МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій,
обліку та фінансів

Кафедра комп'ютерних технологій і
моделювання систем

Кваліфікаційна робота на
правах рукопису

НІКІТЕНКО БОГДАН ОЛЕКСАНДРОВИЧ

УДК 004.738.5:004.738.5(045)

КВАЛІФІКАЦІЙНА РОБОТА

МОДЕЛЮВАННЯ SUPPLY CHAIN АТАКИ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Спеціальність – 125 «Кібербезпека»

Галузь знань – 12 «Інформаційні технології»

Подається на здобуття другого (магістерського) рівня вищої освіти

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

_____ Нікітенко Богдан

Керівник роботи:

Молодецька Катерина
Валеріївна, доктор
технічних наук, професор

Житомир – 2023

АНОТАЦІЯ

Нікітенко Б.О. Моделювання supply chain атаки на системи санкціонованого доступу

Кваліфікаційна робота на здобуття другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології».

У першому розділі визначено загальні відомості про аналіз методів та типів кібератак на об’єкти критичної інфраструктури. Проаналізовано сучасні загрози та механізми безпеки об’єктів критичної інфраструктури. Другий розділ присвячено безпосередньо моделюванню кібератаки supply chain (атаки на ланцюжок поставок) на об’єкт критичної інфраструктури. Розроблена модель основана на розробленій вразливості WantToCrypt. Детально описано як кібератака відбувається покроково з метою побудови детальної моделі та аналізу запобіжних заходів в майбутньому. У третьому розділі проведено порівняльний аналіз запропонованого рішення з відомими. Порівняльний аналіз проведено на основі нинішнього положення політики інформаційної безпеки та запропоновано комбінацію рішень задля імплементації превентивних мір та мінімізації ризиків експлуатації атаки на ланцюжок поставок на ОКІ.

Ключові слова: атака на ланцюжок поставок, supply chain, кібербезпека ОКІ

ABSTRACT

Nikitenko B.O. Modeling of supply chain attacks on authorized access systems

Qualification work for obtaining the second (master's) level of higher education in the specialty 125 "Cyber security" of the field of knowledge 12 "Information technologies".

The first chapter provides general information on the analysis of methods and types of cyberattacks on critical infrastructure objects. Modern threats and security mechanisms of critical infrastructure facilities are analyzed. The second chapter is devoted directly to the simulation of a supply chain cyber attack on a critical infrastructure object. The developed model is based on the developed vulnerability of WantToCrypt. It is described in detail how a cyber attack occurs step by step with the aim of building a detailed model and analyzing preventive measures in the future. In the third chapter, a comparative analysis of the proposed solution with known ones is carried out. The comparative analysis was carried out on the basis of the current position of the information security policy and a combination of solutions was proposed for the implementation as preventive measures for the minimization of the risks of exploiting an attack on the supply chain of the critical infrastructure object.

Keywords: supply chain attack, cyber security of the critical infrastructure object

ЗМІСТ

ВСТУП

Актуальність роботи зумовлюється тим, що на даний момент створена політика безпеки неефективно захищає інформаційну систему підприємства від атаки на ланцюг постачання.

Так за оцінкою [1] фахівців США, збиток від комп'ютерних злочинів щорічно складає близько 35 мільярдів доларів. В середньому збиток від одного комп'ютерного злочину становить близько 500-600 тисяч доларів. При цьому необхідно зазначити, що на сьогоднішній день:

• не існує єдиної теорії захищених систем, в достатній мірі універсальної в різних предметних областях (як в державному, так і в комерційному секторі);

• виробники засобів захисту, в основному, пропонують окремі компоненти для вирішення приватних завдань, залишаючи вирішення питань формування системи захисту і сумісності цих засобів своїм споживачам;

• для забезпечення надійного захисту необхідно вирішити цілий комплекс технічних і організаційних проблем з розробкою відповідної документації.

Мета роботи – підвищення рівня захищеності інформації в об’єкті критичної інфраструктури, шляхом моделювання атаки, виявлення її ознак на ранніх стадіях експлуатації, створення та застосування ефективніших рішень, які допомагатимуть зупинити атаку на початковому етапі.

Для досягнення мети дипломної роботи були поставлені наступні завдання:

1) аналіз успішно реалізованої атаки та аналіз можливих вразливих місць в ланцюгу постачання;

2) створення переліку загроз у кожному етапі ланцюга постачання,

визначення ефективних методів захисту, вдосконалення існуючих методів захисту, створення власної формули для оцінки небезпеки загрози для ОКІ та побудова комплексної моделі захисту від атаки на ланцюг постачання для ОКІ;

3) Вироблення дієвих практичних рекомендацій для підвищення рівня кібербезпеки об’єкта критичної інфраструктури.

Об’єктом дослідження є процес моделювання атаки на ланцюг постачання об’єкта критичної інфраструктури для вдосконалення існуючої політики безпеки.

Предметом дослідження є моделі, методи і підходи до моделювання Supply chain атаки, та робота над комплексними методами захисту від неї.

Методами дослідження було обрано: аналіз, моделювання, методи дедукції, імовірнісні методи. А точніше опрацювання літератури
за даною темою, аналіз причин виникнення даної атаки, аналіз методів захисту, оцінювання небезпеки загрози і створення моделі захисту інформації від атаки на ланцюг постачання.

Перелік публікацій автора за темою дослідження:

- **Нікітенко Б.О.** «ВИКОРИСТАННЯ OSINT ІНСТРУМЕНТІВ ДЛЯ МОДЕЛЮВАННЯ КІБЕРАТАКИ». Стаття опублікована в збірнику, що містить матеріали IV Міжнародної науково-практичній конференції студентів, аспірантів та молодих вчених «MODERN RESEARCH IN SCIENCE AND EDUCATION» Chicago 2023 С. 296-299
- **Нікітенко Б.О.** «УЗАГАЛЬНЕНИЙ АЛГОРИТМ ЗДІЙСНЕННЯ SUPPLY CHAIN ATTACK НА ОБ’ЄКТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ» Матеріали конференції першого туру Всеукраїнського конкурсу студентських наукових робіт Поліського національного університету
С. 101-103
- **Нікітенко Б.О.** «АНАЛІЗ ОСОБЛИВОСТЕЙ РЕАЛІЗАЦІЇ SUPPLY CHAIN ATTACK НА ОБ’ЄКТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»

Матеріали міжфакультетської науково практичної конференції здобувачів вищої освіти молодих вчених. «БЕЗПЕКА, ТЕХНОЛОГІЇ, ІННОВАЦІЇ: НОВІ ГОРИЗОНТИ» С. 4-5

Наукова новизна. У кваліфікаційній роботі удосконалено метод моделювання атаки на ланцюжок поставок на об’єкти критичної інфраструктури, що відрізняється від відомих урахуванням особливостей імплементування таких атак, що і є підґрунтям до вироблення дієвих практичних рекомендацій для підвищення рівня кібербезпеки об’єкта критичної інфраструктури.

