Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: *«Розробка методології захисту інформації від атак через посередника на підприємствах малого та середнього бізнесу»*

Виконав: студент (ка) *VI* курсу, групи *СБм-61*
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Єпур В. П
підпис (прізвище та ініціали)

Керівник ____ *Карпінський М. П.*
підпис (прізвище та ініціали)
Нормоконтроль ____ _____
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 20*21*

АНОТАЦІЯ

Розробка методології захисту інформації від атак через посередника на підприємствах малого та середнього бізнесу // Дипломна робота ОР «Магістр» // Єпур Вадим Павлович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2021 // С. – 53 , рис. – 10, табл. – 3.

Ключові слова: АТАКА ЧЕРЕЗ ПОСЕРЕДНИКА, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, ПІДПРИЄМСТВА.

Дана магістерська кваліфікаційна робота присвячена дослідженню проблем захисту інформації на підприємствах малого та середнього бізнесу, основну увагу приділено захисту інформаційно-комунікаційної системи від атак через посередника. В роботі проведено огляд літературних джерел в області дослідження. Проведено систематизація дослідженого матеріалу та визначено найбільш поширені типи атак, які можуть бути застосовані до інформаційно–комунікаційних систем малого та середнього бізнесу. Відповідно до досліджених ризиків розроблено нову методологію захисту підприємств малого та середнього бізнесу, яка не потребує великих затрат, що дозволяє застосовувати її навіть на тих підприємствах, де не передбачено витрат для роботи спеціаліста з інформаційної безпеки та придбання спеціального програмного забезпечення для запобігання атак через посередника. Розроблена методологія є гнучкою, що дозволяє використовувати її на підприємствах малого та середнього бізнесу з різним родом діяльності.

ANNOTATION

Development of information protection methodology against man-in-the-middle attacks in small and medium-sized businesses // Thesis of "Master" Degree// Fihol Valerii Yaroslavovych // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group SBm-61 // Ternopil, 2021 // S. – 53 , fig. - 10, table. - 3.

Key words: MAN-IN-THE-MIDDLE, INFORMATION AND COMMUNICATION SYSTEM, ENTERPRISES.

This master's qualification work is devoted to the study of information security issues in small and medium enterprises, in particular - the protection of information and communication system from attacks through intermediaries. The paper reviews the literature in the field of research. The researched material is systematized and the most common types of attacks that can be applied to information and communication systems of small and medium business are identified. In accordance with the studied risks, a new methodology for the protection of small and medium-sized enterprises has been developed, which does not require large costs, which allows its application even in those enterprises where there are no costs for information security specialists and purchase of special software to prevent attacks through intermediaries. . The developed methodology is flexible, which allows to use it in small and medium enterprises with different activities.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІКС – Кнформаційно-комунікаційна систма

MitM – Man in the middle

СБУ – Служба безпеки України

SSL – Secure Sockets Layer

ARP – Address Resolution Protocol

DNS – Domain Name System

ЗМІ – засоби масової інформації

TCP – Transmission Control Protocol

TLS – Transport Layer Security

UDP – User Datagram Protocol

AES – Advanced Encryption Standard

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

VPN – Virtual Private Network

ВСТУП

Роботу сучасних підприємств неможливо уявити без використання інформаційно–комунікаційних систем. Їх застосування значно спрощує можливість створення, редагування, аналіз, передавання та використання накопичених даних для ведення бізнесу. Однак якщо підприємства великого бізнесу зазвичай мають спеціалістів для забезпечення інформаційного захисту, то підприємства малого та середнього бізнесу можуть ігнорувати це, стаючи об’єктом злочинних посягань.

Проблема фінансування витрат для забезпечення інформаційної безпеки гостро стоїть в Україні. На підприємствах малого та середнього бізнесу в цілях економії ігнорують витрати для досягнення інформаційної безпеки, зокрема для захисту ІКС від атаки через посередника. Це робить їх легкою ціллю для зловмисників. Незахищеність підприємств малого та середнього бізнесу від кібератак шкодить не лише цим підприємствам, а і економічній та національній безпеці України в цілому.

Метою даної роботи є аналіз можливих ризиків, пов’язаних з використанням атаки через посередника та розробка методології попередження кібератак та захисту ІКС, яка не потребує великих фінансових затрат.

З поставленої мети випливають такі задачі дослідження:

- провести аналіз існуючих літературних джерел з досліджуваної області;
- дослідити найбільш поширені форми атак через посередника на підприємства малого та середнього бізнесу;
- розробити методологію захисту ІКС для підприємств, яка не потребує фінансових затрат на підприємстві;
- розробити гнучкі методичні рекомендації для працівників компаній, для підвищення рівня інформаційної безпеки;
- систематизувати та запропонувати набір інструментів для вирішення задачі захисту підприємств від атак через посередника.

Об'єкт дослідження є захищеність інформаційно–комунікаційних систем від атак через посередника.

Предметом дослідження є методи протидії кібератак через посередника та підвищення рівня захищеності систем на підприємствах малого та середнього бізнесу.

Наукова новизна даної роботи полягає в розробці методології захисту від MitM атак, яка не передбачає великих витрат на програмні засоби, що робить її доступною для впровадження на підприємствах малого та середнього бізнесу. Зокрема в роботі сформовано набір рекомендацій та комплексів програмних засобів для спеціалістів з інформаційної безпеки для захисту системи від різних форм атаки через посередника для захисту від атаки "Людина посередині" для підприємств малого та середнього бізнесу.

Практичне значення роботи полягає у можливості використання запропонованої методології захисту систем від атак через посередника на підприємствах малого та середнього бізнесу.

Апробація результатів роботи. Окремі результати доповідались на IX науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 8–9 грудня 2021 р.

1 ТЕОРЕТИЧНА ЧАСТИНА

1.1 Поняття атаки через посередника

В сучасному світі застосування інформаційних технологій широко впроваджене в повсякденне життя людей та роботу різних типів підприємств. Використання інформаційно–комунікаційних систем спрощує створення, обробку. Аналіз та використання великих масивів даних.

Однак використання ІКС дає можливість зловмисникам несанкціоновано впливати на інформацію, отримувати потрібні дані для незаконного використання, компрометування організацій, заволодіння фінансами, втручання в роботу структури або унеможливлення її роботи загалом, тощо.

Для реалізації інформаційних атак може бути використано різні методи. Одна з найпоширеніших типів атак, яка наразі існує, є MitM (англійскою Man in the middle) – атака через посередника [1]. Вона за поширенням поступається лише фішингу та шкідливому програмному забезпеченню, яке зайняло перше місце.

Атака через посередника – вид атаки при якій зловмисник перехоплює двосторонню транзакцію, стаючи між відправником та отримувачем даних. Таким чином зловмисник може здійснювати підміну даних, їх спаплюження, редагування. Це дає можливість використовувати дані у власних цілях, або ж шкодити відправнику чи отримувачу.

Ключова характерна риса цієї атаки полягає в тому, що ні відправник, ні отримувач даних не підозрює про існування сторонньої особи, яка може здійснювати несанкціоновані дії з інформацією.

Модель атаки через посередника можна побачити на рисунку 1.1, де відображений взаємозв’язок відправника, отримувача та зловмисника, який здійснює втручання в процес передачі інформації. Таким чином через сторонню особу проходить вся передана інформація.

Рисунок 1.1 – Модель атаки через посередника

Зловмисник може використовувати апаратні та програмні засоби для втручання в процес комутації. Найпростіший приклад реалізації атаки через посередника є пасивне прослуховування [2]. Перші перехоплення даних при передачі інформації з'явились ще до використання комп'ютерів. Яскравий приклад реалізації атаки – пасивне прослуховування телефонної розмови зі стаціонарних проводових телефонів. Якщо у будинку до однієї мережі підключено два і більше телефонів, то знявши трубку другого телефону під час розмови, можна чути розмову. Це і є приклад «людини посередині» без використання комп'ютерної техніки.

1.2 Аналіз предметної області дослідження

Відповідно до наукової термінології та діючого в Україні законодавства, до підприємств малого бізнесу відносяться новостворені та діючі підприємства з штатом працюючих осіб до 200 чоловік, якщо мова йде про підприємства промисловості та будівництва. В інших галузях підприємницької діяльності підприємство відноситься до малих у разі чисельності штату до 50 осіб. В галузях наукової та обслуговуючої сфери – до 100 чоловік. У галузях невиробничої сфери підприємство вважається малим з чисельністю працюючих

осіб до 25 чоловік. У роздрібній торгівлі – до 15 осіб [3]. Середні підприємства – це ті, які не можуть за своїми ознаками бути віднесені до малих чи великих підприємств.

В Україні існує чимала кількість зареєстрованих підприємств. За останніми даними, опублікованими Державною службою статистики, в Україні, станом на 1 листопада 2019 року, було зареєстровано 697 тис. діючих підприємств. З них понад 16 тис. відносяться до сфери інформації та телекомунікації [4].

Значна кількість підприємств, в яких немає належної системи захисту від кібератак зловмисників, стає жертвами зловмисників. Про це свідчать щорічні звіти Національної поліції України. Українські правоохоронці відмітили зростання кількості злочинів у кіберпросторі. За останніми даними у звіті «Національної поліції України про результати роботи у 2020 році» відмічають зростання кількості кіберзлочинів під час впровадження карантинних обмежень, коли більшість підприємств перейшли до роботи в онлайн–режимі [5]. Лише за рік роботи Департаменту кіберполіції було зареєстровано понад 5 тис. кіберзлочинів. Завдано матеріальних збитків на 241 мільйон гривень.

Про збільшення кількості кіберзлочинів свідчить і статистика звернень громадян. За 2020 рік на лінію call-центру кіберполіції України надійшло понад 100 тисяч дзвінків та понад 40 тисяч електронних звернень. Детальну статистику звіту роботи кіберполіції можна побачити на рисунку 1.2, де наведені дані за 2020–й рік.

Рисунок 1.2 – Кількість зареєстрованих кіберзлочинів у 2020–му році

Тому можна стверджувати, що рівень кіберзлочинності в Україні зростає. При цьому вартість розробки комплексу захисту ІКС є дороговартісним. Це потребує або звернення до спеціалізованих компаній, які надають послуги захисту інформаційно–комунікаційних систем, або оплата роботи спеціаліста з кіберзахисту, або придбання та налаштування дороговартісного програмного забезпечення. Через необхідність великих витрат, підприємці можуть ігнорувати необхідність витрат на захист. До того ж, в період 2020–2021 року фінансових труднощів підприємцям малого та середнього бізнесу додала пандемія COVID-19. Це загальносвітова проблема, яка вплинула на економіку в цілому. Від карантинних обмежень та локдауну постраждали представники бізнесу. У аналітичній роботі «Бізнес та COVID-19: вижити не можна померти» наводять статистичні дані – приблизно 74% підприємств має до 250 працівників та не відносяться до великих підприємств. Пандемія викликала значні фінансові труднощі у підприємств. 24% проаналізованих компаній вимушені зупинити роботу, 40% працюють лише частково, 20% перейшли до дистанційного формату роботи і лише 16% продовжували нормальну роботу [6]. Саме тому є необхідність розробки методології захисту, якими зможуть скористатися підприємці малого та середнього бізнесу. Ця методологія не повинна потребувати значних фінансових затрат, а її впровадження повинно бути можливим для усіх підприємців.

