НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ МЕРЕЖЕВОГО ЗАХИСТУ ІНФОРМАЦІЇ»

Виконала: здобувачка 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Табала Ксенія Андріївна

Керівник: к.т.н., доцент
Кухаренко Сергій Вікторович

Рецензент: к.т.н., доцент
Ахмаметьєва Ганна Валеріївна

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачці Табала Ксенії Андріївні

1. Тема роботи: «Дослідження сучасних методів мережевого захисту інформації»
Керівник роботи: к.т.н, доцент Кухаренко Сергій Вікторович
затверджені наказом НУ ОЮА від «02» квітня 2024 року № 809-06
2. Строк подання здобувачем роботи «20» травня 2024 рік
3. Дата видачі завдання«15» вересня 2023 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Дослідження сучасних методів мережевого захисту інформації» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 1 рисунок, 1 таблицю, 30 літературних джерел за переліком посилань. Робота виконана на 40 сторінках загального тексту і 32 сторінках основного тексту.

Метою роботи є дослідження сучасних методів мережевого захисту інформації, таких як криптографічний захист інформації, автентифікація та авторизація, методів захисту від розподілених атак, методи захисту від зчитування відбитків браузерів.

Під час дослідження було проведено приклад збору даних користувача за допомогою відбитків браузерів та способи зменшити ризики від отримання цих даних зловмисниками.

Можливі напрями подальших досліджень включають розробку нових технологій для виявлення та протидії збору відбитків браузерів та подальше розвинення методів мережевого захисту інформації.

ЗАХИСТ ІНФОРМАЦІЇ, МЕТОДИ ЗАХИСТУ, МЕРЕЖА, МЕРЕЖЕВИЙ ЗАХИСТ, ВІДБИТКИ БРАУЗЕРІВ.

ABSTRACT

Qualification work on the topic «Research of modern methods of network information protection» for obtaining the first (bachelor) level of higher education in specialty 125 Cybersecurity, educational program: Cybersecurity, contains 1 drawing, 1 table, 30 literary sources according to the list of references. The work was done on 40 pages of general text and 32 pages of main text.

The aim of the work is to study modern methods of network protection of information, such as cryptographic protection of information, authentication and authorization, methods of protection against distributed attacks, methods of protection against reading browser fingerprints.

The study conducted an example of collecting user data using browser fingerprints and ways to reduce the risks of hackers obtaining this data.

Possible areas of further research include the development of new technologies to detect and counter the collection of browser fingerprints and the further development of methods of network protection of information.

INFORMATION PROTECTION, PROTECTION METHODS, NETWORK, NETWORK PROTECTION, BROWSER FINGERPRINTS.

ЗМІСТ

ВСТУП 6

1 ЗАХИСТ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ МЕРЕЖ 8

1.1 Сучасні тенденції у розвитку мережевих загроз 8

1.2 Основні принципи мережевого захисту 12

1.3 Захист інформації 16

2 ЗАГРОЗИ ТА ПОПЕРЕДЖЕННЯ АТАК НА МЕРЕЖЕВУ СИСТЕМУ 18

2.1 Методи криптографічного захисту інформації 18

2.2 Методи автентифікації та авторизації в мережах 20

2.3 Розгляд методів захисту від розподілених атак 23

3 ВІДБИТКИ БРАУЗЕРІВ 26

3.1 Методи збору та використання відбитків браузерів 26

3.2 Оцінка приватності та безпеки зібраних відбитків браузерів 27

3.3 Дослідження різних браузерів за рівнем захисту 29

3.4 Аналіз браузеру Mozilla Firefox на створення цифрового відбитку 31

ВИСНОВКИ 36

ПЕРЕЛІК ПОСИЛАНЬ 38

ВСТУП

У наш час, у зв’язку з поширенням мережі Інтернет, де інформація стала одним з найцінніших ресурсів, стоїть важливе питання щодо проблеми конфіденційності та доступу до особистих даних користувачів.

У сучасному цифровому світі, де обмін інформацією відбувається через мережі, захист конфіденційності, цілісності та доступності даних є ключовим питанням. Кількість кіберзагроз зростає щодня, в той же час коли атаки стають все більш складними та витонченими. Тому наразі є дуже важливим розуміння розробки та методів вдосконалення сучасних методів мережевого захисту інформації.

