постійне блокування цієї послуги. Наприклад, якщо атакуючий використовує уразливість FTP і неавторизований доступ обмежується файлами даних FTP, то інцидент може бути стриманий тимчасовим блокуванням послуги FTP. Якщо FTP використовується для несанкціонованого доступу до інформаційних активів, тоді послуга FTP повинна бути блокована постійно;

– блокування маршрутів атакуючого. Слід перешкоджати доступу атакуючого до сусідніх активів, які можуть бути наступними цілями. Приклади: блокування вхідних з'єднань до конкретного сегменту мережі або від'єднання сервера віддаленого доступу;

– блокування облікових записів користувача, які могли бути використані при атаці. Одні і ті ж облікові записи і паролі, які були скомпрометовані в одній системі, можуть: працювати в інших системах. Отже, може знадобитися блокування цих облікових записів. Обробники також повинні визначити нові облікові записи користувача, які можуть бути створені атакуючим.

Якщо при усуненні інциденту і відновленні після інциденту несанкціонованого доступу обробники інцидентів припускають, що атакуючий отримав доступ до системи, то можна довіряти ОС. У цьому випадку необхідно відновити операційну систему і ПЗ з резервної копії і потім захистити систему. Рекомендується зміна всіх паролів у всіх системах, які мали відносини з атакований системою. Інциденти несанкціонованого доступу, як правило, використовують безліч вразливостей. Тому важливо для обробників ідентифікувати всі уразливості, які були використані, і визначити стратегії для їх зменшення.

Якщо атакуючий отримує менший рівень доступу, ніж рівень адміністратора, то дії щодо усунення та відновлення можуть відповідати рівню, до якого атакуючий отримав доступ. Повинні бути виконані дії, які зменшили б ризик. Наприклад, якщо атакуючий отримав доступ на рівні користувача

шляхом відгадування слабкого пароля, тоді цей пароль не тільки повинен бути замінений більш сильним паролем, але також адміністратор і власник системи повинні скорегувати вимоги до паролів, можливо, переглянути політики парольного захисту.

6. Збір і обробка свідоцтв інциденту

При зборі і обробці свідчень (доказів) інциденту несанкціонованого доступу і підготовці завершального звіту необхідно зафіксувати відносяться до цього інциденту дані, що включають записи журналів моніторингу ІБ вузлів і додатків, попередження про виявлення вторгнення і журнали МСЕ. Ці дані забезпечать доказ інциденту несанкціонованого доступу. Інциденти неавторизованого доступу частіше, ніж більшість інших інцидентів, ведуть до судового розгляду. Тому, важливо дотримуватися встановлених процедур збору та обробки свідчень для подальшого розслідування інциденту несанкціонованого доступу.

ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

1. Підготовка до обробки інциденту

При підготовці до обробки інциденту необхідно побудувати можливі сценарії відомих інцидентів, впроваджених зловмисним кодом. В наступній таблиці [2.10] наведені критичні дії і пов’язані з ним небажані події.

Інцидент впровадження шкідливого коду може призвести до розкриття конфіденційної інформації, розкрадання інтелектуальної власності, що зберігається в електронній формі, що спричинить за собою грошові втрати і шкоди репутації. Також інцидент впровадження шкідливого коду може призвести до переривання одного або декількох бізнес-процесів і втрати даних, збільшення часу на виконання завдань в системі, помилок користувачів, що в свою чергу викличе втрату продуктивності, внаслідок чого організації буде завдано матеріальних збитків і шкоди репутації.

Таблиця 2.10 – Критичні дії і небажані події інциденту заданого зловмисним програмним забезпеченням

Критична дія	Небажана подія
Вірус	Зміни в шаблонах документів текстової обробки, великоформатних таблиць і т.д. Недоступність файлів.
	Видалення або руйнування файлів. Порушення в роботі програмного забезпечення. Компрометація кореня вузла: • використання вузла для атаки інших систем: • порушення працездатності вузла: • модифікація або доповнення процесів послуг; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації: • отримання привілейованого доступу до вузла. Нестабільність або відмова системи. Виконання невідомих процесів. Недоступність послуг. Вірусна містифікація: • нав'язування неправдивої інформації про стан системи: • навіювання почуття тривога, паніки користувачам: • роздратування користувачів
Хробак	Недоступність файлів. Порушення в роботі програмного забезпечення. Компрометація кореня вузла: • використання вузла для атаки інших систем; • порушення працездатності вузла; • модифікація або доповнення процесів послуг; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації; • отримання привілейованого доступу до вузла. Нестабільність або відмова системи
Троянський кінь	Компрометація кореня вузла: • використання вузла для атаки інших систем; • порушення працездатності вузла; • модифікація або доповнення процесів послуг; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації; • отримання привілейованого доступу до вузла. Виконання невідомих процесів, таких як передача даних про атакується системі на віддалений вузол і дії, спрямовані на відмову в обслуговуванні конкретного вузла
Зловмисний мобільний код	Зміни в шаблонах документів текстової обробки, великоформатних таблиць і т.д. Недоступність файлів. Видалення або руйнування файлів. Порушення в роботі програмного забезпечення. Нестабільність або відмова системи. Виконання невідомих процесів. Недоступність послуг.

2. Вибір захисних заходів

Захисні заходи для запобігання впровадження шкідливого коду, обрані на основі результатів оцінки ризиків, націлені на протидію реалізації виявлених загроз і зниження можливості використання вразливостей для проведення атак. Такими захисними заходами, наприклад, можуть бути:

- використання антивірусного програмного забезпечення;
- забезпечення поінформованості користувачів про проблеми, пов'язані з впровадженням шкідливого коду;
- навчання користувачів безпечної обробки вкладень e-mail;
- застосування на критичних вузлах централізованих систем виявлення вторгнення;
- конфігурація серверів і клієнтів e-mail, спрямована на блокування підозрілих файлів;
- обмеження використання неосновних програм зі здібностями передачі файлу;
- використання установок безпеки Web-браузерів (систем перегляду), щоб обмежити поширення мобільного коду.

Крім того, за результатами оцінки ризиків можуть бути обрані захисні заходи, що дозволяють виявляти інциденти впровадження шкідливого коду. До таких захисних заходів, наприклад, можуть ставитися засоби моніторингу ІІБ організації. Зважаючи на високий рівень залишкового ризику, появи нових загроз і вразливостей обраних захисних заходів може бути недостатньо, і інциденти кібербезпеки відбуватимуться. Необхідна своєчасна і оперативна обробка інцидентів кібербезпеки. щоб знизити можливі збитки від них.

На основі аналізу сценаріїв інциденту повинні бути визначені захисні заходи щодо стримування, усунення інциденту і відновленню після нього. Ці заходи вибираються і реалізуються персоналом з реагування на інциденти відповідно до сценарію розвитку інциденту.

До захисних заходів, стримуючим інцидент впровадження шкідливого коду, відносяться:

- запобігання поширенню шкідливого коду на інші системи;
- отримання від постачальника оновлених антивірусних сигнатур для обробки нового шкідливого коду;
- конфігурація серверів і клієнтів e-mail з метою блокування повідомлень e-mail;
- блокування конкретних вузлів;
- відключення серверів e-mail;
- ізолювання мереж від Internet.

Заходами щодо усунення інциденту і відновленню після інциденту впровадження шкідливого коду можуть бути:

- виявлення і ізолювання інфікованих вузлів;
- оновлення антивірусних сигнатур;
- передача невідомого шкідливого коду постачальникам антивірусів;
- відновлення з резервних копій пошкоджених файлів;
- зміна всіх паролів у всіх системах;
- ідентифікація вразливостей, які були використані, і визначення стратегії для їх зменшення.

3. Послідовність дій і порядок обробки інциденту

Для забезпечення ефективного реагування на інцидент на підприємстві повинна бути сформована послідовність дій при обробці інцидентів впровадження зловмисного коду. Послідовність етапів може змінюватися в залежності від особливостей інцидентів і стратегій по стримуванню інциденту, що обрані підприємством. Ця послідовність наведена в таблиці 2.11.

Таблиця 2.11 – Контрольний перелік дій з обробки інциденту впровадження зловмисного коду.

	Дія	**Завершено**
	Аналіз інциденту	
1	Збір та документування додаткових свідоцтв (доказів) інциденту для визначення його реальності і значимості	
2	Визначення значимості інциденту з точки зору його впливу на бізнес	
2.1	Ідентифікація зачеплених активів і прогнозування, які активи можуть бути зачеплені	
2.2	Оцінювання існуючих і потенційних впливів інциденту	
2.3	Визначення по матриці значущості інцидентів умов реагування на основі технічного впливу і зачеплених активів	
3	Повідомлення про інцидент супутньому внутрішньому персоналу	
	Стримування, усунення і відновлення	
4	Стримування інциденту	
4.1	Виявлення інфікованих систем	
4.2	Вимкнення інфікованих систем від мережі	
4.3	Аналіз і зниження вразливостей, котрі були використані зловмисним кодом	
4.4	Блокування механізмів передачі зловмисного коду за необхідністю	
5	Усунення інциденту	
5.1	Видалення компонентів інциденту	
5.2	Зниження використаних вразливостей у відношенні до інших вузлів підприємства	
6	Відновлення після інциденту	
6.1	Відновлення зачеплених інцидентом систем у робочий стан	
6.2	Перевірка функціонування зачеплених систем	
7	Підготовка завершального звіту	
	Діяльність після інциденту	

На підприємстві повинен бути визначений порядок обробки інцидентів впровадження шкідливого коду в залежності від їх значимості. Орієнтовна матриця визначення значущості інцидентів впровадження шкідливого коду показана в табл. 2.12. Заголовки стовпців показують різну ступінь критичності активів, а заголовки рядків - різні категорії технічного впливу. Рівень

значущості інциденту впровадження шкідливого коду в матриці визначає пріоритетність його обробки. Заголовки стовпців показують різну ступінь критичності активів, а заголовки рядків - різні категорії технічного впливу. Рівень значущості інциденту впровадження шкідливого коду в матриці визначає пріоритетність його обробки.