1.3 Обґрунтування необхідності захисту інформації на підприємствах

Важливість розробки методології захисту від MitM атак обумовлена не лише економічними факторами та ризиками втрати коштів, витоку важливої інформації та персональних даних на підприємствах. Законодавство в Україні чітко регулює необхідність створення таких умов при роботі підприємств, при яких буде забезпечено захист певних типів інформації.

Серед інформації, яка часто циркулює на підприємствах малого та середнього бізнесу, підлягає захисту персональна інформація. Це може бути база даних, в яких є персональні дані як клієнтів, так і співробітників. Необхідність захисту персональних даних регламентує Закон України «Про захист персональних даних». Ці дані можуть бути збережені в ІКС та використовуватися підприємством за згоди суб'єкта персональних даних.

Такі дані можуть належати до конфіденційної інформації і не можуть бути розголошені без згоди суб'єкта, який надав право на зберігання та обробку своїх персональних даних. Це зобов'язує власника ІКС створити такі умови, при яких ці дані не можуть потрапити до третіх осіб, не можуть бути розголошені. Крім заволодіння цими даними зловмисниками, вони повинні бути достовірними. Це регламентує пункт 2 статті 6 Закону «Про захист персональних даних». Тому інформація, яка циркулює в ІКС повинна бути захищена не лише від несанкціонованого розголошення чи видалення, а і редагування. Суб'єкту персональних даних Закон гарантує захист його персональних даних від незаконної обробки, випадкової втрати, знищення, тощо. Також суб'єкт має бути захищеним від розголошення недостовірних даних, які ганблять честь, гідність чи ділову репутацію фізичної особи [7].

Захист персональних даних повинні забезпечувати володільці чи розпорядники цих даних. Тому проблема створення захищеної ІКС, де зберігатимуться та оброблятимуться дані лягає на підприємців, що ці дані збиратимуть та використовуватимуть.

Крім персональних даних володільців, захисту підлягає і інші види інформації, зокрема наступні типи даних:

- службова інформація;
- відкрита інформація, що належить для державних інформресурсів;
- дані про суб’єкти владних повноважень;
- інформація, що становлять державну чи іншу передбачену Законом таємницю.

Вся відповідальність за забезпечення захисту інформації в ІКС лягає на керівника підприємства або його заступника. Це регламентує постанова Кабміну. При цьому розробка системи захисту може бути покладена і на одну людину. Оскільки на підприємствах малого та середнього бізнесу може не бути економічних можливостей створення окремої служби захисту інформації, може бути призначена одна особа [8]. Оскільки більшість підприємств малого та середнього бізнесу не розпоряджаються інформацією, що становить державну таємницю, процедура організації криптографічного захисту для них є спрощеною.

Оскільки атака через посередника можлива на етапі обміну інформації, важливо дотриматись основних властивостей інформації. Критерії захищеності при обміні інформації незахищеними каналами теж регламентуються нормативними документами, зокрема вони описані в «Критеріях оцінки захищеності інформації в комп'ютених системах від несанкціонованого доступу» Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ [9]. Так під час обміну даними повинно біти дотримано властивість інформації – конфіденційність. Існує чотири рівні забезпечення конфіденційності при обміну інформації:

- мінімальна;
- базова;
- повна;
- абсолютна.

Рівні обираються на підставі повноти захисту і вибірковості керування. Також обирається рівень цілісності інформації при обміні незахищеними каналами. Їх існує три:

– мінімальна;
– базова;
– повна.

Таким чином нормативні документи регламентують вимоги до підприємств, однак не надають практичних рекомендацій та методологій захисту для забезпечення виконання цих вимог. Тому нами було розроблено методологічні рекомендації для забезпечення захисту від атак через посередника на підприємствах малого та середнього бізнесу.

1.4 Аналіз перспективи розробки методології захисту від MitM атак

Розробка метододології захисту ІКС підприємств малого та середнього бізнесу дозволить вирішити одразу кілька задач. Головна з них – забезпечення захисту від однієї з найпоширеніших видів атак на підприємствах, що не можуть забезпечити повноцінний контроль та захист підприємства.

Створення універсальної методології дозволить застосовувати її на підприємствах різної спеціалізації. Передусім там, де є циркуляція персональних даних, що потребують захисту. Це підприємства оптової та роздрібної торгівлі, інформації та телекомунікації, фінансової та страхової діяльності, операцій з нерухомим майном, діяльності в сфері адміністрування та допоміжного обслуговування, професійної, наукової та технічної діяльності, охорони здоров’я та надання соціальної допомоги, надання інших видів послуг.

1.5 Висновки до першого розділу

На даний час невелика кількість українських компаній витрачає достатньо зусиль та фінансів для забеспечення досконалого захисту від можливих кібератак та загроз, пов’язаних з MitM атаками. Переважно це

стосується лише підприємств великого бізнесу, державних організацій. Підприємства малого та середнього бізнесу залишаються недостатньо захищеними, або ж такий захист формальний для дотримання чинного законодавства. Це становить загрозу не лише для конкретних компаній, а і для держав в цілому, оскільки основну частину надходжень до державного та місцевих бюджетів забезпечують саме представники малого та середнього бізнесу.

В даний час розроблені вимоги до підприємств щодо забезпечення захисту, однак немає загальних рекомендацій для підприємців, які б допомогли виконати вимоги до інформаційної безпеки. Це стає причиною високого рівня кіберзлочинності.

2. АНАЛІТИЧНА ЧАСТИНА

2.1 Аналіз форм атак через посередника

Атака через посередника не є точним, чітким та єдиним методом реалізації атаки. Це поняття яке передає суть порушення конфіденційності, цілісності та доступності інформації. Проаналізувавши джерела [10-13] було досліджено найбільш поширені типи даної атаки. Кожен тип атаки використовує певні вразливості та способи незаконного перехоплення та роботи з інформації. Так на підприємствах малого та середнього бізнесу найбільш ризикованим та імовірним типом атаки через посередника може бути «прослуховування по Wi-Fi». Цей тип атаки може бути використаний як проти працівників компанії, так і проти її клієнтів.

Ще один поширений спосіб реалізації атаки – перехоплення електронної пошти. Ця атака частіше направлена саме на працівників підприємства, а не на їх клієнтів. Методом соціальної інженерії чи спам–розсилки зловмисник може увійти в довіру користувача системи і використати це для реалізації атаки.

Підміна або маскування протоколу ресурсу HTTPS використовується для реалізації фішингових сайтів, на які можуть помилково або цілеспрямовано увійти користувачі мережі. Для направлення на підроблений сайт можна використати уже вищевказаний метод перехоплення електронної пошти.

Також можуть бути використані і інші типи реалізації атаки через посередника. Зокрема в ході аналізу виділено наступні:

- прослуховування по Wi-Fi;
- перехоплення електронної пошти;
- підміна HTTPS;
- підміна IP-адреси;
- підміна ARP;
- підміна DNS.

2.1.1 Аналіз прослуховування по Wi-Fi

Даний тип реалізації атаки може бути використаний як проти працівників підприємства, так і проти клієнтів. Цю атаку називають «атакою злого близнюка» [12]. Її суть полягає не у використанні вразливостей існуючої безпроводової мережі, а створення нового клону. Для цього необхідно створити нову точку доступу до мережі і обрати назву для неї співзвучну з назвою підприємства. Після цього необхідно дочекатися, доки до мережі почнуть підключатися користувачі.

Ця атака в першу чергу буде розрахована на клієнтів підприємств малого та середнього бізнесу, де клієнти проводять час в очікуванні чи черзі. До прикладу, клон реальної мережі Wi-Fi може бути створено зловмисником на таких підприємствах:

- заклади громадського харчування;
- магазини продовольчих та непродовольчих товарів;
- салони краси;
- автомайстерні;
- агенції надання послуг населенню;
- вуличні кіоски, тощо.

Оскільки в цих місцях клієнти можуть тривалий час очікувати на замовлення, чекати на свою чергу або відпочивати, є велика імовірність того, що клієнт помилково підключиться до точки мережі зловмисника. Такий метод особливо ефективний в тих закладах, де справжня точка доступу для клієнтів недоступна через пароль або точка доступу до безпроводової мережі взагалі відсутня, тому користувачі сприймають клон як справжню точку доступу.

Навіть працівники підприємства можуть бути в зоні ризику, якщо їх пристрої налаштовані на автопідключення до мережі Wi-Fi. Або ж працівник може помилково обрати мережу зловмисника.

Результат підключення до клону точки доступу може бути реалізація атаки з відключенням SSL, щоб змусити користувачів проходити через незашифровані версії веб–ресурсів або ж вони можуть організувати захоплення

DNS, що перенаправляти користувачів на фішингові версії порталів та ресурсів, до яких вони намагаються підключитися.

Під час передавання інформації по каналам зв'язку можливе її перехоплення. В такому випадку можлива реалізація аналізу трафіку, нав'язування користувачам помилкової інформації, порушення інформаційного обміну, маскування під зареєстрованого користувача або запит системи, тощо[14].

2.1.2 Аналіз можливості перехоплення електронної пошти

Завдяки перехопленню електронної пошти також можуть бути реалізовані атаки через посередника. Суть цієї атаки полягає в тому, що зловмисник (спамер) розсилає користувачам листи на електронну пошту, яка має адресу авторитетного користувача чи компанії. В листі можуть бути вказані інструкції та посилання на фішингові ресурси. Також зловмисник може в листі виманити у користувача важливі дані, змусити виконати фінансові операції чи заразити пристрій шкідливим програмним забезпеченням.

Проаналізувавши повідомлення у ЗМІ, ця форма атаки виявилась однією з найбільш поширених, від яких страждають підприємства малого та середнього бізнесу, що не мають достатнього захисту. Так лише від однієї атаки з використанням корпоративної електронної пошти Microsoft у березні 2021 року постраждали понад 60 тис. компаній. Жертвами стали як великі організації, так і підприємства малого та середнього бізнесу [14].

В Україні на початку грудня 2020–го року сталась масова кібератака на користувачів через електронну пошту. Користувачі отримали листи ніби від компанії «Укрпошта». В листі йшлося про необхідність сплати додаткового мита у розмірі 2,15 гривень, щоб отримати міжнародне відправлення [15]. Посилання у листі відправляло користувачів на фішінговий сайт, стилізований під вигляд компанії. Метою шахраїв було не заволодіння вказаною сумою, а банківськими реквізитами.

2.1.3 Аналіз можливості підміни HTTPS

Протокол HTTPS є основним елементом сучасних веб–комунікацій, оскільки він забезпечує високий рівень безпеки. При цьому використовується надійна криптографія TLS.

Проте підміна HTTPS використовується кіберзлочинцями для реалізації атаки через посередника. Суть цього методу полягає у створенні копії домену авторитетного ресурсу чи сайту.

Інша назва цієї атаки – атака на омографію. Зловмисник створюючи копію ресурсу повинен не лише відтворити зовнішній вигляд та функціонал справжнього ресурсу, а і відтворити домен сайту, щоб він був максимально схожий або ідентичний з вигляду на справжній. Це можна досягнути завдяки заміні одного символу домену, на ідентичний або схожий в таблиці ASCII.