Сучасні тенденції несанкціонованого збору, накопичення та обробки персональних даних з пристроїв комунікації користувачів, долучених до інтернет-простору, все частіше викликають занепокоєння не лише у громадських правозахисних організацій, а й у все більшої кількості користувачів. Такий стан справ зумовлює нагальну потребу в проведенні поглибленого аналізу принципів створення цифрових відбитків пристроїв комунікації, які цілком ґрунтуються на зборі персональних даних з веббраузерів. Результати такого аналізу дозволять значно підвищити приватність та анонімність користувачів і, як наслідок, знизити вплив монополістів ринку цифрових профілів на їхні рішення та поведінкові переваги. Тому питання захисту інформації та інформаційних мереж є доволі актуальним на сьогоднішній день.

Метою кваліфікаційної роботи є дослідження та оцінка можливості мережевого захисту від кібератак та кіберзлочинів, а також розробка заходів, що запобігають ідентифікації пристроїв користувачів.

Об’єкт дослідження – можливості здійснення ідентифікації пристроїв комунікації користувачів за допомогою створення унікальних цифрових відбитків веббраузерів, що використовуються для комунікації в інтернет-просторі.

Предмет дослідження – цифрові відбитки веббраузерів, що отримуються у різних варіантах їх конфігурації та їх вплив на вірогідність ідентифікації пристроїв комунікації користувачів.

Практична значність роботи полягає в нівелюванні будь-якої ідентифікації громадян України у цифровому просторі, особливо враховуючи сучасні тренди у інформаційному віртуальному протистоянні. Розроблені заходи суттєво підвищать рівень захищеності громадян, та організацій від особистого цифрового профілювання і пов’язаного з ним інформаційного маніпуляційного впливу.

Під час підготовки бакалаврської роботи дослідження, які представлені у третьому розділі були апробовані на наукових та науково-практичних конференціях, зокрема: тези «Сучасні напрями забезпечення кіберзахисту та удосконалення інформаційних технологій» на Всеукраїнській науково-практичній конференції здобувачів вищої освіти «Суспільство та держава в умовах воєнного стану: виклики та перспективи», м. Одеса, 27 квітня 2024 року, а також опубліковані тези «Цифрові відбитки веббраузерів» на конференції «Кібербезпека в сучасному світі: актуальні виклики: : матеріали III Всеукр. наук.-практ. конф. (м. Одеса, 19 листопада 2021 р.) / за ред. О.В. Дикого; уклад.: С. А. Горбаченко, Н. І. Логінова. – Одеса : Гельветика, 2021. – С. 77-80.

1 ЗАХИСТ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ МЕРЕЖ

1.1 Сучасні тенденції у розвитку мережевих загроз

У сучасному цифровому світі швидкий і безперервний розвиток технологій відкриває безліч можливостей, але також створює нові виклики у сфері кібербезпеки. Тенденції розвитку мережевих загроз постійно змінюються, що вимагає від організацій і фахівців з кібербезпеки постійного оновлення підходів і заходів захисту. У цьому розділі описані ключові тенденції розвитку мережевих загроз, включаючи такі поняття, як штучний інтелект, машинне навчання та інтернет речей, які є не тільки предметом наукових досліджень, але й становлять реальну загрозу кібербезпеці. Ці тенденції дозволять краще зрозуміти сучасні виклики в цій сфері та розробити ефективні стратегії захисту мережевих систем.

Питання інформаційної безпеки загалом можна розділити на дві категорії: захист інформації (запобігання загроз інформації); захист від інформації (запобігання інформаційних загроз). Іншими словами, інформаційна безпека має два аспекти: технічний та гуманітарний, кожен з яких має зовнішні та внутрішні елементи [1].

Ці два аспекти мають зовнішні та внутрішні елементи відповідно. Обидва ці аспекти в першу чергу стосуються людей та їхньої інформаційної культури.

Технічні аспекти інформаційної безпеки – це здатність і навички людей передбачати і запобігати загрозам інформації, що циркулює в технічних системах, а також самим системам.

Однак технічні аспекти не є первинними в структурі інформаційної безпеки. Необхідно не тільки захистити інформацію від знищення, зміни, перехоплення, несанкціонованого витоку та порушення встановленої послідовності маршрутів. Необхідно також забезпечити інформаційну безпеку суспільства, щоб запобігти негативним впливам на навколишнє середовище, які можуть виникнути в результаті непередбаченої обробки інформації [2].

Сучасні тенденції розвитку мережевих загроз створюють нові виклики для кібербезпеки.

Інформаційна безпека – це сукупність методів захисту інформації від випадкового або навмисного впливу. Такі протиправні дії зазвичай завдають шкоди особі, яка володіє інформацією. Шкода може бути як матеріальною, так і моральною, наприклад [3].