Таблиця 2.12 Примірна матриця визначення значимості інцидентів впровадження зловмисного коду

Існуючий вплив або ймовірний майбутній вплив інциденту	Критичність (важливість) активів, котрі зачеплені в даний час або які, цілком ймовірно, будуть порушені інцидентом		
	Висока (наприклад. Зв'язність з Internet. Web-сервери. робочі станції системних адміністраторів)	Середня (наприклад, сервери файлів, сервери друку, поштовий сервер)	Низька (наприклад, робочі станції користувачів)
Вплив шкідливого коду на системному рівні	Значимість 1	Значимість 2	Значимість 3
Вплив шкідливого коду на чутливі дані	Значимість 1	Значимість 3	Значимість 3
Вплив шкідливого коду на рівні користувача	Значимість 2	Значимість 4	Значимість 4
Роздратування (Приставання)	Значимість 1	Значимість 5	Значимість 5

4. Виявлення і аналіз інциденту

Оскільки інциденти, пов'язані з використанням шкідливого коду, можуть приймати різні форми, вони можуть бути виявлені за допомогою ряду провісників і покажчиків. У табл. 2.13 перераховуються можливі передвісники атаки впровадження шкідливого коду і наводяться дії, які можуть запобігти виникнення інциденту.

Таблиця 2.13 – Передвісники інциденту впровадження шкідливого коду та реагування на них

Передвісники	Реагування
Система сповіщення попереджає про новий шкідливий код, який націлений на програмне забезпечення, що використовується організацією	Необхідно досліджувати новий вірус, щоб визначити, чи є він реальністю або містифікацією. Це може бути зроблено за допомогою Web-сайтів постачальника антивірусу і сайтів, що містять вірусні містифікації. Якщо зловмисний код підтверджується як автентичний, знадобиться забезпечити впевненість у тому. що антивірусне програмне забезпечення оновлюється сигнатурами вірусів щодо нового шкідливого коду. Якщо сигнатура вірусу поки недоступна (відсутній), а погроза є серйозною н невідворотною, така діяльність може бути блокована іншими засобами, такими як конфігурація серверів або клієнтів e-mail з метою заблокувати повідомлення e-mail, що збігається за характеристиками з новим шкідливим кодом. Група реагування може також побажати оповістити про новий вірус постачальників антивірусу.
Антивірусне програмне забезпечення виявляє і успішно «дезінфікує» або «відправляє на карантин» знову отриманий інфікований файл.	Необхідно визначити, яким чином шкідливий код був введений в систему і яку вразливість або недолік він намагався використовувати. Якщо шкідливий код може становити значний ризик для інших користувачів і вузлів, знадобиться зменшити недоліки, які були використані шкідливим кодом, щоб досягти системи, і які були б використані, щоб інфікувати цільової вузол.

Вказівники небажаних подій, що надані далі в таблиці 2.14 визначених в сценаріях інциденту, можуть бути виявлені за допомогою:

- повідомлень мережевих і вузлових СВВ;
- перегляду журналів моніторингу ІБ;

- повідомлення користувачів про відхилення в роботі систем.

Таблиця 2.14 – Вказівники небажаних подій інциденту впровадження зловмисного коду

Можливі вказівники	Небажані події
Антивірусне програмне забезпечення сповіщає про інфіковані файли	Зміни в шаблонах документів текстової обробки. великоформатних таблицях і т.д. Недоступність файлів. Видалення або руйнування файлів. Порушення в роботі ПЗ. Компрометація кореня вузла: • використання вузла для атаки інших систем: • порушення працездатності вузла: • модифікація ІТН доповнення процесів/послуг; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації; • отримання привілейованого доступу до вузла. Нестабільність або відмова системи. Виконання невідомих процесів. Недоступність послуг. Вірусна містифікація: • нав'язування неправдивої інформації про стан системи; • навіювання почуття тривоги, паніки користувачам; • роздратування користувачів
Антивірусне програмне забезпечення сповіщає про версії файлів, інфікованих «троянським конем»	Компрометація кореня вузла: • використання вузла для атаки інших систем; • порушення працездатності вузла; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації: • модифікація ІТН доповнення процесів/послуг; • отримання привілейованого доступу до вузла. Виконання невідомих процесів: • передача даних про атакується системі на віддалений вузол; • дії, спрямовані на відмову в обслуговуванні конкретного вузла
Несподіване зростання кількості надісланих та отриманих повідомлень e-mail	Недоступність файлів. Порушення в роботі ПЗ. Компрометація кореня вузла: • використання вузла для атаки інших систем; • порушення працездатності вузла; • модифікація або доповнення процесів / послуг; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації; • отримання привілейованого доступу до вузла. Нестабільність або відмова системи. Виконання невідомих процесів, таких як передача даних про атакується системі на віддалений вузол і дії, спрямовані на відмову в обслуговуванні конкретного вузла.

Продовження таблиці 2.14 – Вказівники небажаних подій інциденту впровадження зловмисного коду

Можливі вказівники	Небажані події
Повідомлення користувачів про зміни в шаблонах для документів текстової обробки	Зміни в шаблонах документів текстової обробки, великоформатних таблиць і т.д. Недоступність файлів. Видалення або руйнування файлів. Порушення в роботі програмного забезпечення. Компрометація кореня вузла: • використання вузла для атаки інших систем; • порушення працездатності вузла; • модифікація або доповнення процесів/послуг; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації; • отримання привілейованого доступу до вузла. Нестабільність або відмова системи. Виконання невідомих процесів. недоступність послуг
Повідомлення користувачів про видалення руйнуванні або недоступності файлів	Зміни в шаблонах документів текстової обробки, великоформатних таблиць і т.д. Недоступність файлів. Видалення або руйнування файлів. Порушення в роботі програмного забезпечення. Компрометація кореня вузла: • використання вузла для атаки інших систем; • порушення працездатності вузла; • модифікація або доповнення процесів / послуг; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації; • отримання привілейованого доступу до вузла. Нестабільність або відмова системи. Недоступність послуг
Незвичні елементи на екрані, такі як незвичні повідомлення і графіки	Порушення в роботі програмного забезпечення. Нестабільність або відмова системи. Виконання невідомих процесів. Недоступність послуг. Вірусна містифікація: • нав'язування неправдивої інформації про стан системи; • навіювання почуття тривоги, паніки користувачам; роздратування користувачів
Повідомлення користувачів про повільний старт у виконанні програм, нестабільності і повній відмові системи	Недоступність файлів. Видалення або руйнування файлів. Порушення в роботі програмного забезпечення. Компрометація кореня вузла: • використання вузла для атаки інших систем; • порушення працездатності вузла; • модифікація або доповнення процесів/послуг; • модифікація критичних файлів, програм; Нестабільність або відмова системи. Виконання невідомих процесів, таких як передача даних про атакується системі на віддалений вузол і дії, спрямовані на відмову в обслуговуванні конкретного вузла. недоступність послуг

Продовження таблиці 2.14 – Вказівники небажаних подій інциденту впровадження зловмисного коду

Можливі вказівники	Небажані події
Сканування порту і безуспішні спроби з'єднання, націлені на вразливу послугу (наприклад, відкриті ресурси загального користування Windows, HTTP)	Виконання невідомих процесів, таких як передача даних про атакується системі на віддалений вузол, і дії, спрямовані на відмову в обслуговуванні конкретного вузла
Зростання використання мережі	Порушення в роботі програмного забезпечення. Компрометація кореня вузла: • використання вузла для атаки інших систем; • порушення працездатності вузла; • модифікація або доповнення процесів / послуг; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації; • отримання привілейованого доступу до вузла. Нестабільність або відмова системи. Недоступність послуг. Виконання невідомих процесів, таких як передача даних про атаковану систему на віддалений вузол і дії, спрямовані на відмову в обслуговуванні конкретного вузла
Система виявлення вторгнення в мережу сповіщає про передачу «троянського коня» при взаємодії клієнт-сервер	Компрометація кореня вузла: • використання вузла для атаки інших систем; • порушення працездатності вузла; • модифікація або доповнення процесів/послуг; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації; • отримання привілейованого доступу до вузла. Виконання невідомих процесів, таких як передача даних про атакується системі на віддалений вузол і дії, спрямовані на відмову в обслуговуванні конкретного вузла
Записи в журналах реєстрації міжмережевого екрану і маршрутизатора про передачу «троянського коня»	Компрометація кореня вузла: • використання вузла для атаки інших систем; • порушення працездатності вузла; • модифікація або доповнення процесів / послуг; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації; • отримання привілейованого доступу до вузла. Нестабільність або відмова системи. Виконання невідомих процесів, таких як передача даних про атаковану систему на віддалений вузол і дії, спрямовані на відмову в обслуговуванні конкретного вузла

Продовження таблиці 2.14 – Вказівники небажаних подій інциденту впровадження зловмисного коду

Можливі вказівники	Небажані події
Мережеві з'єднання між вузлом і невідомими віддаленими системами	Компрометація кореня вузла: • використання вузла для атаки інших • систем; • порушення працездатності вузла; • модифікація або доповнення процесів / послуг; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації; • отримання привілейованого доступу до вузла. Нестабільність або відмова системи. Виконання невідомих процесів, таких як передача даних про атакується системі на віддалений вузол і дії, спрямовані на відмову в обслуговуванні конкретного вузла
Незвичайне і несподіване відкриття портів	Компрометація кореня вузла: • використання вузла для атаки інших систем; • порушення працездатності вузла; • модифікація або доповнення процесів / послуг; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації; • отримання привілейованого доступу до вузла. Нестабільність або відмова системи. Виконання невідомих процесів, таких як передача даних про атакується системі на віддалений вузол і дії, спрямовані на відмову в обслуговуванні конкретного вузла
Записи журналу моніторингу ІБ про виконання невідомих процесів	Передача даних про атаковану систему на віддалений вузол. Дії, спрямовані на відмову в обслуговуванні конкретного вузла. Порушення в роботі програмного забезпечення. Компрометація кореня вузла: • використання вузла для атаки інших систем; • порушення працездатності вузла; • модифікація або доповнення процесів/послуг; • модифікація критичних файлів, програм, бібліотек системи і файлів конфігурації; • отримання привілейованого доступу до вузла. Нестабільність або відмова системи. Недоступність послуг.
Несподівані діалогові вікна, що вимагають дозволу щось зробити, несподівана графіка, така як перекриваються або перекриті вікна повідомлень	Недоступність файлів. Видалення або руйнування файлів. Порушення в роботі програмного забезпечення. Нестабільність або відмова системи. Виконання невідомих процесів. Недоступність послуг. Вірусна містифікація: • нав'язування неправдивої інформації про стан системи; • навіювання почуття тривоги, паніки користувачам; • роздратування користувачів.