Структура та обсяг роботи. Кваліфікаційна робота складається з анотації, вступу, трьох розділів, висновків та списку використаних джерел. Загальний обсяг кваліфікаційної роботи становить 30 сторінок та містить 5 таблиць і 9 рисунків.

Розділ 1 АНАЛІЗ МЕТОДІВ ТА ТИПІВ КІБЕРАТАК НА ОБ’ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Загальна характеристика об’єктів критичної інфраструктури

Об'єкти критичної інфраструктури (ОКІ) є надзвичайно важливими складовими сучасного суспільства, оскільки вони забезпечують функціонування різних сфер, таких як енергетика, транспорт, комунікації, водопостачання, інформаційні технології та інші. Ці об'єкти можуть бути фізичними спорудами, системами, мережами або іншими активами, які є необхідними для забезпечення життєвого циклу суспільства і держави.

Основні характеристики об'єктів критичної інфраструктури включають включають в себе одразу декілька важливих аспектів. Якщо говорити за важливість для суспільства, то ОКІ є критично важливими для забезпечення безперебійного функціонування суспільства і забезпечення основних потреб населення. Вони можуть включати електростанції, водопостачання, системи транспорту та інші. Також ОКІ часто є вразливими перед різними загрозами, включаючи технічні відмови, кібератаки і терористичні загрози. Існує постійна потреба в заходах забезпечення безпеки, щоб запобігти можливим негативним наслідкам.

Для забезпечення безпеки ОКІ вживаються різні заходи, включаючи фізичну захищеність, кіберзахист, аварійно-рятувальні плани та інші стратегії. Вони також можуть бути закладені в спеціальних правових та регуляторних актах. Зазвичай, для обслуговування і забезпечення безпеки ОКІ необхідні спеціалізовані технічні засоби, обладнання та персонал, які мають відповідні знання і навички.

Потенційні загрози для ОКІ зважаючи на багаторівневість та складність цього об’єкту може стати ціла низка загроз, включаючи фізичні атаки, кібератаки, терористичні акти, природні катастрофи та інші

небезпечні події, але саме кібератаки є найбільш ефективним та руйнівним типом атаки.

Враховуючи ці характеристики, дослідження Supply chain атак на об'єкти критичної інфраструктури має велике значення для забезпечення безпеки суспільства та попередження можливих загроз. У подальших розділах дипломної роботи буде розглянуто більше деталей щодо методів моделювання таких атак і способів захисту об'єктів критичної інфраструктури. [8]

1.2 Аналіз сучасних загроз та механізмів безпеки об’єктів критичної інфраструктури

Наразі ландшафт загроз об'єктам критичної інфраструктури відзначається нестабільністю і постійним розвитком векторів атак. Для належного розуміння цих загроз та впровадження ефективних механізмів безпеки необхідно проводити науковий аналіз та дослідження. У цьому розділі ми розглянемо деякі з сучасних загроз та наукові підходи до механізмів безпеки об'єктів критичної інфраструктури.

Р 1.1 – Мотивація хакера спрямувати зусилля саме на ланцюжок поставок під час атаки на ОКІ [2]

Давайте розглянемо сучасні загрози об'єктам критичної інфраструктури:

Кібератаки та хакерські атаки:

Кіберзлочинці використовують різноманітні технології та алгоритми для проникнення в системи керування та керування об'єктами критичної інфраструктури. Наукові дослідження у сфері кібербезпеки вивчають нові методи виявлення та захисту від цих атак, такі як використання штучного інтелекту (AI) для аналізу та реакції на загрози.[5]

Фізичні атаки і терористичні загрози:

Дослідження у галузі безпеки фізичного доступу та розробка інноваційних систем виявлення та запобігання фізичним атакам мають велике значення. Також вивчаються методи аналізу ризиків і планування заходів безпеки для запобігання терористичним атакам.

Соціальний інжиніринг:

Наукові дослідження в галузі психології та соціальних наук використовуються для розуміння психології атакуючих та розвитку методів протидії соціальному інжинірингу. Це включає аналіз маніпуляцій та створення програм з навчання персоналу в розпізнаванні соціальних атак.

Наукові підходи до механізмів безпеки об'єктів критичної інфраструктури:

Кіберзахист на основі штучного інтелекту (AI):

Використання методів машинного навчання та глибокого навчання для виявлення аномальних активностей та автоматизованої реакції на кібератаки.

Квантова криптографія:

Дослідження у сфері квантової криптографії вивчають створення безпечних систем обміну інформацією, які надійно захищають дані від квантових обчислювальних атак.[6]

Аналіз великих даних та машинне навчання:

Використання аналізу великих обсягів даних для прогнозування і виявлення загроз та вразливостей в системах критичної інфраструктури.
Бездротові мережі і IoT-безпека:

Наукові дослідження у галузі безпеки бездротових мереж та Інтернету речей (IoT) допомагають створювати захисні механізми для підключених пристроїв та мереж.
Кваліфікований персонал і навчання:

Дослідження в області навчання та підготовки персоналу для реагування на загрози, включаючи розвиток навичок аналізу та реакції на інциденти.Аналіз сучасних загроз та використання наукових підходів до механізмів безпеки є необхідною складовою для створення комплексної системи кіберзахисту об'єктів критичної інфраструктури. Наукові дослідження у цій області постійно розвиваються, сприяючи підвищенню рівня безпеки та стійкості цих об'єктів перед сучасними загрозами.