В ході виконання магістерської роботи було досліджено можливість підміни латинських літер на ідентичні літери кирилиці. Ці комбінації приведено в таблиці 2.1 з вказанням символу, порядковим номером в таблиці ASCII в десятковому та шістнадцятковому форматі

Таблиця 2.1 – Символи ідентичні в латиниці та кирилиці в таблиці ASCII

Ідентичний символ	Десятковий код символу в латиниці	Шітнацятковий код символу латиниці	Десятковий код символу кирилиці	Шітнацятковий код символу кирилиці
A	65	41	128	80
B	66	42	130	82
C	67	43	145	91
E	69	45	133	85
H	72	48	141	8D
I	73	49	178	B2
K	75	4B	138	8A
M	77	4D	140	8C
O	79	4F	142	8E

Продовження таблиці 2.1

P	80	50	144	90
T	84	54	146	92
X	88	58	149	95
a	97	61	160	A0
c	99	63	225	E1
e	101	65	165	A5
i	105	69	179	B3
o	111	6F	174	AE
p	112	70	240	F0
y	121	79	227	E3

Таким чином є 19 ідентичних великих та малих літер у латиниці та кирилиці, які мають різні коли в системі ASCII, що дозволяє використати це для реалізації підміни HTTPS, створюючи клон домену, який буде ідентичним справжньому.

В результаті, коли людина почала взаємодіяти з клоном веб–сайту, вона стає жертвою MitM атаки, не усвідомлюючи, що вона передає інформацію зловмиснику.

Дослідником інформаційної безпеки Сюдун Чженом було доведено, що механізми захисту омографа в розповсюджених браузерах Chrome, Firefox, Opera не працюють, якщо кожен символ домену можна замінити аналогічним символом іноземної мови [16]. Так на прикладі домену «apple.com» дослідник довів можливість реалізації атаки, замінивши символи латиниці на кирилицю.

Тому ця особливість становить реальну загрозу не лише для звичайних користувачів, а і для підприємств малого та середнього бізнесу, які вимушені використовувати різні ресурси та здійснювати з їх допомогою передачу даних, фінансові операції, облікові операції, тощо.

2.1.4 Аналіз можливості підміни IP-адреси

Кожний пристрій має адресу інтернет протоколу. Завдяки підміні IP-адреси, ще цей тип атаки носить назву IP-спуфінг, зловмисник може змісити думати жертву, що вона обмінюється даними з веб–сайтом або знайомою людино. Так жертва надає дані злочинцю.

Даний метод використовують в цільових атаках. Зловмисник модифікує дані адреси відправника в IP–пакеті.

Протокол транспортного рівня TCP має вбудований механізм захисту від підміни. Однак протокол UDP є вразливим до механізму атаки [17].

Візуалізація підміни IP-адреси зображена на рисунку 2.1.

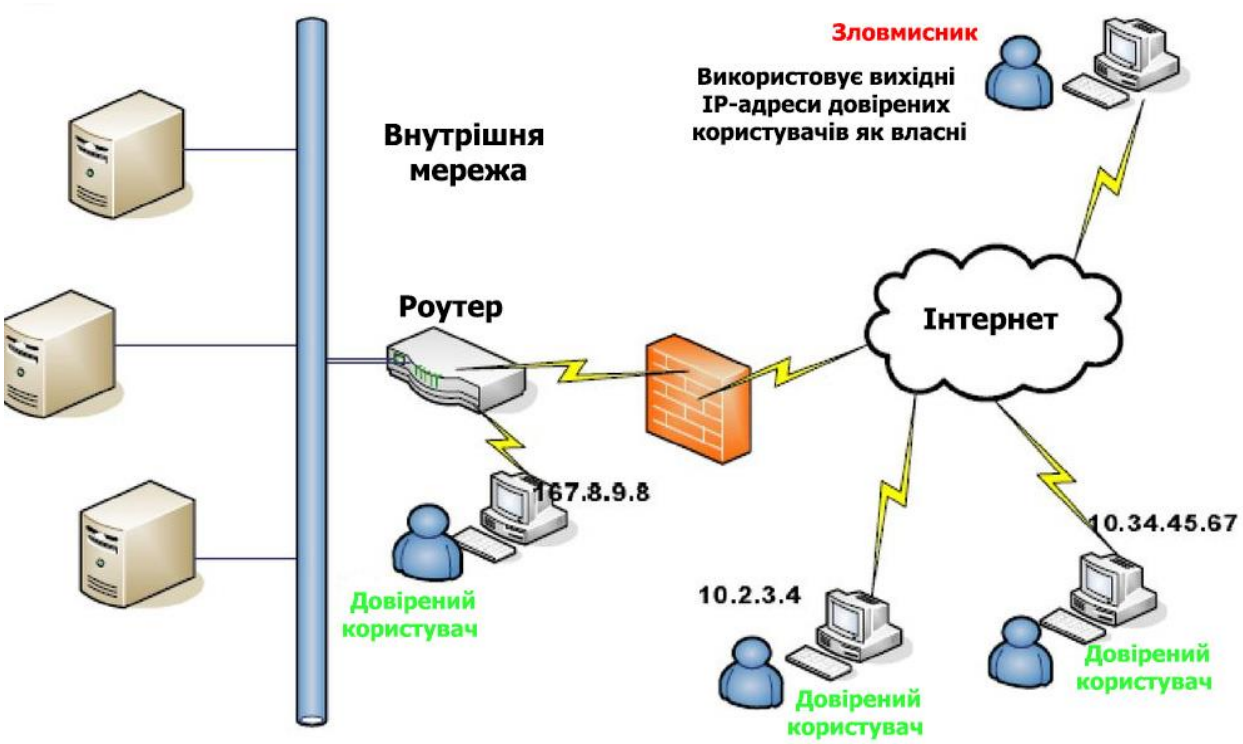

Рисунок 2.1 – Візуалізація підміни IP-адреси

На відміну від інших атак, зловмисники використовують IP-спуфінг направлено проти конкретного користувача. В інших же випадках атаки спрямовані на цілий ряд можливих користувачів.

2.2 Дослідження програмних засобів для реалізації MitM атак

Для реалізації атаки через посередника не потрібно розробляти нове програмне забезпечення чи утиліти. Існує чимала кількість готових програмних продуктів для реалізації MitM атак. Нами було досліджено програмні рішення для виконання атаки.

Оскілки ці програмні продукти вже готові та доступні, кожен користувач, може завантажити його та використати в злочинних цілях. І хоча реалізація кібератак може тягнути за собою кримінальну відповідальність, існують ризики, використання цих програм. Тому під загрозою опиняються підприємства малого та середнього бізнесу, які не оснащені методологією захисту та відповідним програмним забезпеченням від атак через посередника.

MITMf – фреймворк для реалізації атаки через посередника. Його додано в склад Kali Linux. Фреймворк побудовано на базі sergio-proxy. З його допомогою можна відстежувати спроби логіну для різних протоколів. Дозволяє виконати атаку «отруєння кешу». Дозволяє підмінити файли, які відправлено через HTTP протокол. Дозволяє впроваджувати контент в HTML-сторінку [18].

KARMA – це набір інструментів, який дозволяє здійснювати ряд операцій в безпроводових мережах. Інструменти дозволяють пасивно прослуховувати запити. Також можна виявляти користувачів. Завдяки інструмента може бути реалізована атака прослуховування по Wi-Fi [19]. Зловмисник може створити власну точку доступу та перенаправити на неї користувачів мережі за допомогою автопідключення. Можна створити копію точки доступу та під’єднати до неї користувачів.

Intercepter-NG – інструмент має великий функціонал, серед якого є інструменти для реалізації MitM атак. Він дозволяє здійснювати DNS/NBNS/LLMNR-спуфінг. З допомогою інструменту можна здійснювати ARP-спуфінг – різновид мережевої атаки тиму MitM, з використанням ytljksrsd ARP-протоколу. Застосувати його можна в мережах Ethernet [20].

The Middler – утиліта для проведення атаки через посередника. Вона дозволяє атакувати різна протоколи. З допомогою засобу можна моніторити мережевий трафік. Ця утиліта є максимально автоматизована і не потребує особливих знань та управління зловмисником. Цю утиліту можна використати для крадіжки cookies-файлів та самостійно витягувати їх з боку клієнта. Утиліта допомагає збирати акаунти комп'ютерної мережі [21].

Це лише деякі утиліти, використання яких може допомогти реалізувати атаку через посередника. Недоліком даних утиліт є те, що вони розраховані на незахищені системи або на менш актуальні протоколи, зокрема – HTTP. Протокол HTTPS з допомогою описаних утиліт атакувати не вдасться, оскільки він є більш захищеним і стійким.

2.3 Аналіз платних інструментів для запобігання реалізації MitM–атак

Для захисту ІКС підприємств можна використовувати спеціалізовані програмні засоби. В ході роботи було проаналізовано існуючі платні програмні засоби. У таблиці 2.3 наведено перелік програмних засобів, аргументація необхідності їх використання та актуальна вартість користування.

Таблиця 2.3 Рекомендації щодо використання платних програмних засобів для захисту від MitM атак

Назва інструменту	Обгрунтування необхідності використання	Вартість користування
KasperskyTotal Security	Має набір засобів для захисту від атак через посередника	$30/рік (2 пристрої)
KasperskyInternet Security	Дозволяє маскувати IP–адресу та запобігає окремим атакам через посередника	$18/рік (1 пристрій)
UnHackMe PRO	Дозволяє виявляти руткіти та шкідливе ПЗ, яке використовується для реалізації MitM	$99.95 назавжди (5

	атак	пристроїв)

Продовження таблиці 2.3

CyberGhost	Дозволяє використовувати VPN, знижуючи ризики застосування MitM атаки. Використання AES-шифрування	$47/рік (1 обліковий запис)
Hushmail	Засіб для відправки електронної пошти з допомогою PGP через захищений сервер, що унеможливлює перехоплення.	$50/рік (1 обліковий запис)

Однак необхідність оплати для користування даними програмними засобами може стримувати підприємців. Вартість даних засобів сумарно становить 245 доларів, варто вараховувати, що окремі засоби розраховані лише на один пристрій. Тому якщо підприємство має не один пристрій який необхідно захистити, це може стати фактором стримування для керівників та власників. Саме тому є необхідність у безкоштовній альтернативі для підприємств малого та середнього бізнесу.

2.4 Висновки до другого розділу

Виходячи з проаналізованого матеріалу можна стверджувати, що реалізація MitM не потребує значних навичок та знань з боку зловмисника. Це можна досягнути завдяки уже існуючим утилітам, які є у вільному доступі. Більшість з них використовуються для аналізу або перевірки захисту мережі. Однак в руках зловмисників вони стають інструментом реалізації MitM атак.

Підприємства малого та середнього бізнесу часто можуть ставати об'єктами атаки через необдумані дії працівників, які не проінформовані про можливі ризики.

Об'єктом злочинних посягань можуть бути не лише підприємства малого та середнього бізнесу, а і їх клієнти, які користуються бездротовою мережею. З допомогою відповідних інструментів можливе створення клонів точок доступу

та під'єднання до них користувачів. Таким чином зловмисники можуть виконувати потрібні дії для одержання потрібних даних, акаунтів користувачів, крадіжки cookies-файлів, перенаправлення користувачів на фішингові сайти, тощо.