5. Стримування і усунення інциденту

У зв'язку з тим, що зловмисний код діє приховано і може швидко поширюватися на інші системи, необхідно завчасне стримування інциденту, пов'язаного з впровадженням зловмисного коду, щоб припинити його поширення та нанесення шкоди. Якщо інфікована система не є критичною, рекомендується відключити її від мережі негайно. Якщо система виконує критичні функції, їй слід залишатися в мережі тільки в тому випадку, якщо збиток, який буде завдано організації в результаті недоступності послуг, буде більше, ніж ризики безпеки, створювані невиконанням негайного відключення (від'єднання) цієї системи.

Інші дії, виконання яких може знадобитися при стримуванні інциденту, пов'язаного з впровадженням зловмисного коду, викладені нижче:

- запобігання поширенню зловмисного коду на інші системи;
- забезпечення поінформованості користувачів про проблеми, пов'язані з використанням зловмисного коду. Така інформація повинна включати в себе основний аналіз методів, які зловмисний код використовує для поширення, і симптоми інфікувань. Проведення регулярних навчальних занять з користувачами допомагає забезпечити впевненість у тому, що користувачі інформовані про ризики, які створюють шкідливий код. Користувачі повинні бути також проінструктовані про те, що вони повинні робити, якщо відбувається інфікування (наприклад, відключити робочу станцію від мережі, викликати службу допомоги), оскільки неправильна обробка «інфекції» може посилити навіть незначний інцидент;
- читання бюлетенів постачальників антивірусу. Користувачі можуть скористатися списками розсилки, що випускаються постачальниками антивірусного програмного забезпечення, які забезпечують своєчасну інформацію про нові загрози, які несе з собою шкідливий код;

- застосування на критичних вузлах централізованих систем виявлення вторгнення. СВВ може виявити ознаки інцидентів, пов'язаних з

використанням шкідливого коду, такі як зміни конфігурації і модифікації виконуваної системи. Програми перевірки цілісності файлів є корисними при ідентифікації порушених компонентів системи;

- виявлення і ізолювання інших інфікованих вузлів.

Антивірусні попереджувальні повідомлення є корисним джерелом інформації, але не кожна «інфекція» може бути виявлена антивірусним програмним забезпеченням. Обробники інцидентів можуть зіткнутися з необхідністю пошуку вказівників інфікування іншими засобами, такими як:

- виконання сканувань портів, щоб виявити вузли, що працюють з програмою «троянського коня» або невідомим (потайним) портом;
- використання антивірусних інструментальних засобів сканування і очищення, призначених для боротьби з конкретними видами шкідливого коду;
- перегляд журналів реєстрації з серверів e-mail, міжмережевих екранів і інших систем, через які може пройти шкідливий код. а також журналів реєстрації окремих вузлів;
- конфігурація програмного забезпечення з виявлення вторгнення в мережу і вузол для виявлення діяльності, пов'язаної з інфікуванням;
- проведення аудиту процесів, що проходять в системах, з метою підтвердження, що всі вони є коректними;
- передача невідомого шкідливого коду постачальникам антивірусів.

Зрідка шкідливий код. який не може бути точно ідентифікований антивірусним програмним забезпеченням, впроваджується в середу. Усунення шкідливого коду з систем і запобігання додаткового інфікування може бути ускладнене або неможливе без отримання від постачальника оновлених антивірусних сигнатур. Обробники інцидентів повинні бути знайомі з процедурами надання на розгляд копій невідомого шкідливого коду постачальникам антивірусів організації;

- конфігурація серверів і клієнтів e-mail з метою блокування повідомлень e-mail. Багато e-mail клієнтів можуть конфігуруватися вручну з метою блокування повідомлень e-mail за допомогою конкретних суб'єктів, імен

вкладень або інших критеріїв, які відповідають даному зловмисному коду. Таке конфігурування не є ні вирішенням проблеми захисту від випадкових помилок, ні ефективним рішенням, але воно може бути кращим варіантом, який можливий, якщо існує неминуча загроза, а антивірусні сигнатури ще недоступні;

- блокування конкретних вузлів. Наприклад, якщо зловмисний код намагається генерувати вихідні повідомлення e-mail або з'єднання, обробники повинні розглянути можливість блокування доступу до IP адресами або послуг. до яких інфікована система може намагатися підключитися. Крім того, якщо інфіковані вузли усередині організації намагатимуться поширити інфекцію далі, організація може побажати блокувати мережевий трафік від IP адрес цього вузла, щоб контролювати ситуацію, в той час як інфіковані вузли будуть фізично локалізовані і «дезінфікувати»;
- відключення серверів e-mail. При найбільш значущих інцидентах впровадження зловмисного коду, коли інфікуються сотні або тисячі внутрішніх вузлів, сервери e-mail можуть повністю переповниться вірусами, які намагаються поширитися через e-mail. Може виявитися необхідним відключити якийсь сервер e-mail, щоб зупинити поширення вірусів, породжених e-mail;
- ізолювання мереж від Internet. Мережі можуть переповниться трафіком хробаків в разі серйозного інфікування хробаками. Іноді хробак генерує такий величезний трафік по всій Internet, що периметри мережі стають повністю порушеними. Найкраще від'єднати організацію від Internet, особливо, якщо наявність доступу до Internet є для організації. по суті, марним через об'ємності трафіку «хробака». Така дія повинна захищати системи організації від атак зовнішніх «черв'яків»: якщо системи організації вже інфіковані. дана дія запобіжить їх атаки відносно інших систем і додаткову перевантаження трафіку.

Виявлення заражених вузлів і вразливих вузлів значно ускладнюється динамічної природою обчислювальних засобів. Якби всі вузли були включені (тобто споживали енергоживлення) і підключені до мережі постійно, то їх

чистка від шкідливого коду була б досить легкою. Фактична ж ситуація складається в тому. що вузли можуть бути інфіковані і відключені, перенесені в інші мережі або залишені без нагляду на час, поки власник системи буде відсутній в офісі. Уразливі вузли, відключені на той час, поки їх власники знаходяться у відпустці, могутній швидко інфікуватися, коли вони будуть включені знову. При виявленні вразливих вузлів і заражених вузлів не слід покладатися виключно на участь користувача. Однак організаціям часто не вистачає персоналу і часу, щоб відстежувати кожну машину вручну, особливо коли існує значна кількість мобільних користувачів і користувачів на дому. Автоматизовані методи також можуть бути неадекватними для ідентифікації всіх вузлів, наприклад, тих. які можуть завантажуватися для багатьох операційних систем або які можуть використовувати ПЗ віртуальних операційних систем. Організації повинні ретельно враховувати такі проблеми до того, як відбудеться значимий інцидент впровадження шкідливого коду з тим. щоб ці організації були готові реалізувати ефективні стратегії стримування.

6. Відновлення після інциденту

Антивірусне ПЗ ефективно ідентифікує та видаляє інфікування зловмисним кодом. Однак, деякі інфіковані файли не можна дезінфікувати. Файли можуть бути видалені або замінені чистими резервними копіями. Зачеплене ПЗ може бути інстальоване повторно. Якщо зловмисний код забезпечив атакуючим доступ на системному рівні, то може бути неможливим визначити, які інші дії могли виконати атакуючі. В таких випадках система повинна бути відновлена з попередньої неінфікованої резервної копії, або перебудована з нуля. Потім цю систему слід захистити таким шляхом, щоб вона була несприйнятлива до іншої інфекції, властивою тому ж самому зловмисному коду. Рекомендується також змінення всіх паролів у всіх системах, які мали відношення з атакованою системою.

7. Збір і обробка свідоцтв інциденту

Часто шкідливий код передається або автоматично, або випадково інфікованими користувачами, тому виявлення джерела шкідливого коду є дуже складним і трудомістким процесом. Проте збір зразків шкідливого коду в деяких випадках може бути корисним для проведення подальшого розслідування. Виявлення джерела шкідливого коду є дуже складним і трудомістким процесом. Проте збір зразків шкідливого коду в деяких випадках може бути корисним для проведення подальшого розслідування.

ЗБІР ІНФОРМАЦІЇ

1. Підготовка до обробки інциденту

При підготовці до обробки інциденту необхідно побудувати можливі сценарії відомих інцидентів збору інформації. В таблиці 215 наведені критичні дії та пов’язані з ними небажані події інциденту збору інформації.

Таблиця 2.15 – Небажані події інцидентів збору інформації.

Критична дія	Небажана подія
Ідентифікація топології мережі	Ідентифікація доступних серверів і адрес в мережі за допомогою: • аналізу заголовків переданих пакетів; • сканування DNS-сервера. Ідентифікація активних вузлів за допомогою: • відправки тестових запитів по випадковим мережевих адрес; • зондування мережі.
Ідентифікація вразливостей системи	Ідентифікація операційної системи вузла за допомогою зондування мережі. Ідентифікація мережевих служб на вузлах і версій ПЗ цих служб шляхом: • відправки тестових запитів по випадковим мережевих адрес: • аналізу заголовків переданих пакетів, які були перехоплені в процесі пасивного прослуховування мережі: • зондування мережі. Сканування доступних мережевих портів. Сканування одного або декількох сервісів з відомими уразливими по діапазону мережевих адрес.
Ідентифікація способу отримання конфіденційної інформації	Вилучення даних аутентифікації з перехоплених в процесі пасивного прослуховування мережі пакетів. Витяг вмісту електронних листів, перехоплених в процесі пасивного прослуховування мережі.

Інцидент збору інформації може призвести до розкриття конфіденційної інформації при пасивному прослуховуванні мережі внаслідок передачі її в незахищеному віще по каналах зв'язку або внаслідок отримання атрибутів аутентифікації. Це спричинить за собою матеріальні збитки організації та збитки її репутації. Також, якщо стався інцидент збору інформації, слід вважати, що зловмисник отримає інформацію про уразливість системи або мережі організації і планує використовувати ці дані при організації атаки на систему. Внаслідок цього організації буде завдано матеріальних збитків, а якщо отримані зловмисником дані будуть опубліковані, то буде завдано шкоди репутації організації.