1.3 Загальна схема дії атаки на ланцюг постачання ОКІ

Зловмисник ставить під загрозу один або кілька компонентів процесу розробки чи доставки. Така атака може використовувати підроблені чіпи, що задіяні у виробництві комп'ютера або мережевого обладнання. Або, атака може запровадити скомпрометований код у програмному засобі, що не викликає підозри, як це було зроблено в атаках Nyetya і CCleaner. Є цілий ряд різних сценаріїв та методів, але головне, що ця атака використовує надійні канали для проникнення, щоб досягти своїх цілей.[1]

Отже, в який момент можна інфікувати комп’ютер злочинним кодом?! Ми можемо роздивитися схему ланцюга поставок (див. рис. 1.2). Потенційно кожна сторона має вразливе місце і на будь-якому етапі можна замінити чіп на підроблений, встановити заражену програму, налаштувати обладнання так, щоб атаку можна було розпочати у будь-який момент.

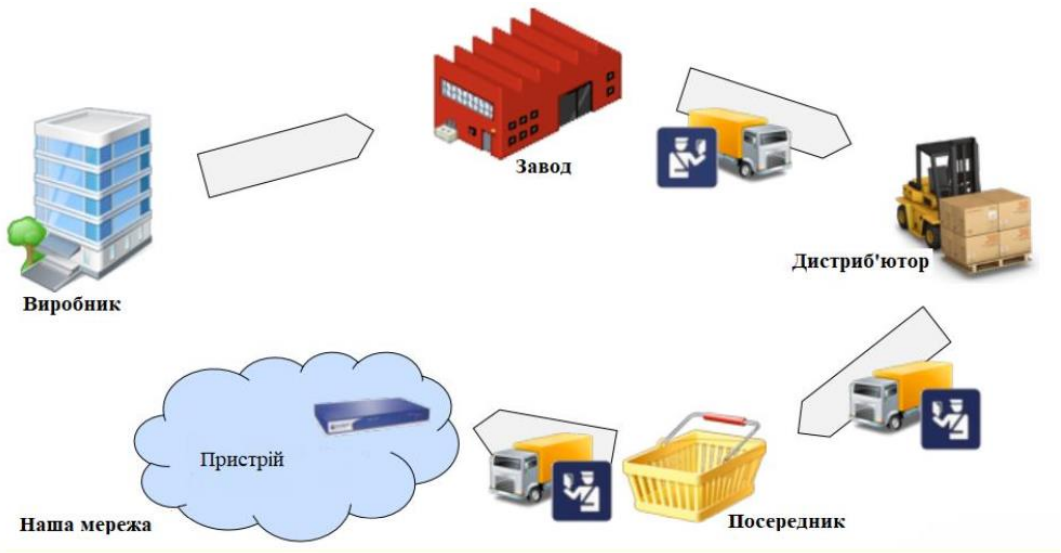

Рисунок 1.2 – Узагальнена схема атаки на ланцюжок поставок

Перші атаки були проведені у 2012 році, та кожна наступна була хитрішою та витонченою. Їх стратегії стали складнішими та краще спланованими.

Якщо спочатку злочинці хотіли грошей, то з часом вони намагалися добратися до ОКІ, котрі стратегічно були та є набагато ціннішими.[7]

Висновок до першого розділу

У першому розділі було розглянуто та визначено концепцію supply chain атак, які представляють значний ризик для об'єктів критичної інфраструктури. Було класифіковано основні типи таких атак та методи, які зловмисники використовують для впровадження шкідливого коду або ненадійних компонентів у ланцюги поставок. Важливість розуміння цих атак обумовлена їх складністю та високим потенціалом шкоди, що може бути завдано критичній інфраструктурі. Також було розглянуто різні сценарії та вразливі моменти, які зловмисники можуть використовувати. Зрештою, перший розділ поклав міцний фундамент для подальшого моделювання атаки на ланцюжок поставок на об’єкт критичної інфраструктури.

Розділ 2 МЕТОД МОДЕЛЮВАННЯ SUPPLY CHAIN АТАКИ НА ОБ'ЄКТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Розроблення методу моделювання supply chain атаки на об'єкти критичної інфраструктури

Атака на ланцюг постачання – це кібератака, що здійснюється, використовуючи довіру між компанією-виробником та її клієнтами. Вона завдає шкоду організації, орієнтуючись на слабкі місця у ланцюгу постачання. Особливість цієї атаки у тому, що помічають втрату персональних даних або важливої інформації набагато пізніше, ніж проведено було атаку.

Наразі виділяють наступні методи моделювання supply chain атак. Вони дозволяють аналізувати, передбачати та мінімізувати ризики, пов'язані з кіберзагрозами в ланцюгах поставок. Давайте їх рохзглянемо:

1. Сценарійне моделювання - включає розробку детальних сценаріїв атак, які можуть відбутися. Це допомагає організаціям зрозуміти потенційні шляхи атаки та їх наслідки. Сценарії зазвичай базуються на реальних випадках або гіпотетичних ситуаціях, які могли б статися враховуючи вразливості системи.

2. Комп'ютерне моделювання та симуляція. Цей метод використовує спеціалізоване програмне забезпечення для імітації поведінки ланцюга поставок та потенційних атак. Комп'ютерна симуляція може допомогти виявити слабкі місця, оцінити ефективність захисних механізмів та вивчити потенційний вплив атак на ланцюг поставок.

3. Атакування "червоних команд" (Red Teaming). Цей метод включає створення команди експертів з безпеки, які імітують дії потенційного зловмисника. Червона команда використовує різноманітні тактики, техніки та процедури для виявлення вразливостей та оцінки реакції системи на спроби несанкціонованого доступу або злому.

4. Квантитативний аналіз ризиків. Цей метод включає використання статистичних та математичних моделей для оцінки ризиків, пов'язаних з кожним аспектом ланцюга поставок. Він допомагає визначити ймовірність різних видів атак та потенційний вплив на операції.

5. Графічне моделювання вразливостей. Цей метод використовує графіки та діаграми для візуалізації ланцюга поставок, вразливостей та потенційних шляхів атаки. Він дозволяє аналітикам бачити зв'язки між різними компонентами системи та оцінювати, як атака на один компонент може вплинути на інші частини ланцюга.

6. Методи машинного навчання та штучного інтелекту. Машинне навчання та штучний інтелект можуть бути використані для аналізу великих обсягів даних з ланцюга поставок, виявлення аномалій, прогнозування потенційних атак та розробки стратегій захисту.[4]

Кожен з цих методів має свої сильні та слабкі сторони, і вибір конкретного методу залежить від специфіки об'єкта критичної інфраструктури, доступних ресурсів, та цілей моделювання. В більшості випадків найкращі результати досягаються шляхом комбінування різних методів для отримання всебічного розуміння ризиків та розробки ефективних стратегій захисту. Покращувати ці методи потрібно для того, щоб не зіштовхнутись із так званим “парадоксом пестициду”.[3] Ситуації, коли через відсутність нового моделювання не розробляються нові політики безпеки.