3 ПРАКТИЧНА ЧАСТИНА

3.1 Розробка методології захисту від MitM атак

Під час аналізу можливих способів реалізації атаки через посередника та дослідження прикладів зафіксованих масових атак можна зробити висновок, що підприємства малого та середнього бізнесу можуть страждати від кібератак. Кібербезпека підприємств малого та середнього бізнесу тісно пов'язана з економічною безпекою.

Економічна безпека на підприємствах може вказати на рівень безпеки господарських відносин з зовнішніми контрагентами. Це взаємодія з іншими організаціями, постачальниками, кредиторами, партнерами, інвесторами, тощо. Завдання шкоди економічній безпеці впливає і на інших суб'єктів співпраці з підприємством. До того ж, така безпека є складовим елементом національної безпеки в економічній сфері [22]. Тому необхідно максимально виключити можливість злочинного втручання та шкоди підприємству з боку кіберзлочинців. Це дозволяє зберегти фінанси компанії, довіру та співпрацю з її партнерами. Водночас, запропонована методологія не може бути дороговартісною, та повинна бути доступною будь–якому підприємству, навіть з мінімальним капіталом, де не передбачені витрати на реалізацію захисту ІКС від можливих кібератак.

Таким чином було проведено аналіз найбільш актуальних методів реалізації атак MitM та запропоновано алгоритм запобігання їх реалізації.

Запропоновані методи захисту ІКС від атак через посередника у розділі 3.1.1 – 3.1.4 можуть бути використані відповідальною за інформаційну безпеку на підприємстві особою або керівником. Переваго наведених методів є їх дешевизна та відсутність необхідності значних затрат для налаштування системи захисту від атак через посередника, що вкрай важливо для підприємств малого та середнього бізнесу.

У підрозділі 3.2 було проведено порівняльний аналіз сучасного антивіросного програмного забезпечення та програмних продуктів, які використовуються для захисту від атак через посередника.

У розділі 3.3, на основі проаналізованої інформації та складеної методології було запропоновано методичні рекомендації для працівників підпиємств малого та середнього бізнесу для підвищення їх знань у сфері інформаційної безпеки та підвищення рівня захисту підприємства, оскільки працівники зможуть мати чіткі рекомендації щодо роботи з ІКС.

3.1.1 Захист Wi-Fi мережі від методів атаки посередника

Оскільки безпроводовою мережею можуть користуватися як працівники, так і клієнти підприємства, існують ризики перехоплення файлів під час їх передачі або створення клону мережі. За допомогою радіопередатчика зловмисник може створювати радіошум для заглушки Wi-Fi сигналу та відключення користувачів від точки доступу до мережі. Після цього зловмисник створює фіктивну точку доступу з такою ж адресою для перепідключення користувачів і використовує це в своїх цілях.

Створення «глушилки» для сигналу можливе не лише з допомогою використання дороговартісного обладнання чи карт USRP, а і недорогих Wi-Fi адаптерів. Для виготовлення таких глушилок використовують чіпи TP-Link WN722N, AWUS036NHA и WNDA3200 [23].

Для захисту від даної типи атаку необхідно залишити в мережі лише підтримку протоколу AES-CCMP. Стандарт шифрування AES є одним з найбільш безпечних методів шифрування даних. Для налаштування протоколу CCMP необхідно переконатися, що пристрої та точки доступу підтримують AES та CCMP (CBC-MAC) на апаратному рівні. Переважна більшість сучасних пристроїв підтримує дані алгоритми.

Налаштувати мережу можливо без особливих навичок. Для цього необхідно перейти до налаштування точки доступу до мережі. Порядок дій для налаштування протоколу залежатиме від конкретного пристрою.

Задля запобігання автоматичного перепідключення пристроїв мережі до можливого клону мережі зловмисника, необхідно провести налаштування корпоративних та приватних пристроїв працівників компанії:

- песональні комп'ютери;
- ноутбуки;
- планшетні ком'пютери;
- смартфони;
- периферійні пристрої з підключенням через Wi-Fi;
- будь-яка техніка, яка підключена до Wi-Fi мережі.

Всі перелічені пристрої необхідно налаштувати таким чином, заборонивши автоматичне підключення дл загальнодоступним точкам доступу.

Для унеможливлення зміни налаштування безпроводової точки доступа умисно зловмисником або неумисно працівником підприємства, необхідно встановити надійний пароль для доступу до точки доступу. Пароль повинен містити щонайменше шість символів. Необхідно використовувати літери, цифри та спецсимволи. Пароль не повинен бути словом, тим паче, пов'язаним з родом діяльності підприємства. Це підвищує стійкість паролю до атаки методом перебору та виключає атаку по словнику. Також паролі не повинні зберігатися в доступних файлах, сценаріях автоматичної реєстрації. До них не повинні мати доступ неуповноважені особи [24].

3.1.2 Методологія захисту від перехоплення електронної пошти

Оскільки підприємства малого та середнього бізнесу ризикують бути уражені атаками за допомогою підміни електронної пошти, необхідно використовувати засоби захисту від даного типу атаки.

Існують вже готові програмні рішення для реалізації захисту електронно пошти. На ПК підприємств можна використовувати програму PGP Desktop от Symantec. Вона дозволяє виконати асиметричне шифрування з використанням відкритого та приватного ключа. Програмний засіб дозволяє виявляти трафік поштового клієнта і шифрує відправлені повідомлення. Для захисту з

допомогою програмного засобу задається використовувана пошта та SMTP/POP/IMAP [25].

Для захисту від клонів електронної пошти авторитетних користувачів та компаній запропоновано використовувати для роботи з електронними листами віртуальні машини. Це дозволить запобігти зараження комп'ютера шкідливим ПЗ. На віртуальні машині для забезпечення захисту не можна зберігати важливу інформацію, яка буде представляти цінність. Навіть якщо зловмисники використають спам-розсилку для того, щоб впровадити на комп'ютері жертви шкідливе ПЗ, це не вплине на ІКС підприємства. У разі виявлення атаки, віртуальну машину можна буде видалити та створити нову.

Для економії коштів підприємством малого чи середнього бізнесу можна використовувати безкоштовне програмне забезпечення для створення віртуальних машин. Серед найбільш поширених та простих у використанні безкоштовних програм можна виділити:

- Oracle Virtualbox.
- Microsoft Hyper-V.
- VMware Workstation Player.

3.1.3 Методологія захисту від підміни HTTPS

Атака на омографію передбачає створення фішингового ресурсу з схожим або ідентичним ресурсом. Оскільки зловмисники можуть за допомогою спам–розсилки або методами соціальної інженерії можуть змусити працівника підприємства малого або середнього бізнесу перейти на фішинговий сайт та ввести важливі дані, необхідно запобігти цьому.

Одна з головних проблем, через яку цю атаку вдається реалізувати – людський фактор. Працівник може бути необізнаним про цю загрозу або бути переконаним, що виконує є певні її на авторитетному ресурсі, а не на клоні сайту злочинця. Сам тому необхідно мінімізувати цю можливість.

Щоб захистити ІКС від даної атаки необхідно використовувати захищені браузери які повинні вчасно та регулярно оновлюватися. Сучасні браузери

можуть виявляти спробу реалізації атаки на омографію та попереджувати про це користувача.

Для більш надійного захисту можна використовувати спеціальні програмні засоби та розширення, які можуть виявляти та блокувати даний тип атаки.

За результатами аналізу сервісу StatCounter за 2020-й рік, було проаналізовано понад 15 млрд переглядів на 3 млн сайтів. Відповідно, стало відомо, які веб-браузери є найбільш популярними. Лідером є браузер Chrome – близько 66% користувачів [26]. Однак в Україні цей показник значно вищий. Він у 2019–му році становив понад 73% [27].

Для захисту браузера можна використати спеціальне розширення. Для Chrome було розроблене розширення PhishProtect Beta, яким користується понад 20 тис. користувачів. Воно виконує аналіз усіх доменів, де використовуються нестандартні символи. При переході на такий ресурс розширення заблокує його та попередить користувача про це. На рисунку 3.1 зображено вигляд сторінки браузера при переході на фішинговий ресурс, який використовує атаку на омографію.

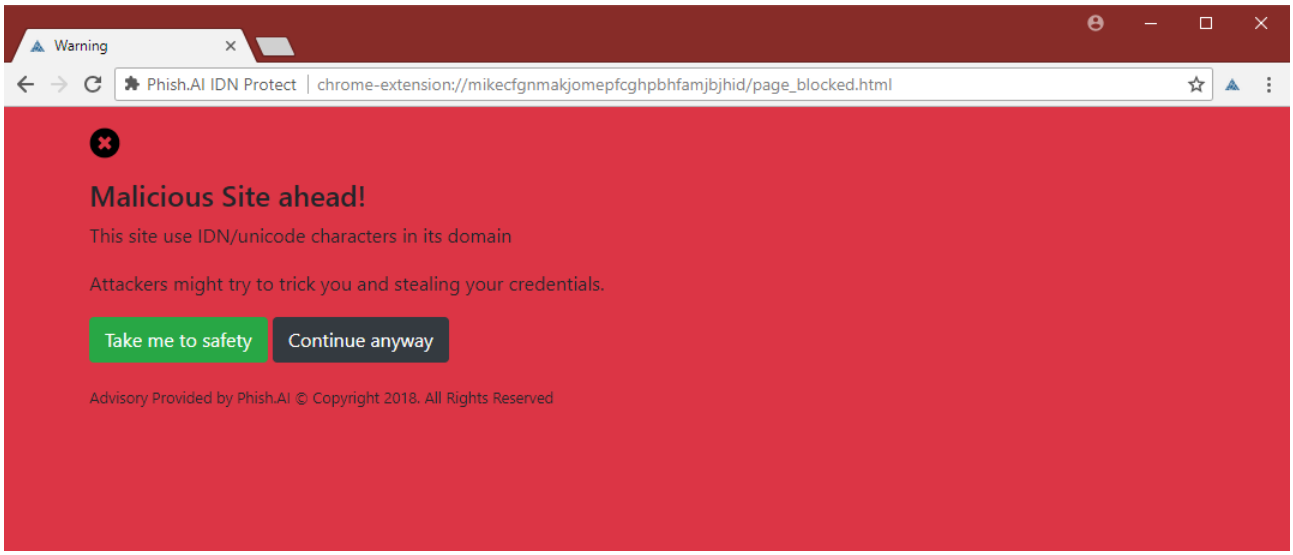

Рисунок 3.1 – Попередження про омографічну атаку на сторінці браузера

Тому такий метод може бути найбільш ефективний на підприємствах малого та середнього бізнесу, оскільки це не потребує затрат на програмне забезпечення

та виключає фактор людської помилки чи неуважності при переході за посиланнями на фішингові ресурси.

3.1.4 Розробка захисту від підміни IP-адреси

Захист від даного типу атаки потребує комплекс заходів. Це дозволить зменшити ризики реалізації даного типу атаки на підприємстві. Оскільки мова йде саме про підприємства малого та середнього бізнесу, де бюджет на інформаційний захист системи обмежений або взагалі відсутній, використання підтримки з боку аналітиків з кібербезпеки чи платного програмного забезпечення не розглядається. Запропоновано використання загальнодоступних та безкоштовних методів захисту.