2. Вибір захисних заходів

Захисні заходи з протидії інцидентів збору інформації. обрані на основі результатів оцінки ризиків, націлені на протидію реалізації виявлених загроз і зниження можливості використання вразливостей систем. Такими захисними заходами, наприклад, можуть бути:

- установка і настройка МСЕ;
- використання технології VPN (Virtual Private Network);
- установка СВВ і аналізаторів пакетів для відстеження специфічного трафіку;
- установка публічно доступних послуг в безпечних сегментах системи;
- виконання регулярної оцінки вразливостей, щоб ідентифікувати ризики і зменшити їх до прийнятного рівня;
- оперативне встановлення виправлень для програм і використовуваних операційних систем (patching).

Самі по собі інциденти збору інформації не повинні впливати на продуктивність системи, виявити їх важко. Заходами щодо виявлення інцидентів збору інформації можуть служити регулярні перевірки статистики МСЕ, СВВ, моніторинг стану інтерфейсів систем.

Зважаючи на високий рівень залишкового ризику, появи нових інструментів і засобів збору інформації обраних захисних заходів може бути недостатньо. Необхідна своєчасна і оперативна обробка інцидентів збору інформації, щоб попередити подальші злочинні дії по відношенню до системи.

На основі аналізу сценаріїв інциденту повинні бути визначені захисні заходи щодо стримування, усунення інциденту і відновленню після нього. Ці заходи вибираються і реалізуються персоналом з реагування на інциденти відповідно до сценарію розвитку інциденту.

До захисних заходів, стримуючим інцидент збору інформації. відносяться:

- аналіз переданого зловмисником трафіку;
- виявлення і ізолювання порушених вузлів і систем;
- реалізація фільтрації на основі аналізу трафіку.

Заходами щодо усунення інциденту збору інформації та відновленню після нього можуть бути:

- виявлення вразливостей систем, вузлів і сервісів;
- усунення виявлених вразливостей;
- маскування мети;
- зміна паролів у всіх системах, дані аутентифікації яких могли бути перехоплені.

3. Послідовність дій і порядок обробки інциденту

Для забезпечення ефективного реагування на інцидент в організації повинна бути сформована послідовність дій при обробці інцидентів збору інформації. Ця послідовність приводиться в табл. 2.16. Послідовність дій може змінюватися в залежності від особливостей інцидентів і стратегій щодо стримування інциденту, обраних конкретною організацією.

Таблиця 2.16 – Послідовній дій при обробці інциденту збору інформації

	Дія	**Завершено**
Аналіз інциденту		
1	Збір і документування додаткових свідчень (доказів) інциденту для визначення його реальності і значимості	
2	Визначення значущості інциденту з точки зору його впливу на бізнес	
2.1	Ідентифікація порушених активів і прогнозування, які активи можуть бути порушені	
2.2	Оцінювання існуючих і потенційних впливів інциденту	
2.3	Визначення по матриці значущості інцидентів умов реагування на основі технічного впливу і порушених активів	
3	Повідомлення про інцидент відповідному внутрішньому персоналу і зовнішнім організаціям	
Стримування, усунення інциденту і відновлення після інциденту		
4	Виконання початкового стримування інциденту (наприклад, блокування вхідного підозрілого трафіку)	
5	Отримання, документування, збереження і забезпечення безпеки свідоцтв (доказів) інциденту	
6	Необхідність упевнитися в стримуванні інциденту	
6.1	Аналіз інциденту і визначення, чи достатньо було стримування (включаючи перевірку інших систем на ознаки вторгнення)	
6.2	Реалізація додаткових заходів стримування при необхідності	
7	Усунення інциденту	
7.1	Ідентифікація та мінімізація всіх вразливостей, які були використані	
7.2	Видалення компонентів інциденту	
8	Відновлення після інциденту	
9	Підготовка до завершального звіту	
Діяльність після інциденту		

На підприємстві повинен бути визначений порядок обробки інцидентів збору інформації в залежності від їх значущості. Приблизна матриця визначення значущості інцидентів збору інформації наведена в таблиці 2.17. Заголовки стовпців показують різну ступінь критичності активів, а заголовки рядків - різні категорії технічного впливу. Рівень значущості інциденту

впровадження шкідливого коду в матриці визначає пріоритетність його обробки.

Таблиця 2.17 Примірна матриця визначення значимості інцидентів впровадження зловмисного коду

Існуючий вплив або ймовірний майбутній вплив інциденту	Критичність (важливість) активів, котрі зачеплені в даний час або які, цілком ймовірно, будуть порушені інцидентом		
	Висока (наприклад. Зв'язність з Internet. Web-сервери. робочі станції системних адміністраторів)	Середня (наприклад, сервери файлів, сервери друку, поштовий сервер)	Низька (наприклад, робочі станції користувачів)
Ідентифікація засобу отримання конфіденційної інформації	Значимість 1	Значимість 2	Значимість 3
Ідентифікація вразливостей системи	Значимість 1	Значимість 2	Значимість 3
Ідентифікація топології мережі	Значимість 2	Значимість 3	Значимість 4

4. Виявлення і аналіз інциденту

Виявлення і аналіз інцидентів збору інформації може відбуватися за допомогою різних передвісників і вказівників інциденту. В таблиці 2.18 перераховуються можливі передвісники інциденту збору інформації і надаються заходи, які можуть запобігти виникненню інциденту.

Таблиця 2.18 – Передвісники інциденту впровадження зловмисного коду

Передвісники	Дії по запобіганню
Підвищення інтересу до структури і діяльності організації, її окремих підрозділі або співробітників. Отримана інформація нетехнічного характеру може бути використана для визначення напрямків і інструментів атаки технічного збору інформації	Дана інформація може бути до душі, наприклад, обманним шляхом, під виглядом соціологічного опитування з проблем трудящих або забезпечення технічної безпеки і т.п. Запобігти витоку інформації про структуру та діяльність організації можна за допомогою введення режиму секретності оформлення підписок про нерозголошення і т.д. інформування співробітників про безпеку роботи в Інтернеті, з електронною поштою і про можливі види шахрайства в мережі
Нещодавно виготовлений інструмент збору інформації	Персонал з реагування на інциденти зобов'язаний стежити за появою нових інструментальних технічних засобів, які можуть бути використані для збору інформації: вивчення цих коштів, а також використання їх для виявлення вразливостей мереж і систем у своїй організації дозволить ідентифікувати захисні заходи для протидії новим загрозам
Публікація інформації про уразливість операційних систем і ПЗ	Крім регулярної установки оновлень і виправлень для програм і операційних систем від їх виробника, необхідно також стежити за інформацією, що з'явилася, наприклад, на інформаційних порталах в Інтернеті, в спеціалізованих друкованих виданнях або повідомленнях ЗМІ про погрози і інциденти кібербезпеки і вживати заходів з протидії їм

Вказівники інциденту – це ознаки небажаний подій, котрі можуть бути виявлені за допомогою:

- повідомлення мережевих і вузлових СВВ;
- перегляд статистики мережевого екрану;
- аналізаторів реакції мережевих інтерфейсів.

Вказівники інциденту збору інциденту збору інформації наведені в таблиці 2.19.

Таблиця 2.19 – Вказівники інциденту збору інформації

Можливі вказівники	Небажані події
Попередження СВВ про аномальний трафік в мережі	Сканування DNS-сервера. Відправка тестових запитів по випадковим мережевих адрес. Зондування мережі. Сканування доступних мережевих портів. Сканування одного або декількох сервісів з відомими уразливими по діапазону мережевих адрес
Повідомлення про виявлення вторгнень в мережу або до вузла	
Попередження ПЗ аналізаторів реакції мережевих інтерфейсів (наприклад, робота вузла у режимі прослуховування)	Пасивне прослуховування мережі (перехоплення трафіку)
Велика кількість пакетів від одного джерела, адресованих різним машинам в мережі	Сканування DNS-сервера. Відправка тестових запитів по випадковим мережевих адрес. Зондування мережі. Сканування доступних мережевих портів
Велика кількість пакетів, адресованих різним машинам в мережі і спрямованих на один і той же порт	Сканування DNS-сервера. Зондування мережі. Сканування одного або декількох сервісів з відомими уразливими по діапазону мережевих адрес.

Інциденти збору інформації самі по собі не завдають шкоди діяльності організації. Але часто збір інформації розширюється і переходить в інший інцидент, якщо, наприклад, порушник при виявленні уразливості намагається її використовувати.

Небажані події інциденту збору інформації можуть являти собою послідовність розвідувальних дій. Наприклад, запити DNS допомагають

з'ясувати, хто володіє тим чи іншим доменом і які адреси цього домену привласнені; відправка тестових запитів за отриманими адресами дозволяє виявити активні вузли в мережі; сканування доступних мережевих портів дозволяє ідентифікувати використовувані на вузлах мережеві служби і сервіси, версії програмного забезпечення цих сервісів; аналіз характеристик служб і сервісів дозволяє зловмисникові знайти уразливості системи і використовувати їх для проведення атаки. Важливо якомога раніше вжити заходів щодо стримування та усунення інциденту збору інформації, щоб знизити можливі збитки.

5. Стримування інциденту

Час реагування на інцидент є критичним при стримуванні інциденту збору інформації. Перш за все слід провести аналіз переданого на незнайомий адресу трафіку. Аналіз переданого трафіку дозволить встановити, яку інформацію міг отримати зловмисник, від якого вузла або системи, а також, можливо, адреса одержувача цієї інформації. Ці дані допоможуть виявити порушені системи і вузли, а також провести розслідування інциденту збору інформації. Аналіз переданого зловмисником трафіку дозволить побудувати можливу картину майбутньої атаки на систему і перешкоджати їй. За результатами аналізу трафіку можна зробити наступні заходи щодо стримування:

- ізолювання порушених вузлів або служб на вузлі. Якщо, наприклад, при пасивному прослуховуванні мережі зловмисник перехопив пакети, в яких передаються паролі, то необхідно терміново виявити системи, вузли та послуги, яким вони належать. Процедура відключення вузла від мережі або відключення порушеної послуги, поки обробники інциденту визначають, чи був скомпрометований файл паролів, має перешкоджати атакуючому використовувати ці паролі. У більшості середовищ, проте, це не так. Через довірених відносин між системами і користувачами, що забезпечують одні й ті ж або паролі для багатьох систем, вкрадені паролі часто використовуються для

доступу до інших систем. Інцидент може швидко розширитися від одного вузла до багатьох вузлів за хвилини;

- реалізація фільтрації на основі аналізу трафіку. Блокування певного виду пакетів має сприяти перериванню розвідувальної діяльності зловмисника. Необхідно налаштувати мережевий екран або маршрутизатор таким чином, щоб він не пропускав певні пакети. Хоча прийоми фільтрації можуть бути ефективні при стримуванні інцидентів, вони можуть вносити додаткові проблеми. Наприклад, додавання нових правил до маршрутизатора або міжмережевого екрану може викликати суттєве зниження пропускної здатності мережі.