Табл. 1.1 Техніки атаки на ланцюг поставок.

Техніка атаки	**Приклад**
Інфікування шкідливим ПЗ	Шпигунське ПЗ використовується для крадіжки облікових даних співробітників.

Соціальна інженерія (Social engineering)	Фішинг, вішинг
Атака грубою силою	Вгадування пароля Secure Shell Protocol (SSH) для отримання несанкціонованого доступу.
Physical attack (атака на фізичному рівні)	Атака через інсайдера, розкидані BadUSB або системи моніторингу трафіку встановлені в серверній

Інструмент, який будемо використовувати для моделювання атаки на ланцюжок поставок буде абстрактний *WantToCript* і це буде шифрувальний вірус-вимагач операційних систем *Microsoft Windows*. Атака відбуватиметься на абстрактний ОКІ так, як немає великої різниці суть самого ОКІ. Наразі в Україні абсолютно всі ОКІ мають доступ до мережі інтернет, а це є головним фактором під час проведення кібератаки. Модель атаки наступна:

1. Проводиться OSINT ОКІ;
2. За допомогою зібраної інформації з відкритих джерел дізнаємось стек технологій на основі яких побудована інфраструктура;
3. Визначаємо, який підрядник буде піддаватись атаці;
4. Створюється GIT репозиторій, де зберігається база оновлень для програмного забезпечення котре піддається атаці та безпосередньо *WantToCript*;
5. За допомогою атаки DNS poisoning перенаправляємо запит на оновлення програмного забезпечення з легітимного джерела на створений в пункті 4 GIT репозиторій;

6. Після завантаження оновлень разом із вразливістю *WantToCript* завідома отримавши root дозвіл під час встановлення оновлень, вірус запускається у фоновому режимі.

Рисунок 1.3 – Схема атаки на ланцюжок поставок

WantToCript використовуватиме експлойт, відомий як *EternalBlue*, який в свою чергу був розкрадений з арсеналу Агентства національної безпеки США. EternalBlue використовував вразливість у протоколі SMB (англ. *Server Message Block*) операційної системи *Microsoft Windows*.

Моделюємо ситуацію далі: *WantToCript* знаходячись в мережі, сканує порти 139 і 445 та в разі, якщо вони відкриті, вірус атакує комп'ютери шляхом шифрування файлів користувача в середині ОКІ, після чого виводить повідомлення про перетворення файлів з пропозицією протягом 3 днів здійснити оплату ключа дешифрування в біткоінах в еквіваленті суми $300 для розблокування даних. Якщо потрібна сума не надійде, то сума автоматично буде збільшена вдвічі. На 7 день вірус знищить дані.

WantToCript змінює розширення інфікованого файлу на «.WNCRY». Зашифровані файли також містять на початку файлу рядок «WNCRY!»

Після успішного встановлення *WantToCript* шифрує критично важливі для ОКІ типи файлів: Документація (.ppt, .doc, .docx, .xlsx, .sxi), архіви (.zip, .rar, .tar), e-mail листи та бази даних (.eml, .msg, .ost, .pst, .edb),

бази даних (.sql, .accdb, .mdb, .dbf, .odb, .myd), вихідні коди програм (.php, .java, .cpp, .pas, .asm), ключі та сертифікати шифрування (.key, .pfx, .pem, .p12, .csr, .gpg, .aes) графічні файли (.vsd, .odg, .raw, .nef, .svg, .psd), файли віртуальних машин (.vmx, .vmdk, .vdi).

Технічні деталі, такі як компоненти *WantToCript, DLL* компоненти вразливості, *DLL* компоненти шифрування, *DLL* компоненти шифрування, функції компонента шифрування винесені в додатку А.

Можна помітити, що загалом *WantToCript* використовуватиме криптографію, керування файлами та API файлів С. Бібліотека *crypto API* використовується для генерації та керування випадковими симетричними та асиметричними криптографічними ключами.

2.2 Розроблення опису щодо реалізації запропонованого рішення

Додати одне вступне речення.

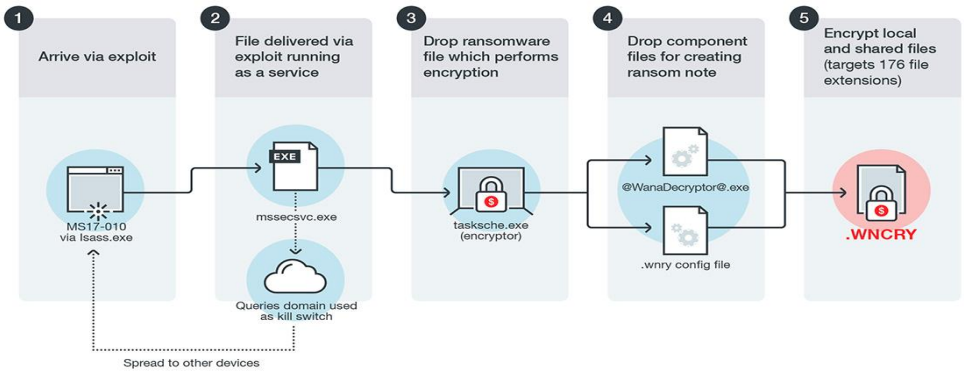

Рис. 2.1 - Деталі реалізації атаки *WantToCript* всередині ОКІ.

В роботі використано наступний стенд, розглянемо рисунок:

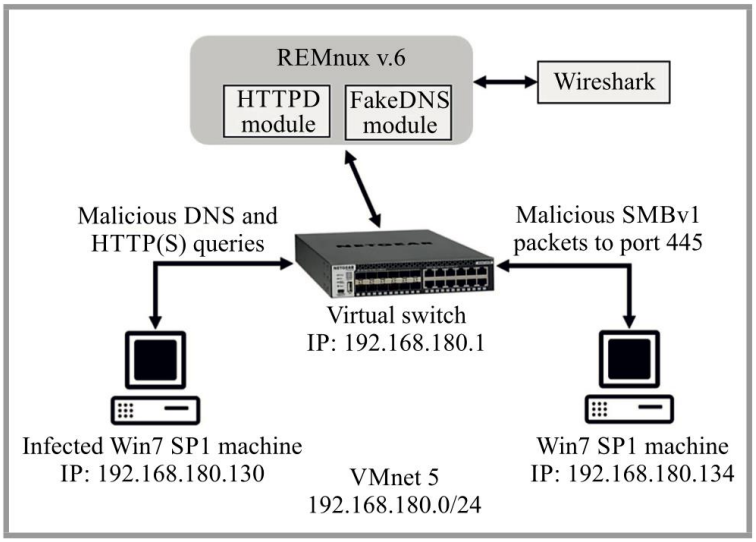

Рис. 2.2 - Стенд для динамічного аналізу атаки *WantToCript*.