Задля збільшення захищеності необхідно використовувати VPN (віртуальної приватної мережі). Це дасть перевагу для забезпечення інформаційного захисту. В першу чергу завдяки тому, що VPN маскує IP-адресу, передаючи його через приватні сервери. Це значно ускладнює роботу зловмиснику, який має намір здійснити атаку через посередника методом підміни IP-адреси.

Ще одна перевага використання VPN – можливість захистити ваш трафік між пристроєм та VPN-шлюзом. Це не дозволить інтернет–провайдеру або будь-яким третім особам, включаючи спецслужби, виконувати атаку через посередника. Націлену на підприємство [28].

Ще один спосіб захисту від даного методу реалізації атаки через посередника є використання спеціального програмного забезпечення для виявлення підміни:

- NetCut.
- Arp Monitor.
- Arpwatc.

Також для захисту від підміни IP–адреси варто використовувати безпечні протоколи зв’язку HTTPS та FTPS. Перевірка структури домену користувачем є одним з ефективних методів запобігання атаки через посередника. Варто

переконатися, що ресурс використовує протокол HTTPS, а не HTTP. Наразі всі авторитетні ресурси мають використовують саме HTTPS протокол. Використання протоколу HTTP на ресурсах, де необхідно вказувати або передавати дані повинно насторожувати користувача. Це може бути ознакою фішингового сайту.

3.2 Рекомендації щодо вибору набору інструментів захисту

Оскільки бюджет для забезпечення інформаційної безпеки на підприємствах малого та середнього бізнесу може бути обмежений або взагалі відсутній, було розроблено рекомендації щодо вибору безкоштовного програмного забезпечення, яке використовується для протидії MITM атак.

В першу чергу проаналізовано [29-33] та запропоновано набір безкоштовних інструментів, які можуть бути використані на підприємствах малого та середнього бізнесу ці дані наведено у таблиці 3.2.

Таблиця 3.1 – Рекомендації щодо використання безкоштовних програмних засобів для захисту від MitM атак

Назва інструменту	Обгрунтування необхідності використання	Вартість користування
Avira Free Antivirus	Функціонал дає можливість зменшити ризик реалізації MITM атак	Безкоштовно
UnHackMe	Дозволяє виявляти руткіти та шкідливе ПЗ, яке використовується для реалізації MitM атак	Безкоштовно
Proton VPN	Дозволяє використовувати VPN, знижуючи ризики застосування MitM атаки. Використання AES-шифрування	Безкоштовно
Oracle Virtualbox	Можливість створення віртуальної машини для безпечної роботи та захисту інформації на ПК працівників	Безкоштовно

Продовження таблиці 3.1

SecureGmail	Плагін в Chrome який використовує симетричне шифрування для захисту електронної пошти, що зменшує ризики реалізації атаки	Безкоштовно

Використовуючи підібраний набір інструментів можна досягнути максимального рівня захисту системи від різних форм атак через посередника.

3.3 Практична спроба запобігання реалізації MitM атак

Ефективність запропонованих безкоштовних програмних засобів було перевірено. За допомогою відповідного програмного забезпечення було реалізовано спроби різних форм атак через посередника. Кожне дослідження проводилося в два етапи. На першому етапі спроба атаки проводилась на пристрої, на якому не встановлено відповідного програмного забезпечення. Вдруге атака була проведена на пристрій, де вже встановлено програмні засоби, призначені для захисту.

3.3.1 Спроба встановлення шкідливого ПЗ для реалізації MitM атаки

Для спроби реалізації MitM атаки було проведено експеримент зі встановленням шклідливого програмного забезпечення на ком’пютер жертви. Для цього використано замаскований .exe файл шкідливого програмного забезпечення. Програма створена на базі існуючої програми для дистанційного керування ПК – RMS Viewer. На відміну від звичайного файлу хоста програми, який можна завантажити та встановити для контролю та управлінням ПК, замаскований файл не подає сигналу користувачу, що над пристроєм здійснюється контроль.

Після запуску шкідливого ПЗ відбувається встановлення хосту програми у фоновому режимі на комп'ютері жертви. Файли хосту встановлюються у новостровеній папці «Windows Files x62» на системному диску пристрою.

Назва папки обумовлена тим, що користувач, побачивши назву операційної системи, не наважиться її видаляти, оскільки вважатиме, що це системні файли і їх видалення негативно вплине на роботу операційної системи.

На першому етапі експерименту на комп’ютері не було встановлено антивірусного програмного забезпечення, окрім базового Windows Defender. Після натискання установочного файлу програма була встановлена у фоновому режимі. При цьому жодних випливаючих вікон не з'явилося. Базовий захисник Windows ніяк не відреагував на програму під час її перенесення на комп'ютер та встановлення шкідливого ПЗ. На рисунку 3.1 зображений вигляд папки з файлами встановленого хосту без відома користувача.

Рисунок 3.1 – вміст папки

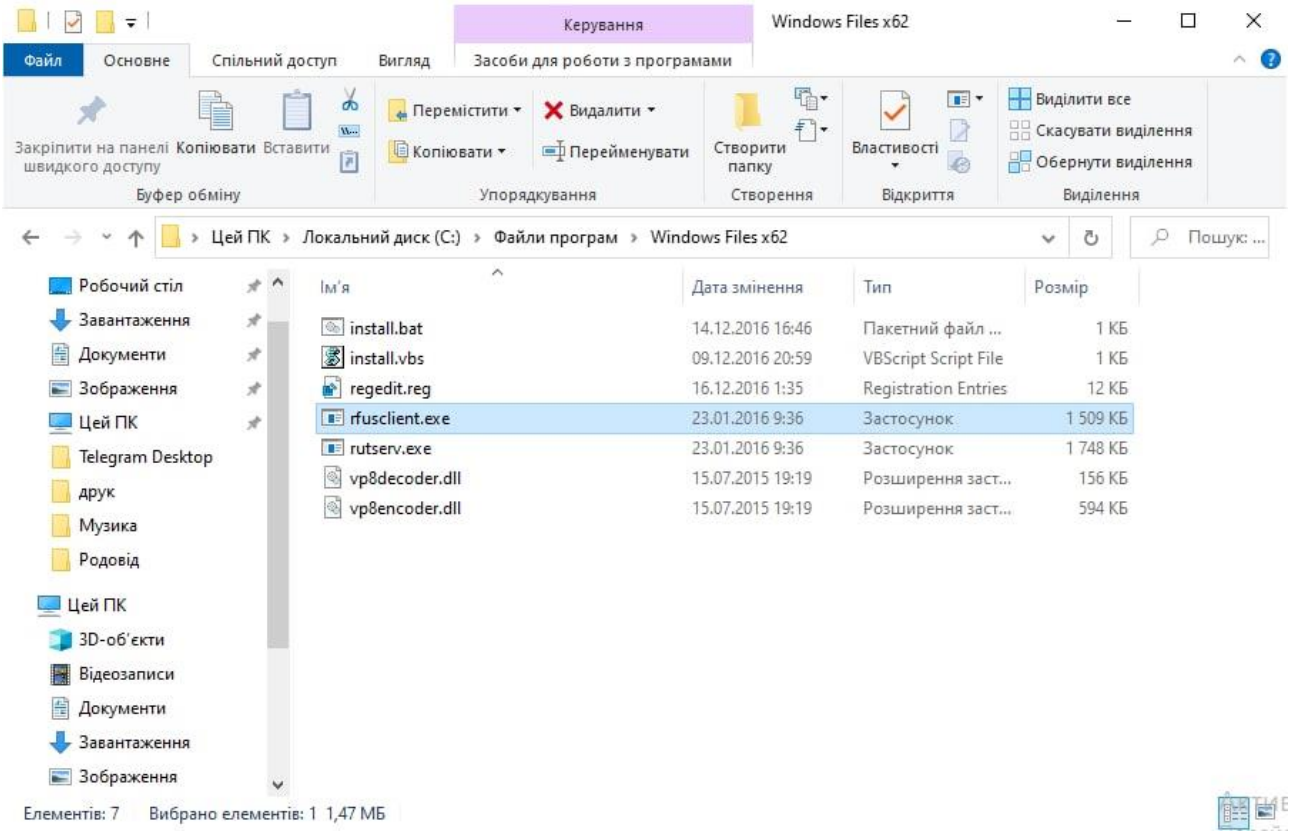

Рисунок 3.1 – Папки з файлами встановленого хосту без відома користувача

На іншому комп’ютері імовірного зловмисника за допомогою програми управління пристроями вдалося підключитися до комп’ютера жертви. При цьому на комп’ютері жертви жодних ознак вторгнення помітно не було. Базове антиврусне програмне забезпечення також не виявило загрозу.

Функціонал програми RMS включає в себе:

– повний контроль над периферичними пристроям;
– пасивний перегляд робочого столу жертви;
– обмін файлами;
– вивід на екран необхідних повідомлень;
– доступ до терміналу;
– контроль диспетчером завдань;
– можливість блокування екрану та доступу до пристрою користувачу.

Фактично, зловмисник може використати цей функціонал для будь–яких цілей – пасивного перегляду важливих переписок між працівником підприємства, перегляд введених конфіденційних даних, перехоплення важливої інформації, відправки листів від імені організації, встановлення іншого шкідливого ПЗ, тощо. Загальний вигляд робочого вікна зображено на рисунку 3.2. На ньому можна побачити доступний пристрій (заражений ПК).