6. Усунення і відновлення інциденту

В першу чергу персонал з реагування на інциденти повинен ідентифікувати уразливості систем, вузлів або служб на вузлах, про які міг отримати інформацію зловмисник. Заходи щодо усунення інциденту збору інформації повинні бути спрямовані на запобігання майбутніх атак на ці системи. Тому важливо для обробників ідентифікувати всі уразливості і вжити заходів щодо їх зменшення або усунення.

Якщо аналіз переданого зловмисникові трафіку показав, що метою атаки був конкретний вузол, то має сенс виконати «маскування мети», тобто привласнення цього вузла іншої адреси IP. Якщо метою була конкретна послуга вузла, то послуга може бути передана іншому вузлу - вузлу без відповідної уразливості.

Рекомендується зміна всіх паролів у всіх системах, дані аутентифікації яких могли бути перехоплені.

7. Збір і обробка свідоцтв інциденту

При зборі і обробці свідчень (доказів) інциденту збору інформації та підготовки звіту необхідно зафіксувати відносяться до цього інциденту дані, що включають попередження про виявлення вторгнення, журнали мережевого екрану. повідомлення аналізаторів стану мережевих інтерфейсів. Ці дані також

можуть бути основою для розслідування інциденту збору інформації і подальшої перевірки ефективності процедур його обробки.

ВІДМОВА В ОБСУГОВУВАННІ

1. Підготовка до обробки інциденту

При підготовці до обробки інциденту необхідно побудувати можливі сценарії відомих інцидентів відмови в обслуговуванні.

Сценарії розвитку інциденту будуються на основі критичних подій, які призводять до інциденту, і попередніх їм небажаних подій. У табл. 2.20 наведені критичні події і небажані події інциденту відмови в обслуговуванні що передували їм.

Таблиця 2.20 – Небажані події інциденту відмови в обслуговуванні

Критична дія	Небажана подія
Відмова в обслуговуванні конкретного вузла	Недоступність вузла. Втрата з'єднання з вузлом.
Відмова в обслуговуванні мережі	Недоступність мережі. Втрата з'єднання з конкретною мережею
Відмова в обслуговуванні операційної системи вузла	Недоступність операційної системи вузла. Втрата з'єднання з операційною системою вузла
Відмова в обслуговуванні ПЗ на вузлі	Недоступність ПЗ на вузлі. Втрата з'єднання з ПЗ на вузлі

Інцидент відмови в обслуговуванні може привести до переривання одного або декількох бізнес-процесів і втрати даних, що в свою чергу викличе втрату продуктивності, матеріальні збитки і збитки репутації.

2.Вибір захисних заходів

Захисні заходи для запобігання відмови в обслуговуванні сервісів, систем, вузлів або мереж, обрані на основі результатів оцінки ризиків, націлені на протидію реалізації виявлених загроз і зниження можливості використання вразливостей для проведення атак. Такими захисними заходами, наприклад, можуть бути:

- конфігурація периметра мережі так. щоб заборонити весь вхідний і вихідний трафік, який не вирішено. Це повинно включати:

1) блокування використання послуг, таких як відлуння і завантаження, які більше не служать встановленої мети і використовуються при атаках DoS;

2) виконання фільтрації виходу і входу, щоб блокувати помилкові пакети;

3) формування правил брандмауера і управління доступом до маршрутизатора, що дозволяють ефективно блокувати небезпечний трафік;

4) конфігурація прикордонних маршрутизаторів таким чином, щоб блокувалася ретрансляція спрямованих широкомовних розсилок;

- обмеження швидкості для певних протоколів, щоб вони могли використовувати тільки певну частину загальної пропускної здатності. Обмеження швидкості може бути реалізовано на прикордонних маршрутизаторах і міжмережевих екранах;
- блокування всіх непотрібних послуг і обмеження використання послуг, які можуть бути використані при атаках DoS, на вузлах. мають доступ в Internet;
- забезпечення впевненості, що мережі і системи не працюють на максимальній пропускній здатності. В іншому випадку це полегшить атаку DoS.

Крім того, за результатами оцінки ризиків можуть бути обрані захисні заходи, що дозволяють виявляти трафік DoS і DDoS. До таких захисних заходів, наприклад, можуть ставитися мережеві і вузлові СВВ і екрани.

Для виявлення небажаних подій інциденту відмови в обслуговуванні може бути використаний моніторинг активів системи. За допомогою нього можна, наприклад, виявити значне відхилення від нормальної поведінки систем, визначити джерело використання мережевої пропускної здатності і критичних активів.

Однак зважаючи на високий рівень залишкового ризику, появи нових загроз і вразливостей обраних захисних заходів може бути недостатньо. і

інциденти кібербезпеки відбуватимуться. Необхідна своєчасна і оперативна обробка інциденту відмови в обслуговуванні. щоб знизити можливі збитки від нього.

На основі аналізу сценаріїв інциденту повинні бути визначені захисні заходи щодо стримування, усунення інциденту і відновленню після нього. Ці заходи вибираються і реалізуються персоналом з реагування на інциденти.

До захисних заходів, стримуючим інцидент відмови в обслуговуванні, відносяться:

- блокування трафіку від джерела активності;
- реалізація фільтрації на основі характеристик атаки.

Заходами щодо усунення інциденту відмови в обслуговуванні можуть бути, наприклад:

- привласнення атакованому вузлу іншої адреси IP (маскування мети);
- дистанційне блокування атакуючих агентів DDoS.

Як заходи по відновленню після інциденту відмови в обслуговуванні можуть бути такі:

- ідентифікація всіх вразливостей, які були використані, і визначення стратегії для їх зменшення;
- відновлення працездатності пошкоджених апаратних і програмних засобів.

3. Послідовність дій і порядок обробки інциденту

Для забезпечення ефективного реагування на інцидент в організації повинна бути сформована послідовність дій при обробці інцидентів відмови в обслуговуванні. Цей перелік наводиться в табл. 2.21. Послідовність дій може змінюватися в залежності від особливостей інцидентів і стратегій щодо стримування інциденту, обраних конкретною організацією.

Таблиця 2.21 – Послідовній дій при обробці інциденту відмови в обслуговуванні

	Дія	**Завершено**
	Аналіз інциденту	
1	Збір і документування додаткових свідчень (доказів) інциденту для визначення його реальності і значимості	
2	Визначення значущості інциденту з точки зору його впливу на бізнес	
2.1	Ідентифікація порушених активів і прогнозування, які активи можуть бути порушені	
2.2	Оцінювання існуючих і потенційних впливів інциденту	
2.3	Визначення по матриці значущості інцидентів умов реагування на основі технічного впливу і порушених активів	
3	Повідомлення про інцидент відповідному внутрішньому персоналу і зовнішнім організаціям	
	Стримування, усунення інциденту і відновлення після інциденту	
4	Виконання початкового стримування інциденту (наприклад, фільтрація трафіку, відключення послуг і т.д.).	
5	Отримання, документування, збереження і забезпечення безпеки свідоцтв (доказів) інциденту	
6	Усунення інциденту (ідентифікація та мінімізація всіх вразливостей, які були використані)	
7	Відновлення після інциденту	
7.1	Відновлення порушених інцидентом систем до робочого стану	
7.2	Перевірка функціонування зачеплених систем	
7.3	Підготовка завершального звіту	
	Діяльність після інциденту	

На підприємстві повинен бути визначений порядок обробки інцидентів відмови в обслуговуванні в залежності від їх значимості. Орієнтовна матриця визначення значущості інцидентів відмови в обслуговуванні показана в табл. 2.22.

Таблиця 2.22 Примірна матриця визначення значимості інцидентів відмови в обслуговуванні

Існуючий вплив або ймовірний майбутній вплив інциденту	Критичність (важливість) активів, котрі зачеплені в даний час або які, цілком ймовірно, будуть порушені інцидентом		
	Висока (наприклад. Зв'язність з Internet. Web-сервери. робочі станції системних адміністраторів)	Середня (наприклад, сервери файлів, сервери друку, поштовий сервер)	Низька (наприклад, робочі станції користувачів)
Відмова в обслуговуванні	Значимість 1	Значимість 2	Значимість 3
Відмова в обслуговуванні на рівні користувача	Значимість 2	Значимість 4	Значимість 5

Заголовки стовпців показують різну ступінь критичності ресурсів, а заголовки рядків - різні категорії технічного впливу. Рівень значущості інциденту в матриці визначає пріоритетність його обробки.

4. Виявлення і аналіз інциденту

Виявлення та аналіз інцидентів відмови в обслуговуванні може відбуватися за допомогою різних провісників і покажчиків. У табл. 2.23 перераховуються можливі передвісники атак DoS і наводяться дії, які можуть запобігти появі інциденту. В таблиці 2.24 надані небажані події інциденту відмови в обслуговуванні і для кожної такої події перелічуються можливі вказівники.