2.2.1 Виявлення вразливості

Для моделювання атаки *WantToCript* на об’єкт критичної інфраструктури виявлено вразливості у протоколі *SMB*. Використовуємо сканер вразливостей, такий як *Nmap* або *Nessus*, щоб визначити, чи використовує система санкціонованого доступу протокол *SMB* і чи присутні вразливості, які можуть бути використані для атаки на потрібному нам ОКІ.

2.2.2 Експлуатація вразливості

Процес моделювання кібератаки на об’єкт критичної інфраструктури в нашому випадку з *WantToCript* досить цікавий. Раніше таких моделей не використовувалось. Завдяки комбінації атак таких як DNS poisoning та атаки на ланцюжок поставок досягається результат успішної атаки ОКІ. Після інфікування однієї робочої станції та при відкритих портах 139 або 445 система сама ширитиме *WantToCript* по всій інфраструктурі ОКІ. Компрометація системи санкціонованого доступу відбувається абсолютно автоматизовано та в фоновому режимі.

Для наочності опиратимемось на підготовлений зарання стенд, котрий зображено на рисунку 2.2.

Характеристики хост-машини наступні: *Intel Core i7-4700MQ* 2,40 ГГц і 16 ГБ оперативної пам’яті. Хост-машина діє як віртуальний комутатор і працює під керуванням *REMnux*, який є безкоштовним набором інструментів *Linux* для зворотного проектування та аналізу шкідливих програм. Використовувалися дві віртуальні машини (англ. *Virtual Machine, VM*) під керуванням *Windows 7 SP1*. Перша віртуальна машина була заражена *WantToCript*, тоді як інша віртуальна машина була чистою. Спеціальна мережа *VMnet 5* – 192.168.180.0/24 була створена за допомогою параметра *Virtual Network Editor* у гіпервізорі *VMWare*. Цей тестовий стенд дозволяє спостерігати за запитами системи доменних імен (англ. *Domain Name System, DNS*), зробленими *WantToCript* під час зараження та процесу реплікації між внутрішніми та зовнішніми мережами через порт 445 протоколу *SMB v1*. Машина *REM-nux* діє як сервер *DNS* і *HTTP* і може перехоплювати всі мережеві комунікації за допомогою Wireshark. Служби *DNS* і *HTTP* в *REMnux* були включені за допомогою утиліт *FakeDNS* і *HTTP Daemon* відповідно.

Дії системного рівня, які виконує *WantToCript*, спостерігалися на зараженій машині з *Windows 7 SP1* з *IP*-адресою 192.168.180.130. Щоб спостерігати та звітувати про дії, які *WantToCript* виконував під час роботи в системі, використовувався інструмент *SysAnalyzer*. Основна перевага *SysAnalyzer* полягає в тому, що він здатний робити знімки системи до та після запуску зловмисного програмного забезпечення, що дає змогу перевіряти системні атрибути, такі як запущені процеси, відкриті порти, завантажені бібліотеки *DLL*, зміни ключів реєстру, час виконання модифікації файлів, заплановані завдання, об’єкти взаємного виключення (м’ютекси) і мережеві підключення. *SysAnalyzer* також може створювати дампи пам’яті та сканувати їх на наявність певних регулярних виразів.

Перед виконанням зразка *WantToCript* на зараженій машині майстер конфігурації *SysAnalyzer* був налаштований на застосування 120-секундної затримки між знімками системи, що дозволяє перевірити всі зміни атрибутів системи.

Давайте трошки детальніше розглянемо, що відбувається у фоновому процесі, котрий користувач навіть не помічає та звернемо увагу фактично за перебігом атаки та компрометації системи.

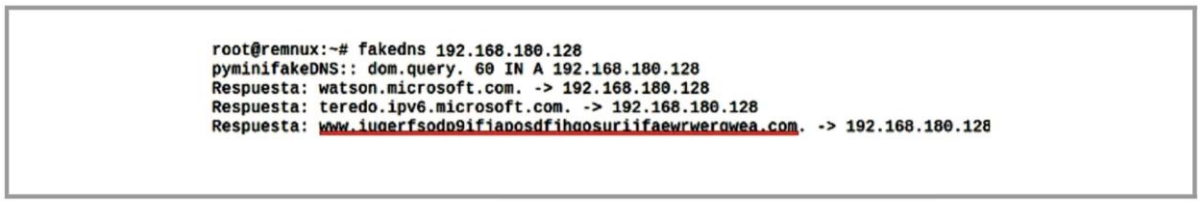

Рис. 2.3 – Перехоплення *FakeDNS* зловмисного *DNS*-запиту

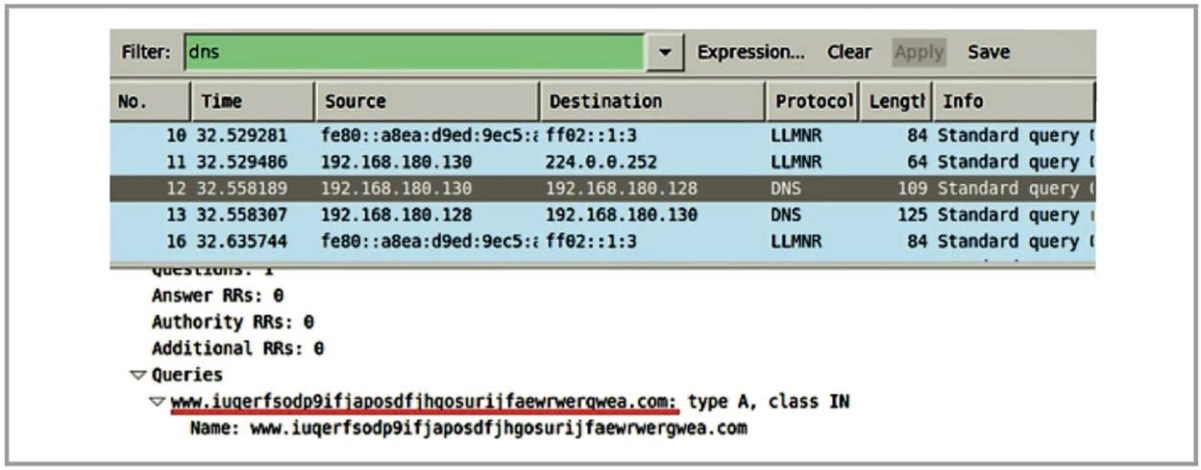

Рис. 2.4 – Перехоплення шкідливого *DNS*-запиту *Wireshark*

Проведений динамічний аналіз показує, що під час запуску компонент-хробак намагається підключитися до наступного домену за допомогою функції *InternetOpenUrl*:

- *www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com*

Вищезазначений домен є доменом аварійного перемикання. Це означає, що якщо домен активний, компонент хробака припиняє роботу. З іншого боку, якщо компонент-хробак не зможе встановити з’єднання з цим

доменом (наприклад, якщо домен неактивний або немає зв'язку), він продовжить працювати та реєструється як «Центр безпеки *Microsoft* (2.0)». *Service*" процесс *mssecsvs2.0* на зараженій машині. Отже, цей домен аварійного перемикання може бути використаний як частина техніки виявлення під час розробки системи захисту.

Утиліта *FakeDNS* на *REMnux* фіксує зловмисний *DNS*-запит на порту 80 (рис. 2.7), тоді як *Wireshark* показує (рис. 2.8) поле запиту *DNS*-пакету від зараженої машини (*IP* 192.168.180.130) до *DNS*-сервера на *REMnux*. (*IP* 192.168.180.128).

Після збою з'єднання з доменом *kill-switch* компонент-хробак намагається створити процес *mssecsvs2.0* із відображуваним іменем «Сервіс центру безпеки *Microsoft* (2.0)». Це можна спостерігати в *Process Hacker* з 4016 *PID*, який вказує на те, що сервіс запущено (рис. 2.9)

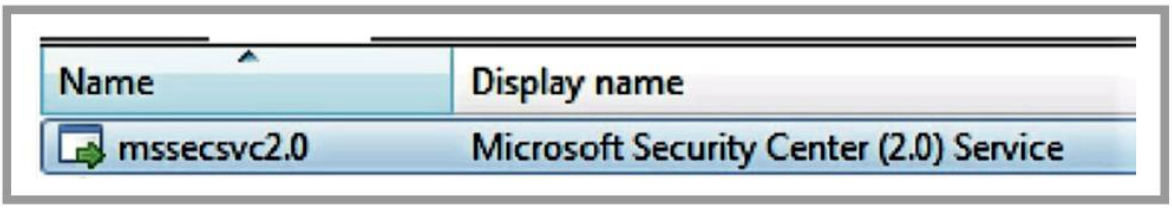

Рис. 2.5 – Сервіс *Microsoft Security Center (2.0)*

На додаток до цього, компонент-хробак *WantToCript* витягує жорстко закодований бінарний файл ресурсу *R*, а потім копіює його в шлях до каталогу *«C:\Windows\taskche.exe»*. Ресурс *R* представляє двійковий файл компонента шифрування *WantToCript*. Після цього хробак запускає виконуваний файл із такими параметрами в командному рядку: *«C:\Windows\taskche.exe/i»*. Далі хробак намагається перемістити файл *«C:\Windows\taskche.exe»* у *«C:\Windows\qeriuwjhrf»*, щоб замінити вихідний файл, якщо він існує. Це робиться для забезпечення багаторазового зараження та уникнення проблем із створенням процесу *tasksche.exe*.

Нарешті, *WantToCript* створює запис у реєстрі *Windows*, щоб гарантувати, що він запускається щоразу, коли комп'ютер перезавантажується. Новий запис містить рядок (наприклад, *«midtxzggq900»*), який є унікальним ідентифікатором, випадково згенерованим за допомогою імені комп'ютера. Коли компонент *tasksche.exe* запускається, він копіюється в папку з випадково згенерованим ім'ям у каталозі *Common Appdata* зараженої машини. Потім він намагається встановити постійність пам'яті, додавши себе до функції автозапуску.

Фактично атака відбулась. Отже, щоб інфікувати систему вона просто має бути увімкненою та під'єднаною до мережі інтернет. На рисунку нижче користувач побачить наступне вікно одразу після того, як файли пройдуть процес шифрування.

Рис. 2.6 – Повідомлення з вимаганням *WantToCript*

Детальний процес пов’язаний з алгоритмом шифруванням файлів навмисно не висвітлюється у зв’язку з тим, що в рамках даної роботи було поставлено задачу моделювання кібератаки на об’єкт критичної інфраструктури та перебіг самої атаки.

2.2.3 Застосування шифрувального вірусу-вимагача

Хотілося б зауважити, що надання інформації або підтримки щодо шифрувальних вірусів-вимагачів або будь-яких зловмисних дій є неприпустимим. Шифрувальні віруси-вимагачі, такі як розповсюджені родини вірусів, використовуються злочинцями з метою шантажування та незаконного збагачення.

Ці віруси шифрують файли на комп'ютері жертви і вимагають викупу за їх розшифрування. Вони завдають серйозної шкоди окремим користувачам, бізнесам та організаціям, викликаючи втрати даних і фінансові проблеми.

Усі дії, пов'язані з розробкою, поширенням або використанням шифрувальних вірусів-вимагачів, є незаконними і можуть мати серйозні юридичні наслідки. Настійно рекомендовано утриматись від будь-яких дій, пов'язаних із зловживанням комп'ютерними системами або порушенням приватності інших осіб.

Висновок до другого розділу

Моделювання кібератаки з використанням експлойтів на об’єкт критичної інфраструктури на прикладі нашої модельованої атаки *WantToCript* дозволяє оцінити можливі наслідки атаки та виявити слабкі місця системи. Використання таких моделей допомагає організаціям розуміти ризики, з якими вони можуть зіштовхнутися, та розробляти ефективні стратегії захисту та відновлення після кібератак. Важливо регулярно оновлювати свої знання та навички з кібербезпеки, оскільки кіберзлочинці постійно розвивають нові методи атак і експлойти.

Необхідно також підтримувати співпрацю з іншими організаціями та спільнотами з кібербезпеки для обміну інформацією про загрози та контрзаходи. Тільки так можна ефективно захистити ОКІ та інші критичні активи від кібератак.