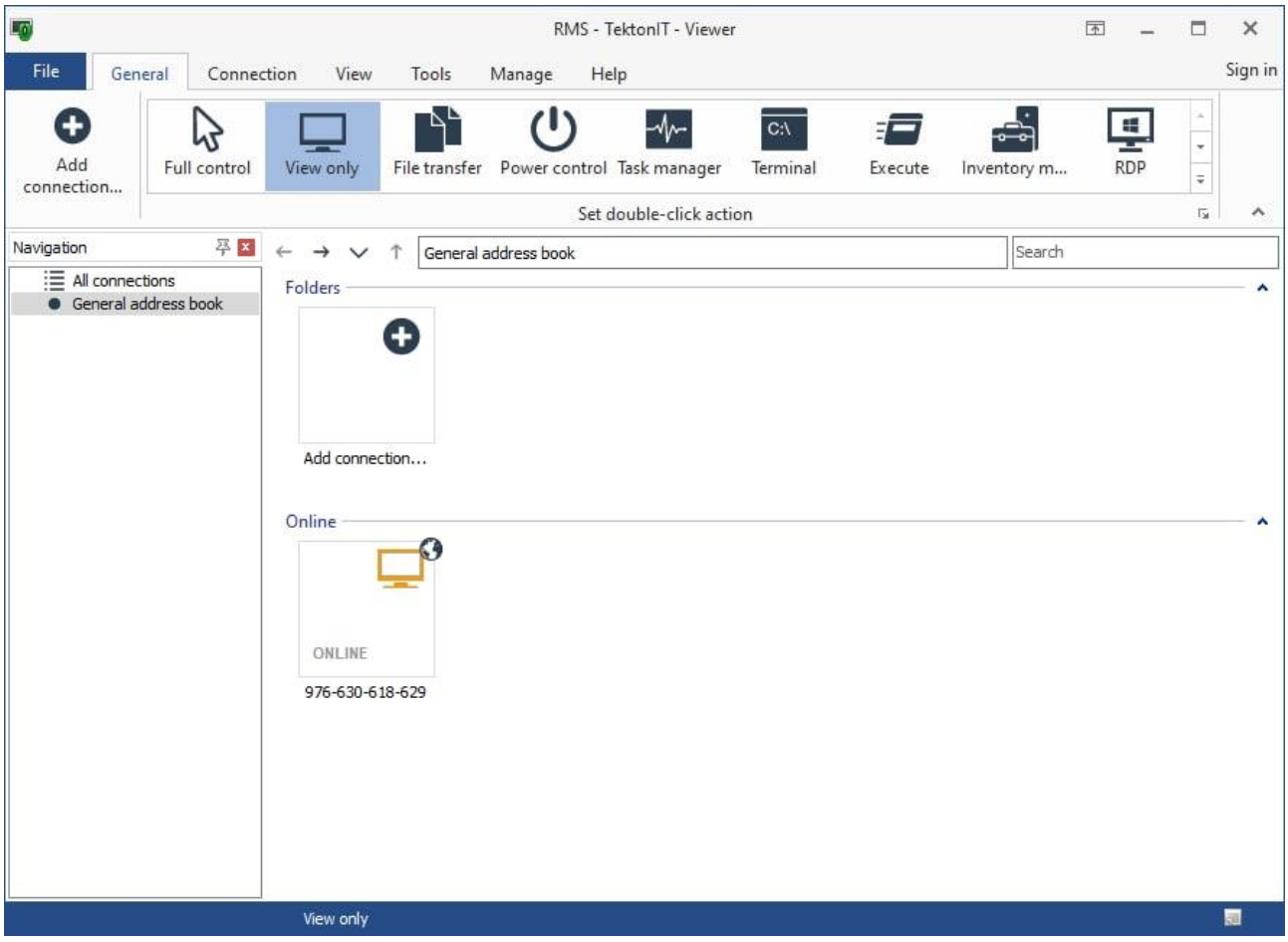

Рисунок 3.2 – Загальний вигляд програми управління RMS

Наступним кроком була спроба викликати командну стічку та виконати комнду ipconfig. Результат виконання можна побачити на рисунку 3.3. При цьому на комп’ютері жертви не відбулося жодних змін – не з’явилось вікно терміналу, випливаючих вікон, тощо. Можна зробити висновок, що шкідливе ПЗ на базі хосту програми RMS спрацювало і його можна використовувати для реалізації MitM атаки або збирання необхідних даних для реалізації атаки іншими методами.

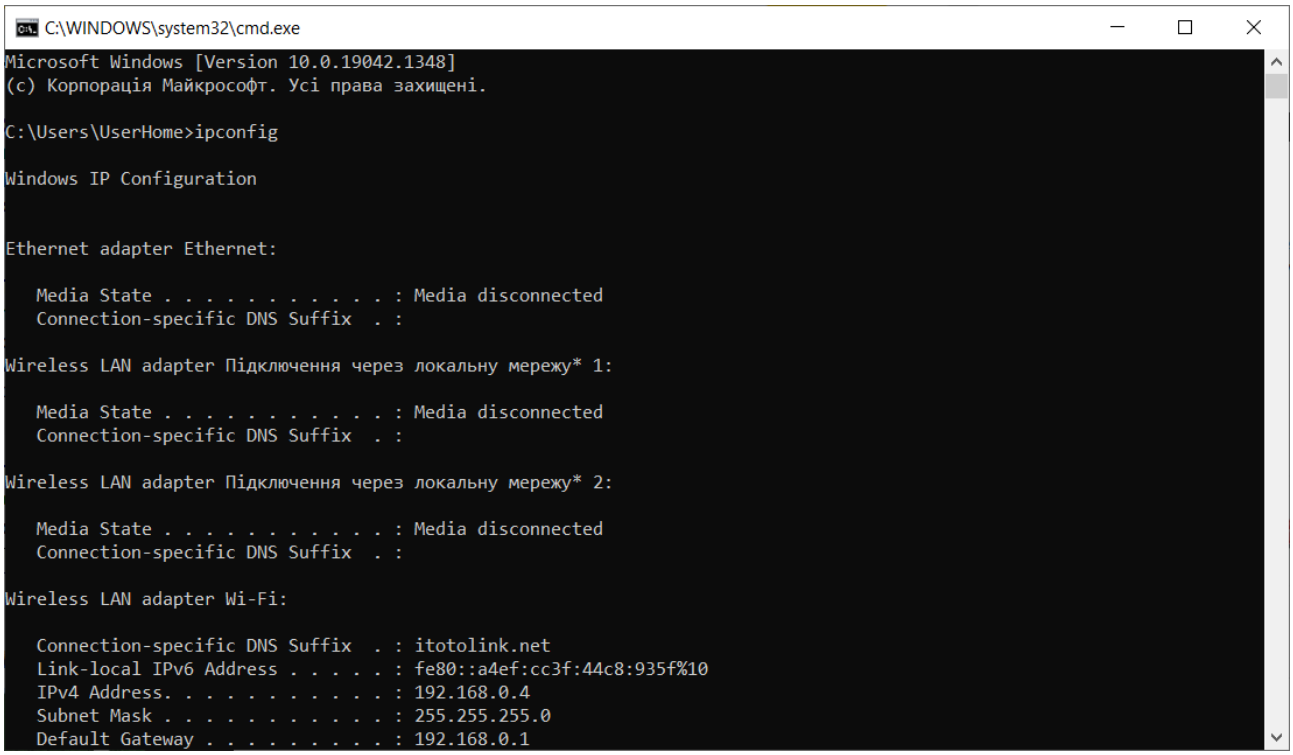

Рисунок 3.3 – Результат виконання дистанційної команди ipconfig зловмисником

Під час другого етапу перевірки всі файли шкідливого ПЗ було попередньо видалено. На пристрій встановлено запропонований безкоштовний антивірус Avira Free Antivirus. Файл встановлення шкідливого програмного забезпечення було повторно перенесено на комп’ютер.

Однак щойно файл потрапив на комп’ютер потенційної жертви, антивірусне програмне забезпечення сповістило про небезпеку. На рисунку 3.4 зображено дане сповіщення .

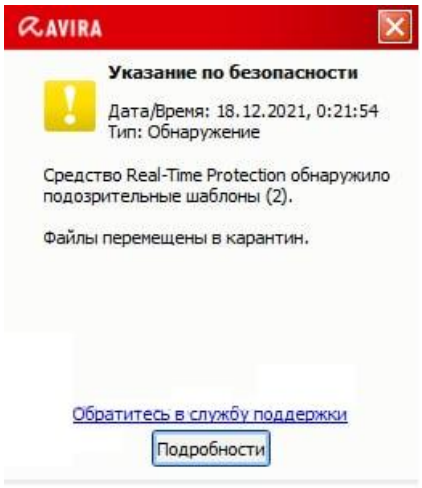

Рисунок 3.4 – Сповіщення безкоштовного антивірусного ПЗ про загрозу

Небезпечний файл одразу було видалено – рисунок 3.5.

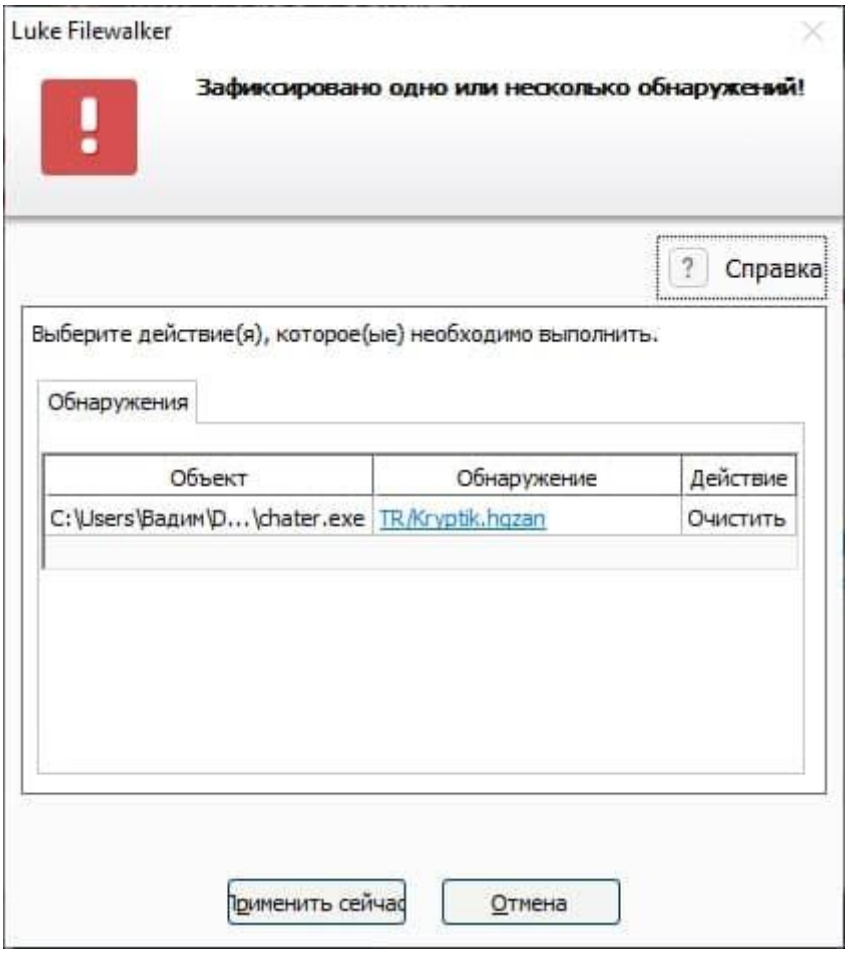

Рисунок 3.5 – Видалення шкідливого файлу

Таким чином за допомогою безкоштовного програмного засобу вдалося уникнути зараження ПК шкідливим ПЗ.

3.3.2 Очищення шкідливого ПЗ за допомого безкоштовних утиліт

У випадку, якщо комп’ютер все ж був заражений шкідливим програмним забезпеченням, на підприємствах малого та середнього бізнесу можуть скористатися запропонованою безкоштовною у методології утилітою UnHackMe. Її перевага не лише у можливості пошуку прихованих та замаскованих шкідливих файлів та в безкоштовності утиліти, а і в можливості використання її з іншими антивірусними програмами.

Для проведення експеременту, з комп’ютера, на який буде проведена атака, було видалено антивірусне програмне забезпечення та встановлено шкідливе ПЗ, яке вже описано в розділі 3.3.1. Оскільки антивірусного програмного забезпечення не було, вірус було встановлено.

Для його пошуку та видалення було запущено утиліту UnHackMe. На рисунку 3.6 показано, що безкоштовний програмний засіб зміг виявити шкідливу програму, яку не виявив захисник Windows та видалити її.