Мережева безпека – заходи щодо захисту інформаційних мереж від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб знищення її компонентів [5].

Безпека інформаційної мережі включає в себе захист обладнання, програмного забезпечення, даних і персоналу. Мережева безпека включає в себе положення і політику, прийняті мережевими адміністраторами для запобігання і контролю несанкціонованого доступу до комп'ютерних мереж і мереж доступних ресурсів, зловживань, змін або відмови в доступі до них. Мережева безпека включає дозволи, надані мережевим адміністратором для доступу до даних у мережі. Користувачі можуть обирати або отримувати ідентифікатори та паролі чи інші засоби автентифікації для доступу до інформації та додатків у межах своїх повноважень.

Мережева безпека охоплює різні комп'ютерні мережі, як публічні, так і приватні, що використовуються в повсякденній роботі для здійснення транзакцій і комунікацій між підприємствами, державними установами та приватними особами. Деякі мережі є приватними, наприклад, всередині компаній, в той час як інші є загальнодоступними для широкої громадськості. Мережева безпека стосується організацій, компаній та інших типів установ. Найпоширеніший і найпростіший спосіб захистити мережеві ресурси - це присвоїти їм унікальне ім'я і відповідний пароль.

Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів [4].

Загроза (у загальному розумінні) – це подія, дія (вплив), процес або явище, що може завдати шкоди чиїмось інтересам.

Загроза інтересам суб’єкта інформаційної діяльності – це подія, процес або явище, що може прямо чи опосередковано призвести до завдання шкоди даним конкретного суб’єкта шляхом впливу на інформацію або інші компоненти інформаційної системи [4].

Загрози інформаційній безпеці можна класифікувати за різними критеріями:

За аспектом інформаційної безпеки, на який спрямована загроза: загрози конфіденційності, доступності та цілісності; за місцем розташування джерела загрози: внутрішні та зовнішні; за характером загрози: штучні та природні; та інші.

Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту [4].

Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [4].

Захист інформації – сукупність заходів, спрямованих на запобігання порушенню конфіденційності, цілісності, доступності інформації, здійсненню її несанкціонованої модифікації. Захисту підлягає інформація у будь-якій формі чи відображення, дані і програми автоматизованих систем, неправомірні дії з якими

можуть зашкодити власникові, користувачеві чи ін. учаснику інформаційної діяльності, призвівши до серйозних втрат у галузях науково-технічної, адміністративно-господарської та комерційної діяльності організацій, підприємств і держави [6].

Погляд на роль штучного інтелекту (ШІ) в кібербезпеці ШІ використовується для виявлення мережевих аномалій і атак, допомагаючи підвищити рівень безпеки Системи ШІ виявляють незвичайні патерни в поведінці користувачів і мережевих пристроїв, а також потенційні загрози. допомагають вчасно реагувати на них. Машинне навчання використовується для розробки моделей, які аналізують великі обсяги даних і допомагають виявляти аномалії та атаки в мережі.

Водночас машинне навчання стає все більш важливим як інструмент для виявлення загроз у режимі реального часу. Алгоритми машинного навчання аналізують великі обсяги даних для виявлення аномальної поведінки та швидкого реагування на потенційні загрози. Це автоматизує процес виявлення загроз і реагування на них, скорочуючи час реагування і підвищуючи ефективність заходів безпеки.

Крім того, зростаюча кількість підключених пристроїв в Інтернеті речей створює нові вектори атак і вразливості. Розуміння цієї тенденції є критично важливим для розробки стратегії безпеки для запобігання атакам на підключені пристрої та забезпечення стабільної роботи мережевих систем. Чим більше пристроїв підключено до мережі, тим більше вразливостей, які можуть бути атаковані. Розуміння цієї тенденції може допомогти розробити стратегії безпеки, спрямовані на запобігання атакам на пристрої IoT [2].

Знання, отримані в результаті розгляду цих тенденцій, допоможуть розробити ефективні стратегії захисту мережевої інфраструктури, здатні вирішити сучасні проблеми кібербезпеки.

Штучний інтелект, машинне навчання та Інтернет речей встановлюють нові стандарти мережевої безпеки, вимагаючи постійного оновлення та розвитку стратегій безпеки.

Розуміння цих понять дозволяє розробити комплексний підхід до кібербезпеки, який може ефективно захистити мережеву інфраструктуру перед обличчям постійно зростаючих загроз.

Робота в сфері кібербезпеки має вирішальне значення в сучасному цифровому суспільстві. Стрімкий розвиток технологій означає, що необхідно постійно вдосконалювати заходи безпеки та здійснювати безперервний моніторинг мережевих систем. Це єдиний спосіб ефективно протистояти сучасним мережевим загрозам і забезпечити стійкість інформаційних систем у майбутньому.