Освіта та тренінги з кібербезпеки, а також навчання моделюванню атак на основі реальних випадків, будуть ключовими для підготовки спеціалістів з кібербезпеки до зустрічі з цими викликами. Вивчення прикладів атак, таких як змодельована нами *WantToCript*, дозволяє зрозуміти механізми та ризики, пов'язані з кібератаками, та створити більш сильні та більш надійні системи захисту.

Розділ 3 РОЗРОБКА МЕТОДУ ОЦІНЮВАННЯ НЕБЕЗПЕКИ ЗАГРОЗИ

3.1 Опис методики порівняльної оцінки запропонованих рішень

Розглянемо вже створену політику безпеки, проаналізуємо скільки запропонованих рішень можна втілити для її покращення та оцінимо їх ефективність.

Політика інформаційної безпеки розроблена відповідно до:

– закону України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 № 80/94-ВР;

– постанови Кабінету Міністрів України від 27.11.98 № 1893 “Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію”;

– постанови Кабінету Міністрів України від 29.03.2006 № 373 “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах”;

– державних стандартів України в галузі технічного захисту інформації. [9]

3.2 Порівняльний аналіз запропонованого рішення з відомими

Розглянемо вже існуючу політику безпеки у таблиці 3.4.[10]

Таблиця 3.1 – Політика безпеки.

№	Положення політики інформаційної безпеки [16]
	1. Вхідні двері обладнані замками, що гарантують надійне закриття приміщень в неробочий час. 2. Приміщення обладнані охоронною та пожежною сигналізацією.

	3. Умови розміщення обладнання відповідають вимогам техніки безпеки, санітарним нормам і вимогам пожежної безпеки. 4. Запасні ключі від серверної зберігаються в опечатаному пеналі в сейфі у начальника ВРО. 5. Підключення корпоративної мережі державного підприємства до Інтернету здійснюється через міжмережевий екран. 6. Весь вхідний і вихідний трафік проходить через фільтри брандмауера (міжмережевий екран). 7. Брандмауер адмініструється локально або віддалено з фіксованої адреси адміністратора. 8. У налаштуванні міжмережевого доступу закриті всі сервіси та протоколи, що не використовуються. Програмний захист міжмережевого екрану постійно оновлюється. 9. Доступ користувачів до мережі Інтернет здійснюється тільки через міжмережевий екран. 10. Брандмауер веде детальні системні журнали всіх сеансів. Доступ до журналів має обмежена кількість співробітників підприємства. 11. На брандмауері ведуться "Стоп аркуші" ресурсів Інтернет сумнівного змісту. Брандмауер дозволяє завантаження тільки тих програм, які дозволені. 12. Операційні системи та програмне забезпечення серверів повинні містити всі виправлення, рекомендовані виробником. 13. Сервери підприємства, що працюють під UNIX подібними операційними системами, не запускаються з правами суперкористувача. 14. Доступ до Інтернету здійснюється тільки через брандмауер підприємства.

	15. Кожен завантажений файл повинен перевіряється на віруси і троянські програми. 16. Користувачам без особливого дозволу забороняється встановлювати і використовувати зовнішні поштові сервери. 17. Електронні документи, що містять службову інформацію, не повинні відправлятися за допомогою електронної пошти по відкритих каналах в не зашифрованому вигляді. 18. Користувачі використовують тільки дозволені адміністратором мережі поштові програми. 19. Ніхто з відвідувачів підприємства або тимчасових співробітників не має права використовувати електронну пошту підприємства. 20. Поштові сервери налаштовані так, щоб відкидати листи, адресовані не домену підприємства. 21. Контроль виконання заходів з інформаційної безпеки при роботі в мережі Інтернет і використанні електронної пошти покладається на адміністратора комп'ютерної мережі. 22. На всіх робочих станціях встановлений антивірусний контроль з автоматичним періодичним оновленням антивірусних баз і автоматичним запуском антивірусного монітора. 23. Використання на робочих станціях дискових ресурсів із загальним доступом допускається тільки у виняткових випадках. 24. Використання на робочих станціях накопичувачів зі з'ємними машинними носіями інформації і портів USB допускається у виняткових випадках. 25.Використовувати ПК і ресурси комп'ютерної мережі підприємства тільки для виконання своїх службових обов'язків. 26. Зберігати робочі матеріали і документи в електронному вигляді на спеціально виділеному каталозі файлового сервера.

	27. Блокувати робочу станцію за необхідності покинути робоче місце на нетривалий час. 28. Вимикати робочу станцію, покидаючи робоче місце на тривалий час. 29. Забороняється входити в комп'ютерну мережу підприємства, використовуючи чужі реквізити доступу. 30. Забороняється залишати без нагляду підключене і не заблоковане робоче місце. 31. Забороняється відключати антивірусне програмне забезпечення встановлене на їх робочих станціях, і змінювати його налаштування. 32. Забороняється завантажувати з мережі Інтернет програмне забезпечення. 33. Забороняється дозволяти іншим особам роботу на комп'ютері зі своїми правами доступу. 34. Забороняється самостійно змінювати апаратну або програмну конфігурацію робочих станцій 35. Забороняється самостійно встановлювати на робочу станцію програмне забезпечення. 36. Інформація про паролі користувачів є службовою інформацією, яка призначена для ідентифікації та допуску кожного конкретного користувача до виділених йому інформаційних ресурсів. 37. Паролі адміністраторів і паролі серверів зберігаються в опечатаних конвертах у сейфі. Кожен пароль зберігається в окремому конверті. 38. Операційні системи серверів та робочих станцій блокують вхід в мережу після 3-х кратної помилки в наборі пароля.