Таблиця 2.23 – Передвісники інциденту відмови в обслуговуванні і дії по їх запобіганню

Передвісники	Дії по запобіганню
Атакам DoS часто передує розвідувальна діяльність, щоб визначити, які атаки можуть бути ефективними, наприклад, визначення обсягу трафіку, небезпечного для даної системи	Якщо буде виявлено активність, яка здається підготовкою для атаки DoS, організація може блокувати атаку за допомогою швидкої зміни її безпеки, наприклад, зміна правил мережевого екрану, щоб блокувати конкретний протокол або захистити вразливий вузол
Нещодавно виготовлений інструмент DoS може уявити значну загрозу для організації	Необхідно розслідувати новий інструмент і. якщо можна, змінити засоби управління безпекою так. щоб цей інструмент став неефективним при реалізації атак DoS на системи організації

Таблиця 2.24 – Вказівники відмови в обслуговуванні

Можливі вказівники	Небажані події
Повідомлення користувача про недоступність системи, мережі або додатки	Недоступність вузла. Втрата з'єднання з вузлом. Недоступність мережі. Втрата з'єднання з конкретною мережею. Недоступність операційної системи вузла. Втрата з'єднання з операційною системою вузла. Недоступність додатки на вузлі. Втрата з'єднання з додатком на вузлі
Незрозумілі втрати з'єднання	Недоступність вузла. Втрата з'єднання з вузлом. Недоступність мережі. Втрата з'єднання з конкретною мережею
Попередження про виявлення вторгнення в мережу	Недоступність вузла. Втрата з'єднання з вузлом. Недоступність мережі. Втрата з'єднання з конкретною мережею. Недоступність операційної системи вузла. Втрата з'єднання з операційною системою вузла. Недоступність додатки на вузлі. Втрата з'єднання з додатком на вузлі
Зростання використання мережевої пропускної здатності	Недоступність вузла. Втрата з'єднання з вузлом. Недоступність мережі. Втрата з'єднання з конкретною мережею
Велике число з'єднань до одного вузла	Недоступність вузла. Втрата з'єднання з вузлом. Недоступність операційної системи вузла. Втрата з'єднання з операційною системою вузла

Продовження таблиці 2.24 – Вказівники відмови в обслуговуванні

Можливі вказівники	Небажані події
Асиметрична картина мережевого трафіку (великий обсяг трафіку, що йде до вузла. Невеликий трафік, що виходить з вузла)	Недоступність вузла. Втрата з'єднання з вузлом. Недоступність мережі. Втрата з'єднання з конкретною мережею. Недоступність операційної системи вузла. Втрата з'єднання з операційною системою вузла
Записи журналу мережевого екрану і маршрутизатора	Недоступність вузла. Втрата з'єднання з вузлом. Недоступність мережі. Втрата з'єднання з конкретною мережею
Пакети з незвичайними адресами джерел	Недоступність вузла. Втрата з'єднання з вузлом. Недоступність мережі. Втрата з'єднання з конкретною мережею. Недоступність операційної системи вузла. Втрата з'єднання з операційною системою вузла. Недоступність додатки на вузлі. Втрата з'єднання з додатком на вузлі
Пакети з неіснуючими адресами призначення	Недоступність мережі. Втрата з'єднання з конкретною мережею
Записи журналу операційної системи	Недоступність операційної системи вузла. Втрата з'єднання з операційною системою вузла
Записи журналу ПЗ	Недоступність додатки на вузлі. Втрата з'єднання з додатком на вузлі

Атаки DoS створюють такі проблеми при аналізі інцидентів:

- атаки DoS часто використовують протоколи, неорієнтовані на з'єднання (UDP і ICMP), або протокол, орієнтований на з'єднання таким способом, щоб не встановлювати повні з'єднання (наприклад, передача пакетів TCP SYN, щоб створити атаку затоплення сигналами). Таким чином, для атакуючих відносно легко використовувати вигадані адреси IP джерела, створюючи труднощі у відстеженні джерела атак. Є ефективним перегляд журналів попередньої розвідувальної активності. Через те, що атакуючий повинен отримати результати розвідки, така активність малоймовірна з

використанням неправдивих адрес, так що вона може вказувати місце розташування атакуючого;

- атаки DoS часто використовують сотні або тисячі робочих станцій, які управляються (контролюються) одним (або. Взагалі, ніяким) оброблювачем. Жертва не бачитиме IP обробника і, навіть якби це було можливо, то це був би. ймовірно, вузол, який скомпрометував атакуючий;
- коли відбувається вихід з ладу активів, часто можна не зрозуміти. що це викликано атакою DoS. Наприклад, сервер може випадково вийти з ладу як результат нестабільності операційної системи, що вимагає повторного завантаження для відновлення її функціонування. Якщо атакуючий посилає спеціальні пакети до сервера, які викликають його вихід з ладу, то системні адміністратори можуть припустити, що вихід з ладу відбувся через нестабільність операційної системи, і не усвідомити, що мала місце атака.

5. Стримування і усунення інциденту та відновлення

Стримування, усунення інциденту відмови в обслуговуванні зазвичай складається у протидії небезпечному трафіку. Часто це протидія полягає в блокуванні всього трафіку від джерела активності. Однак такі атаки мають помилкові адреси джерела або використовують сотні або тисячі скомпрометованих вузлів, що робить важким або неможливим реалізацію ефективної фільтрації, заснованої на адресах I. Навіть якщо підприємство може блокувати адреси джерел, які використовуються, атакуючий може перейти до інших адресами IP. Дії щодо стримування, усунення інциденту відмови в обслуговуванні, а також відновленню після інциденту відмови в обслуговуванні такі:

- зменшення вразливостей, які використовуються. Наприклад, якщо атака може статися через те, що MCE не блокують пакети, що використовують порт 7 UDP (відлуння) і публічно доступний вузол виконує послугу відлуння, то MCE повинні бути скориговані, щоб блокувати пакети, призначені для порту відлуння; і конфігурація вузла повинна бути так змінена, щоб він більше не пропонував послугу відлуння. Якщо операційна система вузла не стійка до атак

DoS, то вона повинна бути скоригована. Цей вузол, можливо, треба буде від'єднати від мережі, щоб зупинити атаку DoS, поки коригується операційна система вузла;

- реалізація фільтрації на основі характеристик атаки. Наприклад, якщо атака використовує запити відлуння ICMP, то можна тимчасово блокувати такі запити від входу в мережу. На жаль, це не завжди практично: якщо атакуючий посилає потік пакетів SYN до порту протоколу гіпертекстової передачі (HTTP) Web-сервера, то блокування пакетів SYN, призначених для цього порту, буде саме викликати відмову в обслуговуванні для користувачів. Інша стратегія полягає в обмеженні швидкості, дозволяючи лише кілька пакетів в секунду для використання специфічного протоколу чи контакту з певним вузлом. Хоча прийоми фільтрації можуть бути ефективні при стримуючи-ШП1 інцидентів, вони можуть вносити додаткові проблеми. Наприклад, додавання нових правил до маршрутизатора або міжмережевий екран може мати суттєвий негативний вплив на роботу пристроїв, викликаючи зниження пропускної здатності мережі;
- маскування мети. Якщо метою є конкретний вузол і інші стратегії стримування не працюють, то вузлу може бути присвоєний іншій адресу IP. Якщо метою є конкретна послуга вузла, то послуга може бути передана іншому узлу7 - вузлу без відповідної уразливості
- атака атакуючих. Наприклад, адміністратори можуть використовувати програми, які дозволяють дистанційно блокувати атакуючих агентів DDoS, або вони (програми) можуть модифікувати конфігурацію мережі або сервера, щоб перенаправити небезпечний трафік назад до джерела атаки. Однак якщо адреса джерела помилковий або адреса джерела законний, але знаходиться в спільному володінні, то ці прийоми можуть ненавмисно атакувати невинну сторону. Такі прийоми hack back (хакерство назад) повинні використовуватися дуже обережно.

6. Збір і обробка свідоцтв інциденту

Збір та обробка свідоцтв (доказів) інциденту відмови в обслуговуванні часто є проблемним і витратною справою за часом з-за наступних причин:

- складність ідентифікації джерела атак з спостережуваного трафіку. Адреси джерела IP часто модифіковані. Атаки DDoS можуть? використовувати сотні і тисячі вузлів, кожен з яких може використовувати безліч помилкових адрес;
- складність вивчення того, як були скомпрометовані атакуючі вузли. При атаках DDoS вузли агентів можуть бути скомпрометовані. Атакуючий може навіть не бути відповідальним за компрометацію; атакуючий просто використовує вузли, які раніше були скомпрометовані іншими;
- складність перегляду великого числа записів журналу моніторингу. Більшість атак DoS генерує великий трафік і при моніторингу систем в журналах фіксується велика кількість записів. Для огляду записів і виділення корисної інформації потрібно багато часу.

2.6 Висновки до другого розділу

В другому розділі проаналізовані вимоги, які повинні бути впроваджені на підприємстві стосовно управління інцидентами кібербезпеки, як важливої складової загальної стратегії забезпечення інформаційної безпеки.

Був детально розкритий зміст процесів системи управління інцидентами. сформована політика управління інцидентами задля зниження негативного впливу на бізнес та мінімізації виникнення інцидентів кібербезпеки.

Детально були наведені рекомендаційні вказівки стосовно раціонального та ефективного управління інцидентами кібербезпеки для рядових співробітників і керівництва підприємства, а саме рекомендації щодо планування системи управління інцидентами, застосування системи управління інцидентами, аналіз обробки інцидентів, покращення системи управління інцидентами. На прикладі малого комерційного підприємства були надані

рекомендаційні вказівки стосовно процесів управління інцидентами кібербезпеки. а саме:

- підготовка до обробки інциденту;
- вибір захисних заходів;
- послідовність дій і порядок обробки інциденту;
- виявлення і аналіз інциденту;
- стримування і усунення інциденту;
- відновлення після інциденту;
- збір і обробка свідоцтв інциденту;

РОЗДІЛ 3
ЕКОНОМІЧНА ЧАСТИНА

3.1 Вступ

Мета економічного розділу – розрахунок економічної ефективності застосування рекомендованих методик та розроблених інструкцій щодо управління інцидентами кібербезпеки для рядових співробітників та керівництва малих комерційних підприємств.

Для визначення ефективності необхідно розрахувати:

1) вартість розробки, впровадження та підтримки рекомендаційних методик та інструкцій;

2) різницю втрат заданих інцидентами кібербезпеки на підприємстві до впровадження рекомендаційних методик та інструкцій, та після їх впровадження;

3) економічну доцільність впровадження та підтримки рекомендаційних методик та інструкцій на підприємстві.