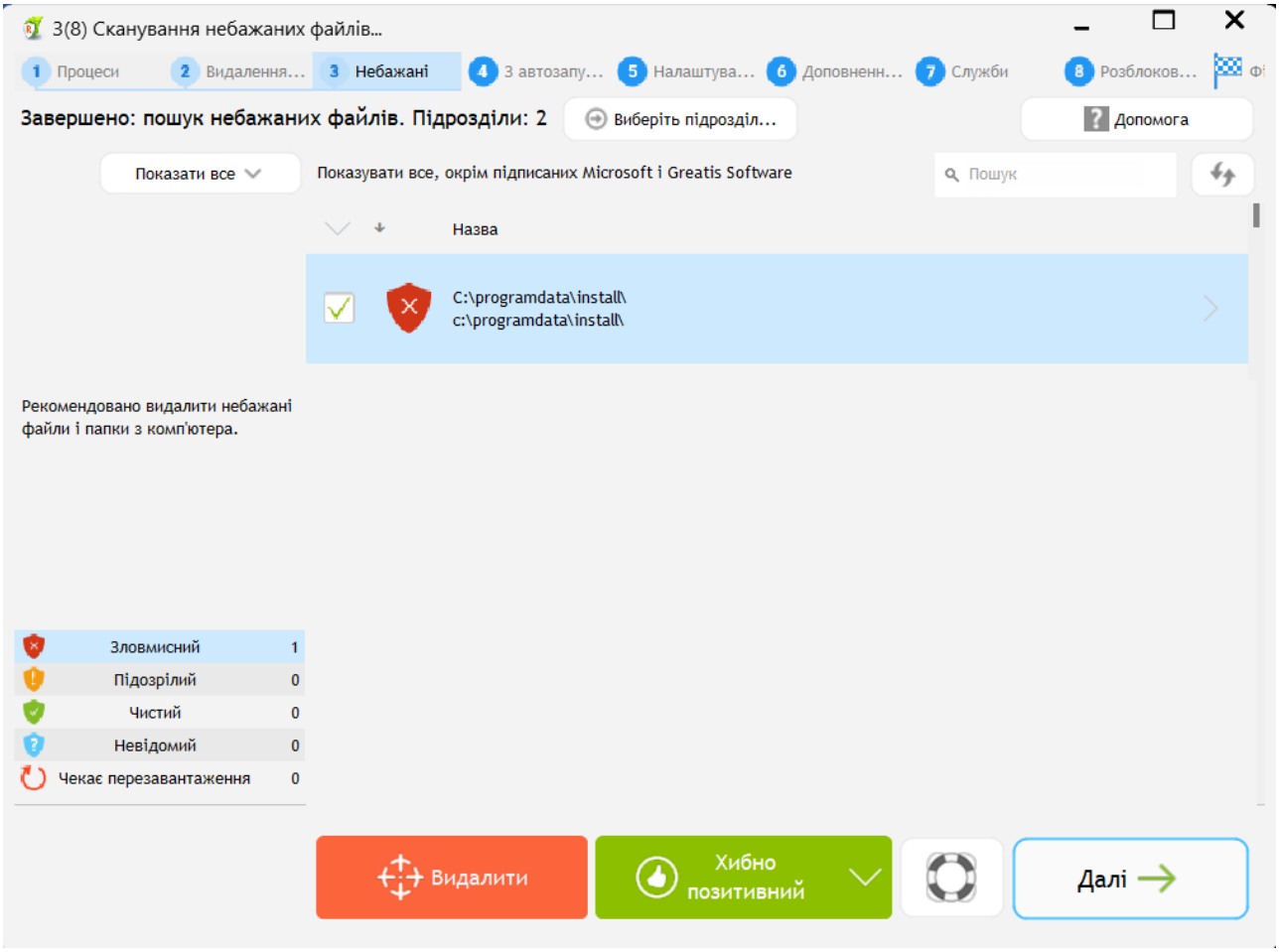

Рисунок 3.6 – Виявлення безкоштовною утилітою шкідливого ПЗ

Тож можна стверджувати, що ця безкоштовна утиліта може бути використана на підприємствах малого та середнього бізнесу для виявлення шкідливого програмного забезпечення та запобігання реалізації атаки через посередника.

3.3 Розробка методичних рекомендацій для користувачів ІКС на підприємствах

На основі проаналізованих ризиків, методів реалізації атак через посередника та методів захисту, було складено методичні рекомендації для працівників підприємств малого та середнього бізнесу. Це дозволить збільшити обізнаність персоналу в сфері інформаційної безпеки та грамотності. В свою чергу, це дозволить зменшити ризики атак на організацію з боку шахраїв.

Таким чином кожен працівник підприємства, незалежно від роду діяльності організації, який має доступ до ІКС підприємства, повинен дотримуватися наступних рекомендацій:

– Використовувати лише те програмне забезпечення, яке встановлено на пристрої. Не завантажувати, не встановлювати та не налаштовувати стороннє програмне забезпечення.

– Не видаляти та не змінювати налаштування антивірусного програмного забезпечення чи іншого ПЗ, яке використовується на пристрої для захисту інформації.

– Не ігнорувати необхідність оновлення операційної системи пристрою, використовуваних програмних засобів чи браузерів.

– Не підключати пристрої до відкритих точок доступу до Wi-Fi. Використовувати виключно безпроводову мережу підприємства, попередньо ввівши пароль мережі.

– Не передавати стороннім особам пароль від точки доступу до Wi-Fi, якщо цього не передбачено політикою безпеки підприємства.

– Не використовувати ІКС для власних цілей – покупок в інтернеті, спілкуванню в соцмережах, інтернет–серфінгу, тощо.

– Користуватися лише тим браузером, який було встановлено та налаштовано, відповідно до методології захисту від MitM атак.

– Вмикати VPN при роботі браузера, якщо це не виконується автоматично системою.

– При користуванні браузером переходити лише на чітко визначений перелік сайтів.

– Не переходити по посиланнях у надісланих листах, а вводити необхідний ресурс самостійно.

– Відвідувати лише HTTPS–сайти.

– Ігнорувати підозрілі листи, надіслані на електронну пошту.

– Використовувати для прочитання пошти віртуальну машину.

– Перевіряти правильність написання адреси електронної пошти відправника при отриманні листі. Якщо виникає підозра в авторитетності відправника – не відкривати лист.

– Не передавати третім особам конфіденційну інформацію.

– При підозрі, що була здійснена атака через посередника негайно повідомити про це керівництво підприємства або відповідальну особу.

– При появі сумніві щодо фіктивності інтернет–ресурсу припинити будь–які дії, негайно припинити введення будь–яких даних та залишити цей ресурс.

– У випадку повідомлення про загрозу від відповідного програмного забезпечення чи браузера про можливість реалізації загрози – не ігнорувати дане повідомлення. Покинути підозрілий ресурс та повідомити про подію відповідальну особу чи керівника.

– У випадку будь–яких позаштатних подій, які можуть вказувати на спробу реалізації кібератаки – негайно повідомити про це керівника або відповідальну за інформаційну безпеку на підприємстві особу.

– Якщо кібератака була реалізована – негайно повідомити про це керівника або відповідальну за інформаційну безпеку на підприємстві особу.

3.4 Висновки до третього розділу

Під час дослідження було встановлено основні методи реалізації атак через посередника. Відповідно до ризиків, було розроблено методологію захисту від даних атак для відповідальної за інформаційну безпеку особу та для інших працівників компанії.

Оскільки підприємтства малого та середнього бізнесу зазвичай не мають достатньо коштів для використання дороговартісного програмного забезпечення, послуг компаній з інформаційного захисту чи оплати роботи окремого спеціаліста, було запропоновано безкоштовні програмні продукти, які допоможуть забезпечити захист від MitM-атак. Акож було запропоновані платні альтернативи з наведенням актуальних цін.

Для мінімізації ризиків, пов’язаних з роботою персоналу було розроблено методичні рекомендації для працівників підприємств малого та середнього бізнесу. Це дозволить підвищити інформаційну грамотність працівників та знизити ризики реалізації атак через посередника на підприємствах.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКИ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Робота підприємств малого та середнього бізнесу неможлива без дотримання вимог до охорони праці. Законодавство України чітко регулює обов'язки та вимоги до забезпечення належних безпечних умов для роботи працівників.

Чинний закон «Про охорону праці» розповсюджується на всіх юридичних та фізичних осіб, які використовують найману працю та на всіх працюючих [34].

Підприємці зобов’язані дотримуватися правил охорони праці. Вони залежать від виду діяльності. Існують нормативно–правові документи для підприємств різного виду діяльності

Розроблена методологія захисту інформаційно–комунікаційних систем від атак через посередника також повинна відповідати усім чинним вимогам охорони праці.

Під час розробки, вибору, замовлення та модифікації програмного забезпечення, а також під час розробки завдань, що передбачають використання устаткування з екранними пристроями, роботодавець має керуватися таким програмним забезпеченням, яке відповідає розв’язуваним завданням і є простим у використанні, а де необхідно – адаптованим до рівня знань і досвіду працівника [35]. Запропоновані програмні засоби відповідають цим нормам, оскільки вони призначені для широкого кола користувачів, а не лише для спеціалістів вузької галузі ІТ та кіберзахисту. Інтерфейс та контроль запропонованих інструментів є інтуїтивно зрозумілим та легким для взаємодії з користувачем. Більшість функцій реалізовано в автоматичному фоновому режимі. Тому для роботи більшості запропонованих програмних засобів захисту навіть не потрібно втручання з боку працівника.

Для забезпечення безпечних умов для працівників та запобігання ризику виникнення пожеж необхідно дотримуватися наказу «Про затвердження Правил пожежної безпеки в Україні». Відповідно до нього. Улаштування та експлуатація тимчасових електромереж забороняються. Інформаційно-комунікаційна система не може бути облаштована на базі тимчасової електромережі. Це загрожує не лише цілісності та доступності даних, які використовують на підприємстві, а і фізичній безпеці колективу підприємства.
Приміщення, де розташована система, яка підлягає захисту, повинне відповідати вимогам діючих санітарних норм. Рівень освітлення, опалення і вентиляції повинні відповідати вимогам будівельних норм і правил. Устаткування може розміщуватися як у спеціально призначених приміщеннях, так і в загальних приміщеннях [36].

Умови розміщення комп'ютерної техніки та складових ІКС не повинні загрожувати виникненню поломки чи збою техніки, короткому замиканню, перегріву, тощо. Це становить загрозу як для працівників підприємства безпосередньо під час їх роботи, так і інформації, яка циркулює в системі.
У літературі з охорони праці виділяють різні типи ризиків – ризик події, ризики нещасного випадку, ризик смерті, виробничий ризик, професійний ризик [37]. В нормативно–правових документах з охорони праці в Україні поняття «ризик» може трактуватися не однаково. Відповідно до наказу №21 від 19.01.15 Міністерства енергетики та вугільної промисловості України, ризик – це імовірність заподіяння шкоди з урахуванням її тяжкості.

Розроблена методологія захисту від реалізації MitM атак ураховує можливі ризики та загрози здоров'ю та життю працівників підприємств під час роботи з інформаційно–комунікаційною системою. Запропонована методологія не передбачає встановлення додаткового обладнання або зміну фізичної організації ІКС. Тому керівник або особа, яка відповідальна за інформаційну безпеку на підприємстві, при впровадженні методології захисту від атак через посередника зобов'язана дотримуватися чинних вимог охорони праці.