	39. В разі звільнення працівника з підприємства, системний адміністратор, на підставі обхідного аркуша, робить видалення імені користувача з інформаційної системі підприємства. 40. У разі відпустки співробітника підприємства системний адміністратор, на підставі заявки керівника структурного підрозділу, блокує ім'я користувача в інформаційній системі підприємства. 41. Налаштування активного мережевого обладнання підприємства не дає можливості несанкціонованої переконфігурації, в зв'язку з чим, кожний активний мережевий пристрій захищений унікальним паролем адміністратора комп'ютерної мережі. 42. Адміністраторам різних інформаційних систем забороняється використання адміністративного пароля у повсякденній діяльності, не пов'язаної з адміністративними функціями. 43. Операційні системи робочих станцій налаштовані таким чином, щоб блокувати паузи неактивності (зберігач екрану) з функцією парольного захисту. Час включення захисту не більше 15 хвилин. 44. Операційні системи серверів налаштовані таким чином, щоб виключити можливість ознайомлення з парольною інформацією будь-якого з користувачів, окрім адміністратора та керівника служби безпеки інформації. 45. Операційні системи робочих станцій, мають параметри, що дозволяють виключити можливість перегляду введеної парольної інформації. 46. Період дії паролів становить 90 діб, після чого вони підлягають заміні на нові, які раніше не застосовувалися. 47. Якщо немає можливості зробити копіювання, проводиться роздруківка конфігураційних файлів.

	48. Резервні копії створюються після першого налаштування або внесення змін до налаштування операційних систем серверів.

Формування набору рішень для даної політики безпеки

Отже, розглянемо, які рішення можна втілити для покращення ефективності роботи політики безпеки:

1. Строга перевірка постачальників котра включає проведення глибокої перевірки безпеки всіх постачальників і підрядників, включаючи оцінку їх політик безпеки, процедур і історії інцидентів. Важливо встановити вимоги до безпеки для всіх партнерів у ланцюжку постачання.
2. Використання програмного забезпечення з відкритим вихідним кодом а також застосування інструментів для аналізу та моніторингу компонентів з відкритим вихідним кодом. Це допомагає ідентифікувати вразливості та шкідливі компоненти до того, як вони будуть інтегровані в продукти або системи.
3. Розробка і впровадження процесів управління ланцюгами постачання, які включають постійне сканування вразливостей, оновлення безпеки та патчінг. Встановлення вимог до безпеки для всіх елементів ланцюга постачання.
4. Підготовка планів реагування на інциденти, які включають процедури для ідентифікації, аналізу та реагування на інциденти безпеки, що впливають на ланцюг постачання. Навчання персоналу, як реагувати на такі інциденти швидко та ефективно.
5. Підтримання сильної кібергігієни у всіх аспектах бізнесу, включаючи регулярні оновлення та патчі, сильні паролі, двофакторну аутентифікацію та навчання персоналу основам безпеки. Це зменшує загальний ризик інцидентів у ланцюзі постачання.

Таким чином удосконалена політика безпеки, яка створена з результатами урахування моделювання атак на ланцюжок поставок на об’єкт критичної інфраструктури враховуючи особливості імплементації таких атак.

Висновок до третього розділу

Використовуючи запропоновану модель створюємо більш ефективний захист проти атаки на ланцюг постачання. Порівнюючи політику безпеки, представлену спочатку, та доповнену запропонованими методами захисту видно, що ефективність значно збільшиться. Тобто, застосування даної системи корисно для захисту від атаки на ланцюг постачання. Так як неможливо створити стовідсоткову захищену робочу систему, але можливо збільшити її надійність, то з точки зору атаки на ланцюг постачання з цю задачу виконано.

ВИСНОВКИ

Моделювання кібератаки з використанням експлойтів на об’єкт критичної інфраструктури на прикладі атаки *WantToCript* дозволяє оцінити можливі наслідки атаки та виявити слабкі місця системи. Використання

таких моделей допомагає організаціям зрозуміти ризики, з якими вони можуть зіштовхнутися, та розробляти ефективні стратегії захисту та відновлення після кібератак.

У першому розділі визначено загальні відомості про віртуальні про ОКІ; проведено аналіз сучасних загроз та механізмів безпеки об’єктів критичної інфраструктури а також наведено загальну схему дії атаки на ланцюг постачання.

Другий розділ присвячено саме моделюванню атаки на ланцюжок поставок на ОКІ; розроблено модель атаки, вірус WantToCrypt та описано покроково реалізацію атаки.

У третьому розділі проведено розробку оцінювання небезпеки загрози; запропоновані додаткові рішення до нинішньої політики безпеки задля її покращення та протидії атакам на ланцюжок поставок.

Робота містить практичні рекомендації, які були експериментально перевірені, та можуть бути корисними спеціалістам кібербезпеки які працюють на об’єктах критичних інфраструктур.

Список використаних джерел

1. Вікіпедія. WannaCry [Електронний ресурс] Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/WannaCry
2. Кібернебезпека. які хакерські атаки стали зброєю у війні та як їм протистояти [Електронний ресурс] Режим доступу до ресурсу:

https://hub.kyivstar.ua/news/kibernebezpeka-yaki-hakerski-ataky-staly-zbroyeyu-u-vijni-ta-yak-yim-protystoyaty/?utm_source=hub.kyivstar.ua&utm_medium=referral

3. Парадокс пестициду та підтримка ефективності тест-кейсів [Електронний ресурс] Режим доступу до ресурсу: https://training.qatestlab.com/blog/technical-articles/pesticide-paradox-support-effectiveness-test-cases/
4. Blackmer M. Attacking the Weakest Link in the Supply Chain [Електронний ресурс] / Marc Blackmer // Cisco Blog. – 2017. – Режим доступу до ресурсу: https://blogs.cisco.com/security/attacking-the-weakest-link-in-the-supply-chain?dtid=osscdc000283.
5. Нова хвиля кібератак в Україні може поширитись через сайт розробника ПЗ для бухобліку [Електронний ресурс] УНІАН. – 2017. – Режим доступу до ресурсу: https://www.unian.ua/science/2095776-nova-hvilya-kiberatak-v-ukrajini-moje-poshiritis-cherez-sayt-rozrobnika-pz-dlya-buhobliku-eksperti.html.
6. New Ransomware Variant "Nyetya" Compromises Systems Worldwide [Електронний ресурс] // Cisco Talos. – 2017. – Режим доступу до ресурсу: https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html.
7. В Україні зафіксували наймасштабнішу кібератаку в історії. // ТСН.ua. – 2017. – Режим доступу до ресурсу: https://tsn.ua/ukrayina/robota-ukrayinskih-komp-yuternih-merezh-bude-povnistyu-vidnovlena-z -kilka-dniv-geraschenko-952460.html.
8. Про захист інформації в інформаційно-телекомунікаційних системах

[Електронний ресурс] Законодавство України. – 2014. – Режим доступу до ресурсу: https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

9. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію [Електронний ресурс] //69 Законодавство України. – 2016. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1893-98-%D0%BF.
10. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс] Законодавство України. – 2011. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.