3.2 Загальні відомості про підприємство

Приватне підприємство «H2O», діяльність якого полягає у продажу питної води, розташовується на першому поверсі житлового 9-поверхового будинку. Об’єктом інформаційної діяльності виступає вся територія приміщення, де циркулює інформація з обмеженим доступом. Офісна будівля підприємства розташовується за адресою м. Дніпро, вул. Кірова , буд. 26. Кількісний склад працівників – 9 чоловіків.

До активів підприємства відносяться:

- транспортний засіб Mercedes Vito 2006, вартість якого складає 190 000 грн.;
- транспортний засіб Volkswagen Transporter 2007, вартість якого складає 210 000 грн.;

- транспортний засіб Volkswagen Transporter 2005, вартість якого складає 180 000 грн.;
- персональні комп'ютери співробітників, вартість яких складає 69300 грн.;
- програмне забезпечення, вартість якого складає 31760 грн.;
- офісні меблі, вартість яких складає 8980 грн.;

3.3 Вартість розробки, впровадження та підтримки рекомендованих методик

Витрати на створення рекомендованих методик $К_і$ складаються з витрат на заробітну плату виконавця рекомендованих методик і інструкцій $З_{зп}$ і вартості машинного часу, необхідного для опрацювання методик і інструкцій $З_{мч}$:

$$К_і = З_{зп} + З_{мч} \quad (3.1)$$

Заробітня платня рахується за формулою:

$$З_{зп} = t \cdot З_{пр} \text{ грн.}, \quad (3.2)$$

де t – загальна тривалість створення методик, годин;

$З_{пр}$ – середньо годинна заробітна плата спеціалісту з кібербезпеки з нарахуваннями, грн./годину.

$$З_{зп} = 480*34,375 = 16500 \text{ грн.}$$

Для розрахунку машинного часу ми візьмемо середню потужність ПК, яка складає 0,5 кВт і вартість електроенергії для приватних підприємств 1,67 грн.

$$З_{мч} = 0,5*1,67 = 0,835 \text{ грн.}$$

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t \cdot C_e + \frac{Ф_{перв} \cdot H_a}{F_p} + \frac{K_{лпз} \cdot H_{апз}}{F_p}, \text{ грн./год.,} \qquad (3.3)$$

де P – встановлена потужність ПК, кВт;

C_e – тариф на електричну енергію, грн./кВт·година;

$Ф_{перв}$– первісна вартість ПК на початок року, грн.;

H_a – річна норма амортизації на ПК, частки одиниці;

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$K_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

F_p – річний фонд робочого часу (за 40-годинного робочого тижня F_p = 1920 год.).

$$C_{мч} = 1,2 \cdot 1 \cdot 1.67_e + \frac{9500 \cdot 0.25}{1920} + \frac{2000 \cdot 0,25}{1920} = 3,5 \text{ грн./год.}$$

Витрати на створення рекомендованих методик складають:

$$K_i = 480 * (3,5 + 34,375) = 18180 \text{ грн.}$$

Капітальні витрати розраховуються за формулою:

$$К_{заг} = К_І + К_А + К_К + К_Б + К_Ф + К_П \quad (3.4)$$

де $К_І$ – витрати на одноразову розробку інструкцій;

$К_А$ – витрати на підписку на антивірус для комп'ютерів працівників;

$К_К$ – витрати на налаштування розмеження доступу до інформації;

$К_Б$ – налаштування джерела безперебійного живлення;

$К_Ф$ – витрати на розробку форми звітності про інцидент кібербезпеки;

$К_П$ – витрати на програмне забезпечення для зберігання паролів внутрішнього користування;

$$К_{заг} = 18180 + 3600 + 2500 + 2700 + 900 + 3500 = 31380 \text{ грн.}$$

Поточні витрати розраховуються за формулою:

$$С_{заг} = (С_І/3) + С_С + С_{САВ} + С_{ЗА} + С_{ЗС} + С_{БД} \quad (3.5)$$

де $С_І$ – витрати на щоквартальний інструктаж стосовно інцидентів кібербезпеки;

$С_С$ – витрати на щомісячне забезпечення хмарного серверу резервного копіювання;

$С_{САВ}$ – витрати на щомісячну підписку на серверний антивірус;

$С_{ЗА}$ – витрати на щомісячні послуги спеціаліста з кібербезпеки;

$С_{ЗС}$ – витрати на додаткову щомісячну заробітню платню діючому співробітнику, який відповідає за сповіщення та реєстрування інцидентів;

$С_{БД}$ – витрати на щомісячне резервне копіювання баз даних з журналом інцидентів кібербезпеки

$$С_{заг} = (1980/3) + 650 + 540 + 1900 + 1500 + 800 = 6050 \text{ грн.} \quad (3.6)$$

Підсумував одноразові та поточні витрати, вартість розробки, впровадження та річна підтримка систем управління інцидентами кібербезпеки, згідно з рекомендаціями і інструкціями, буде коштувати 82380 грн./рік:

$$В_{заг} = 31380 + 6050 * 12 = 103980 \text{ грн./рік.}$$

3.4. Величина можливого збитку від інцидентів кібербезпеки

Для того, щоб підрахувати величини можливого збитку від інцидентів кібербезпеки, необхідні наступні вихідні дані:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин; даний показник складає приблизно $t_п = 4$ години

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин; даний показник складає приблизно $t_п = 4$ години

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин; $t_{ви} = 16$ годин.

$З_о$ – місячна заробітна плата системного адміністратора, вона складає 4000 грн. на місяць;

$З_с$ – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, вона складає 4000 грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб. $Ч_о = 1$ особа;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.; $Ч_с = 7$ осіб.

О – обсяг чистого прибутку/дохід від реалізації атакованого вузла або сегмента корпоративної мережі, грн. у рік, або оподаткований прибуток атакованого вузла або сегмента корпоративної мережі, складає 820000 грн.;

$П_{зч}$ – вартість заміни встаткування або запасних частин складає 0 грн., тому що ми використовуємо існуюче устаткування;

I – число атакованих вузлів або сегментів корпоративної мережі, I = 5;

N – середнє число можливих атак на рік, N = 12.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_{п} + П_{в} + V, \tag{3.7}$$

де $П_{п}$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн.;

$П_{в}$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн.;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_{п} = \frac{\sum З_{с} * Ч_{с}}{F} \cdot t_{п} \ , \tag{3.8}$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 160-176 ч).

$$П_{п} = \frac{\sum 4000 * 7}{160} \cdot 4 = 700 \text{ грн.}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \quad (3.9)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн.;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с * Ч_с}{F} \cdot t_{ви} \quad (3.10)$$

$$П_{ви} = \frac{4000 * 7}{160} \cdot 16 = 2800 \text{ грн.}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати адміністратору:

$$П_{пв} = \frac{\sum З_о * Ч_о}{F} \cdot t_в \ . \quad (3.11)$$

$$П_{пв} = \frac{4000 \cdot 1}{160} \cdot 4 \ = 100 \text{ грн.}$$

$$П_в = 2800 + 100 + 0 = 2900 \text{ грн.}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви}) , \quad (3.12)$$

.

$$V = 820000 / 1920 * (4 + 4 + 16) = 10250 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день).

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = 700 + 2900 + 10250 = 13850 \text{ грн.}$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе

$$B = \sum\sum U*N*I . \quad (3.13)$$

$$B = 13850 * 12 * 5 = 831000 \text{ грн.}$$

3.5 Економічна доцільність впровадження та підтримки рекомендаційних методик та інструкцій на підприємстві

Економічна доцільність, з урахуванням ризиків порушення інформаційної безпеки та кібербезпеки і визначається за формулою:

$$E = B - B_{заг} \quad (3.14)$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис.грн;

$B_{заг}$ – річна підтримка систем управління інцидентами кібербезпеки, згідно з рекомендаціями і інструкціями.

$$E = 831000 - 103980 = 727020 > 0$$

Після того як ми визначили загальний ефекти від впровадження системи, слід визначити термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки, це може бути розраховано за формулою 3.15

$$T_o = \frac{Взаг}{E}, \text{ років} \quad (3.15)$$

$$T = 103980/727020 = 0{,}143 \text{ року}$$

$$T \approx 2 \text{ місяці.}$$

3.6 Висновки до третього розділу.

В результаті прорахованих витрат на впровадження рекомендаційних методик та інструкцій щодо управління інцидентами кібербезпеки та можливих збитків від виникнення інцидентів, було доведено, що впровадження інструкцій та методик на підприємстві окупиться за 2 місяці

ВИСНОВКИ

Будь яка інформація, яка має цінність, підпадає до сфери інтересів зловмисників. Питання запобігання появи небажаних або несподіваних подій ІБ, інцидентів, з якими пов'язана значна вірогідність компрометації бізнес-операцій та створення загроз ІБ, актуальне як ніколи раніше. Дана робота дозволить сформувати загальні представлення про процес управління інцидентами кібербезпеки.

В ході виконання поставлених в дипломній роботі задач були отримані наступні наукові та практичні результати:

– за результатами дипломної роботи була обґрунтована актуальність процесу управління інцидентами, яка підтверджується статистикою. Надані загальні вимоги системи управління інцидентами інформаційної безпеки, їх схематична послідовність та описання процесів;

– була розроблена обґрунтована рекомендаційна база для рядових співробітників і керівників малих комерційних підприємств, що містить в собі всі етапи процесу управління інцидентами кібербезпеки:

- планування системи управління інцидентами кібербезпеки;
- застосування системи управління інцидентами кібербезпеки;
- аналіз обробки інцидентів кібербезпеки;
- покращення системи управління інцидентами кібербезпеки.

На прикладі підприємства були надані рекомендаційні вказівки стосовно процесів управління інцидентами кібербезпеки. а саме:

- підготовка до обробки інциденту;
- вибір захисних заходів;
- послідовність дій і порядок обробки інциденту;
- виявлення і аналіз інциденту;
- стримування і усунення інциденту;
- відновлення після інциденту;
- збір і обробка свідоцтв інциденту.