4.2 Безпека в надзвичайних ситуаціях

Для роботи підприємств необхідно дотримання вимог до правильного освітлення виробничих приміщень для роботи ВДТ (відео-дисплейних терміналів). Оскільки на підприємствах збільшується кількість інформаційної техніки та техніки зв’язку, складовою яких є зоровий інтерфейс ВДТ, необхідно використовувати правильне освітлення. Вимоги до нього відрізняються від вимог освітлення для приміщень, де використовуються традиційні паперові носії інформації.

Правильне освітлення сприяє запобіганню виробничого травматизму, створює нормальні умови для органів зору, підвищує працездатність організму та знижує навантаженість на організм.

На підприємствах малого та середнього бізнесу правильне освітлення робочих приміщень обладнаних візуальними дисплейними терміналами має велике значення, оскільки працівники таких підприємств можуть впродовж всього робочого дня проводити роботу за монітором комп’ютера. Це викликає втому, зорове навантаження та психологічне виснаження. При неправильному освітленні робітник вже через кілька годин роботи втрачає увагу, може виникати головний біль, запаморочення, тощо.

Освітлення робочих приміщень з ВДТ повинне бути передбачене у проекті освітлення. Якісні зорові середовища приміщень з ВДТ повинні відповідати нормативним положенням по охороні здоров'я і забезпеченню безпеки при використанні ВДТ.

Відповідно до вимог «Щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» від 14.02.2018 року, вимоги поширюються на всі суб’єкти господарювання незалежно від форм власності, організаційно-правової форми і видів діяльності та встановлюють мінімальні

вимоги безпеки та захисту здоров’я під час здійснення роботи, пов’язаної з використанням екранних пристроїв незалежно від їхнього типу та моделі [37].

Роботодавець зобов’язаний повідомити працівників про умови праці та про наявність шкідливих виробничих факторів, що виникають при роботі з екранними пристроями та ще не усунені, а також про можливі наслідки їх впливу на здоров'я працівників. При цьому працівник має підписати розписку, що він був ознайомлений з ризиками.

Під час облаштування робочого місця працівника з екранними пристроями необхідно обирати таке устаткування, яке не створює зайвого шуму та не виділяє надлишкового тепла. Рівні шуму на робочих місцях осіб, які працюють з екранними пристроями, мають відповідати вимогам Санітарних норм виробничого шуму, ультразвуку та інфразвуку ДСН 3.3.6.037-99.

При роботі з екранними пристроями не допускається:

– проводити ремонтно–технічні роботи під час роботи працівника за екранним пристроєм;
– вимикати захисні пристрої, спонтанно вносити зміни в конструкцію та склад екрануючих пристроїв або їх технічну адаптацію;
– працювати з пристроями відображення, які мають незвичайні сигнали, нестабільні зображення на екрані та інші несправності під час роботи.

Існуючі стандарти по якості зображення на дисплейних екранах ґрунтуються на принципі граничного контрасту − мінімального контрасту, необхідного для зорового виявлення або розпізнавання. Це означає необхідність підтримання контрасту зображень, що пред'являються, необхідного для достатньої розбірливості.

Для створення необхідного контрасту та комфортної роботи, необхідно мати можливість регулювання кількості світла. Якщо приміщення в денний період доби може бути освітлене сонячним світлом, повинна бути можливість зменшення інтенсивності світла. Віконні прорізи приміщень для роботи з ВДТ мають бути обладнані регульованими пристроями (жалюзі, завіски, зовнішні козирки).

Для внутрішнього оздоблення приміщень з ВДТ слід використовувати дифузно-відбивні матеріали з коефіцієнтами відбиття для стелі 0,7 – 0,8, для стін 0,5 – 0,6. Покриття підлоги повинне бути матовим з коефіцієнтом відбиття 0,3 – 0,5. Поверхня підлоги має бути рівною, неслизькою, з антистатичними властивостями [38].

Система загального освітлення має становити суцільні або преривчасті лінії світильників, розташовані збоку від робочих місць (переважно ліворуч), паралельно лінії зору працюючих. Яскравість світильників загального освітлення в зоні кутів випромінювання від 50 до 90 град. з вертикаллю в повздовжній та поперечній площинах має становити не більше ніж 200 кд/кв. м, захисний кут світильників – не менше ніж 40 град. Світильники місцевого освітлення повинні мати просвічуючий відбивач із захисним кутом не меншим ніж 40 град.

Показник осліпленості у разі використання джерел загального штучного освітлення у виробничих приміщеннях має не перевищувати 20, а показник дискомфорту в адміністративно-громадських приміщеннях має бути не більше за 40.

Коефіцієнт пульсації має не перевищувати 5 %, що забезпечується застосуванням газорозрядних ламп у світильниках загального та місцевого освітлення з ВЧ ПРА для світильників будь-яких типів. Якщо не має світильників з ВЧ ПРА, то лампи багатолампових світильників або світильники загального освітлення, розташовані поруч, слід вмикати на різні фази трьохфазної мережі.

Дотримуючись цих вимог можна створити безпечні та комфортні умови для роботи працівників підприємства.

ВИСНОВКИ

Під час виконання даної роботи було розв’язано ряд важливих задач, які стосуються захисту підприємств малого та середнього бізнесу від MitM атак.

В результаті роботи було виконано наступну роботу:

- проведено аналіз літературних джерел в області досліджень;
- проаналізовано останні масивні атаки на підприємства малого та середнього бізнесу;
- досліджено найбільш поширені форми атак через посередника;
- розроблено методологію для керівників підприємств або відповідальних за інформаційну безпеку осіб щодо протидії атак через посередника.
- проаналізовано існуючі інструменти для запобігання реалізації атак через посередника;
- запропоновано набір безкоштовних інструментів для захисту від різних форм атак через посередника та їх платні альтернативи;
- розроблено методичні рекомендації для працівників підприємств для запобігання реалізацій атак через посередника.

Застосування даної методології можливе на підприємствах малого та середнього бізнесу будь-яких спеціалізацій. Враховані також ризики реалізації атаки направленої не лише на ІКС підприємства, а і на особисті пристрої працівників, які можуть бути використані для роботи, а також пристрої клієнтів, які підключаються до точки доступу безпроводового зв’язку підприємства.

Запропонована методологія не потребує особливих фінансових затрат, що робить її доступною для будь–яких підприємств малого та середнього бізнесу, які не мають достатнього фінансування для реалізації інформаційного захисту на підприємстві.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks. URL: https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/

2. What is a Man-in-the-Middle Attack: Detection and Prevention Tips. URL: https://www.varonis.com/blog/man-in-the-middle-attack/

3. Господарський кодекс України, Редакція від 19.12.2021

4. Державна служба статистики України. Кількість активних підприємств за регіонами України та видами економічної діяльності. URL: http://ukrstat.gov.ua/operativ/operativ2014/kap/kap_u/arh_kap_u.html

5. Звіт Національної поліції України про результати роботи у 2020 році. – 12 с.

6. БІЗНЕС ТА COVID-19: ВИЖИТИ НЕ МОЖНА ПОМЕРТИ. АНАЛІТИЧНИЙ ЦЕНТР ЕКОНОМІКО-ПРАВОВИХ ДОСЛІДЖЕНЬ ТА ПРОГНОЗУВАННЯ. 5–9 с.

7. Про захист персональних даних: Редакція від 15.12.2021

9. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НОРМАТИВНИЙ ДОКУМЕНТ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Київ 1999

10. How to defend against man-in-the-middle attacks. URL: https://www.itgovernance.eu/blog/en/how-to-defend-against-man-in-the-middle-attacks

11. Man in the middle (MITM). URL: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

12. Wi-Fi Eavesdropping. URL: https://doubleoctopus.com/security-wiki/threats-and-tools/wi-fi-eavesdropping/

13. Brute-force Attack. URL: https://doubleoctopus.com/security-wiki/threats-and-tools/brute-force-attack/

14. Microsoft Attack Blamed on China Morphs Into Global Crisis. URL: https://www.bloomberg.com/news/articles/2021-03-07/hackers-breach-thousands-of-microsoft-customers-around-the-world

15. Укрпошта звернулась до правоохоронних органів та Кіберполіції України для розслідування шахрайської розсилки. URL: https://www.ukrposhta.ua/ua/news/57248-ukrposhta-zvernulas-do-pravoohoronnih-organiv-ta-kiberpolicii-ukraini-dlja-rozsliduvannja-shahrajskoi-rozsilki

16. Phishing with Unicode Domains. URL: https://www.xudongz.com/blog/2017/idn-phishing/

17. Що таке IP–спуфінг. URL: https://rusvpn.com/ru/blog/chto-takoe-ip-spufing-i-kak-predotvrashhat-spufing-ataki/

18. Framework for Man-In-The-Middle attacks. URL: https://github.com/byt3bl33d3r/MITMf

19. KARMA Attacks Radioed Machines Automatically. URL: https://theta44.org/karma/

20. Intercepter-NG. URL: http://sniff.su/

21. The Middler: программа для взлома незащищённых аккаунтов Gmail. URL: https://habr.com/ru/post/37792/?mobile=no

22 Сороківська О.А. ОСОБЛИВОСТІ ФОРМУВАННЯ ТЕОРЕТИЧНИХ ЗАСАД ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ МАЛОГО БІЗНЕСУ. 493 с. 493

23. Новый метод mitm атаки в wifi-сетях. URL: https://cryptoworld.su/новый-метод-mitm-атаки-в-wifi-сетях/

24. Жаровський Р.О: Захист інформації у комп'ютерних системах. Тернопіль 2019

25. Обзор средств защиты электронной почты. URL: https://habr.com/ru/company/cybersafe/blog/269513/

26. Названы самые популярные браузеры по итогам 2020 года. URL: https://deps.ua/novosti/novosti-rynka/8869.html

27. БРАУЗЕРЫ. ТОП ПОПУЛЯРНЫХ ВЕБ-БРАУЗЕРОВ 2019 URL: https://marketer.ua/stats-of-browsers-2019/

28. Some security issues when using a VPN. URL: https://riseup.net/ca/vpn/security-issues

29. Avira Free Antivirus. URL: https://www.avira.com/ru/free-antivirus-windows

30. UnHackMe на компьютер с ОС Windows. URL: https://it-tehnik.ru/software/antivirus/unhackme.html

31. ProtonVPN. URL: https://protonvpn.com/

32. VirtualBox. URL: https://www.virtualbox.org/

33. Secure Mail for Gmail. URL: https://www.streak.com/securegmail

34. Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями : Зареєстровано в Міністерстві юстиції України 25 квітня 2018 р. за № 508/31960

35. Про затвердження Державних санітарних норм та правил при роботі з джерелами електромагнітних полів: Зареєстровано в Міністерстві юстиції України 13 березня 2003 р. за N 203/7524

36. Гурик О.Я. ТЛУМАЧЕННЯ РИЗИКУ В ОХОРОНІ ПРАЦІ. URL: http://elartu.tntu.edu.ua/bitstream/123456789/13774/2/VseukrStud_20121v2_Hurik_O-Tlumachennia_ryzyku_v_okhoroni_144.pdf

37. Щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями: Наказ Міністерства соціальної політики України 14.02.2018 № 207

38. Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. URL: https://www.buh24.com.ua/gigiyenichni-vimogi-do-organizatsiyi-roboti-z-vizualnimi-displeynimi-terminalami-elektronno-obchislyuvalnih-mashin/

39. Матеріали IX Науково-технічної конференції «ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ». Тернопіль 2021

ДОДАТКИ