В економічній частині було проведено розрахунок витрат на впровадження рекомендаційних методик та інструкцій щодо управління інцидентами кібербезпеки та можливих збитків від виникнення інцидентів,

було доведено, що впровадження інструкцій та методик на підприємстві окупиться за 2 місяці

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Господарський кодекс України [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/go/436-15.
2. Про підприємства в Україні [Електронний ресурс] : Закон України від 01.01.2004 № 19-20 – Режим доступу: http://zakon5.rada.gov.ua/laws/show/887-12.
3. Про інформацію [Електронний ресурс] : Закон України від 01.01.2017 № 2657-12 – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12.
4. Про Національну програму інформатизації [Електронний ресурс] : Закон України від 01.08.2016 №74/98-вр – Режим доступу: http://zakon5.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.
5. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки [Електронний ресурс] : Закон України від 09.01.2007 №573-16 – Режим доступу: http://zakon3.rada.gov.ua/laws/show/537-16.
6. Про телекомунікації [Електронний ресурс] : Закон України від 18.12.2017 №1280-15 – Режим доступу: http://zakon5.rada.gov.ua/laws/show/1280-15.
7. Класифікація загроз Digital Security [Електронний ресурс] – Режим доступу: http://www.infosecurity.ru/_eshop/detail/dsec_grif_ct.html.
8. Gpo основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України від 05.10.2017 №2163-19 – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2163-19.
9. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу» [Електронний ресурс] – Режим доступу: http://iszzi.kpi.ua/images/Info_bezpeka/ND_TZI/4.
10. Звіт Cisco з інформаційної безпеки на початок 2017 року [Електроний ресурс] – Режим доступу: https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2017_mcr_071817_fnl_hq.pdf?oid=rptsc001643.

11. Звіт компанії InfoWatch з інформаційної безпеки на початок 2017 року [Електронний ресурс] – Режим доступу: https://www.infowatch.ru/.

12. Інформаційно-аналітичний центр Cyence [Електронний ресурс] – Режим доступу: https://www.crunchbase.com/organization/cyence.

13. Аналітично-статистичний центр компанії Avast [Електронний ресурс] – Режим доступу: https://www.avast.ru/.

14. Інформаційний центр компанії Microsoft Global Security Intelligence Report [Електронний ресурс] – Режим доступу: https://www.microsoft.com/en-us/security/Intelligence-report.

15. Статистичні дані, щодо видів інцидентів: – Режим доступу: U.S. Department of Justice, Federal Bureau of Investigation Internet Crime Report 2015.

16. Securing Cyberspace for the 44th Presidency / James A. Lewis // Center for Strategic and International Studies [Електронний ресурс] – Режим доступу: http://csis.org/files/media/csis/pubs/081208_ securingcyberspace_44.pdf.

17. Про Стратегію національної безпеки України : указ Президента України від 12.02.2007 р. № 105/2007 (із змінами від 8.06.2012 р. № 389/2012) [Електронний ресурс]. – Режим доступу: http:// zakon4.rada.gov.ua/laws/show/105/2007.

18. Концепція створення та забезпечення функціонування інфраструктури захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах. [Електронний ресурс] – Режим доступу:http://www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid= 6D68FCE54A40938081139F546DD E47B?art_id=38814&cat_id=38712.

19. Міжнародний стандарт ISO/IEC 27005:2011 «Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56742.

20. Будник М. М. ,Тимофєєв Д. С. Внутрішні загрози інформаційної безпеки та заходи по їх мінімізації [Електронний ресурс] – Режим доступу: http://ir.nmu.org.ua/bitstream/handle/123456789/1666/7.pdf?sequence=1.

21. Міжнародний стандарт ISO/IEC 27035:2011 «Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент інцидентів інформаційної безпеки» [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/44379.html.

22. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. – 2012. – № 2. – С. 162-169.

23. Про Доктрину інформаційної безпеки України : указ Президента України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/514/2009.

24. Міжнародний стандарт ISO/IEC 27001:2013 «Система управління інформаційною безпекою. Вимоги» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56742.

25. 12 ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення. [Електронний ресурс]. – Режим доступу: http://online.budstandart.com/ru/catalog/doc-page?id_doc=61937.

26. Дубов Д. В. Кібербезпека : світові тенденції та виклики для України / Д. В. Дубов, М. А. Ожеван. – К. : НІСД, 2011. – 30 с.

27. Гладиш С.В., Кононович В.Г., Тардаскін М.Ф. Порівняльний аналіз стандартів ISO/IEC та української нормативної бази в частині керування інцидентами інформаційної безпеки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2013. — № 15. — С. 31–39;

28. Система менеджменту інформаційної безпеки [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Система_управління_ІБ

29. Дорофєєв А.В., Марков А.С. Менеджмент інформаційної безпеки. Основні концепції [Електронний ресурс] – Режим доступу: http://cyberrus.com/wp-content/uploads/2014/03/67-73.pdf

30. Суспільна організація «Асоціація керівників служб інформаційної безпеки». Інциденти інформаційної безпеки, рекомендації з реагування [Електронний ресурс] – Режим доступу: http://expo-itsecurity.ru/upload/iblock/215/recommendations_SMALL_FIN_3.pdf

31. Національна стратегія кібербезпеки (NCSS). Від розуміння до можливості..– Holland, Den Haag: National Coordinator for Security and Counterterrorism, 2013. – Режим доступу: //www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.

Твердохліб І.С., студент групи 125м-16

Науковий керівник: Ковальова Ю.В.

(Державний ВНЗ «Національний гірничий університет»,

м. Дніпропетровськ, Україна)

УПРАВЛІННЯ ІНЦИДЕНТАМИ КІБЕРБЕЗПЕКИ НА МАЛИХ КОМЕРЦІЙНИХ ПІДПРИЄМСТВАХ

Питання забезпечення інформаційної безпеки на малих комерційних підприємствах актуальне в наш час, як ніколи раніше. Відповідно, і питання запобігання появи небажаних або несподіваних подій ІБ, інцидентів, з якими пов'язана значна вірогідність компрометації бізнес-операцій та створення загроз ІБ, теж актуальні. А виходячи з того, що значна частина існуючих організацій та підприємств складають малі приватні підприємства, даний питання стає особливо гострим і важливим, якому необхідно приділити належну увагу.

Малі комерційні підприємства є невід'ємною частиною соціально-економічної країни. По-перше, вони сприяють підтримці стабільності ринкових відносин, оскільки значна частина населення втягується в цю систему відносин

По-друге, вони забезпечують необхідну мобільність виробництва в умовах ринку, поглиблення спеціалізації та широке розвиток кооперації виробництва, без яких немислима його висока ефективність. В підсумку це веде до динамічності господарського розвитку та зростання національній економіки.

По-третє, роль малих підприємств у діяльності крупних та середніх підприємств постійно зростає. Велика значення має здатність малих підприємств розширювати сфери доповнення трудової діяльності, створювати нові можливості не тільки для працевлаштування, а перш за все для підприємницької діяльності населення та використання вільних виробничих можливостей.

Інцидент інформаційної безпеки - один або кілька небажаних або несподіваних подій інформаційної безпеки, які з значною ступенем ймовірності піддають небезпеки ділову діяльність та загрожують інформаційної безпеки

В даній таблиці представлені завдання та засоби їх реалізації, безпосередньо пов'язані з управлінням інцидентами інформаційної безпеки. Основна інформаційна частина взята з міжнародного стандарту ІБ 27001. [таб.1]

Управління ризиками інформаційної безпеки вимагає відповідають оцінки ризиків і методу обробки ризиків, які можуть включати оцінку втрат і вигод, законодавчі вимоги, питання, що викликають заклопотаність зацікавлених осіб та інші відповідні вихідні дані. Оцінка ризиків повинна виявляти, кількісно оцінювати і пріоритезувати ризики відповідно до критеріїв прийнятності ризиків і цілями, істотними для організації.

Ці результати повинні служити орієнтиром і визначати відповідаючи дії і пріоритети для управління ризиками інформаційної безпеки і впровадження засобів управління, обраних для захисту від цих ризиків. Оцінка ризиків повинна включати систематичний підхід до оцінки величини ризику (аналіз ризику) і процес порівняння прогнозної оцінки ризику з критеріями для визначення значущості ризиків (визначення ступеня ризику). Оцінка ризиків повинна виконуватися періодично для урахування змін у вимогах інформаційної безпеки і ситуації з ризиками, наприклад, для активів, погроз, уразливостей, впливів, оцінки ступеня ризику, а також коли відбуваються істотні зміни.

Завдання	**Засоби реалізації**
Обов'язки та процедури	Повинні бути встановлені обов'язки керівництва та процедури, щоб гарантувати швидкий, результативний і належну відповідь на інциденти інформаційної безпеки.
Оповіщення про події, пов'язані з інформаційною безпекою	Оповіщення про події інформаційної безпеки повинно доводитися по відповідних каналах управління якомога швидше.
Оповіщення про уразливість в інформаційній безпеці	Від співробітників і працюють за контрактом, що використовують інформаційні системи і сервіси організації, необхідно вимагати фіксувати і

	повідомляти про будь-які виявлені або передбачуваних вразливості в інформаційній безпеці систем і сервісів
Оцінка і рішення щодо подій інформаційної безпеки	Події інформаційної безпеки повинні оцінюватися і потім прийматися рішення, чи слід їх класифікувати як інцидент інформаційної безпеки.
Відповідні заходи на інциденти інформаційної безпеки	Реагування на інциденти інформаційної безпеки має здійснюватися відповідно до документально оформленими методиками.
Лікування уроків з інцидентів інформаційної безпеки	Знання, отримані з аналізу та дозволу інцидентів інформаційної безпеки, повинні використовуватися для зменшення ймовірності інцидентів в майбутньому або їх впливу.
Збір свідчень	Організація повинна визначити і застосовувати процедури для ідентифікації, збору, комплектування і збереження інформації, яка може служити в якості свідчень

В першу чергу, компанія повинна мати чітко визначену політику безпеки, адже без документованих принципів, правил, процедур і багато чого іншого неможливо регулювати інформаційні потоки.

Якщо прислухатися до рекомендацій і порад міжнародних стандартів ІБ, можна значно поліпшити безпеку системи в області управлінні інцидентами інформаційної безпеки. Основою для цих рекомендацій служив міжнародний стандарт ISO 21002, які більш детально описує не тільки питання в області УІІБ, а й основні правила менеджменту ІБ. Резюмуючи, хочеться сказати про те, що якщо керівництво комерційних підприємств буде приділяти належну увагу питанням УІІБ, то воно може заощадити фінанси, які були б витрачені на виправлення наслідків інцидентів і зберегти чисту репутацію своєї фірми.