1.2 Основні принципи мережевого захисту

Оскільки мережеві технології сьогодні використовуються практично в усіх сферах життя, від банківської справи до медичної діагностики, захист мереж став критично важливим питанням. Швидкий і безперервний розвиток інформаційних технологій супроводжується постійним зростанням загроз кібербезпеці. Кібератаки стають все більш складними та витонченими, що робить багато мереж та систем вразливими до потенційних загроз.

Важливість знання основних принципів мережевого захисту полягає в тому, що вони відображають необхідність розуміння і впровадження стратегій і методів ефективного захисту мереж від кіберзагроз. Для підприємств, державних установ, організацій та приватних осіб забезпечення надійного захисту мережі є пріоритетним завданням через ризики, пов’язані з втратою конфіденційної інформації, цілісності даних та порушенням роботи системи [5].

Перегляд основних принципів мережевої безпеки має вирішальне значення для забезпечення стійкості та безпеки мережевої інфраструктури в сучасному цифровому середовищі. Тому цей документ має на меті визначити та проаналізувати основні аспекти цього питання з метою підвищення обізнаності та розробки ефективних стратегій захисту.

До основних принципів безпеки мережі можна віднести наступні:

Захист підключених до мережі пристроїв: забезпечення захисту підключених до мережі пристроїв вимагає використання сучасних високотехнологічних рішень. Наприклад, комп'ютери, які можуть піддаватися вірусним атакам, повинні бути захищені надійним антивірусним програмним забезпеченням і налаштовані на автоматичне оновлення баз сигнатур, щоб мінімізувати ризик атаки.

Мережеве обладнання має бути відмовостійким і здатним до швидкого відновлення. Важливо, щоб інфраструктура підлягала систематичному моніторингу для точного визначення стану конкретних пристроїв, додатків і сервісів, а також для впровадження заходів безпеки, якщо це необхідно [5].

Слід постійно контролювати пропускну здатність мережі. У разі атаки витрати на відновлення працездатності системи завжди значні. Тому необхідно використовувати заходи захисту від цілеспрямованих атак і методи запобігання вторгнення в інфраструктуру. Це мінімізує ризик успішного зловмисника та мінімізує витрати на відновлення даних підприємства.

Локальна мережа підприємства повинна бути відмовостійкою і здатною швидко відновлюватися в разі необхідності. Хоча неможливо захистити мережу на сто відсотків за будь-яких обставин, можна гарантувати, що якщо перший ресурс вийде з ладу, його можна буде швидко перенести з одного ресурсу на інший так, щоб користувач мережі не знав про це.

Ці основні принципи є ключовими елементами ефективної стратегії мережевої безпеки. Ретельне вивчення та впровадження цих принципів може підвищити рівень безпеки та захистити мережеву інфраструктуру від цілого ряду загроз.

Базові принципи мережевої безпеки визначають основу для ефективного захисту мережевої інфраструктури від кіберзагроз. Застосування цих принципів мінімізує ризик порушень безпеки та забезпечує високий рівень мережевої безпеки.

Загальна мета цих принципів – забезпечити стабільність, надійність і конфіденційність мережевих інфраструктур в сучасному цифровому середовищі. Вивчення та впровадження цих принципів має важливе значення для успішного захисту мереж і даних в них [5].

Нижче розглянемо засоби захисту мережевої безпеки від атак на неї.

Атаки на мережеву інфраструктуру можуть бути активними або пасивними (залежно від шкідливого програмного забезпечення, яке використовує зловмисник). Тому для забезпечення мережевої безпеки використовуються комплексні заходи.

Брандмауери: створюють бар’єр між довіреною внутрішньою мережею та ненадійною зовнішньою мережею, такою як Інтернет. Брандмауери використовують певний набір правил, які дозволяють або блокують трафік. Брандмауери можуть бути апаратними, програмними або комбінованими. Також доступні ефективні пристрої уніфікованого управління загрозами (UTM) та брандмауери нового покоління, які спеціалізуються на захисті від загроз.

Безпека електронної пошти: шлюзи електронної пошти є основною мішенню для зловмисників, які прагнуть проникнути в мережі. Хакери аналізують персональні дані та використовують методи соціальної інженерії для створення складних фішингових кампаній, щоб обманом змусити одержувачів відвідувати шкідливі вебсайти.

Сучасне програмне забезпечення для захисту електронної пошти блокує вхідні атаки та відстежує вихідні повідомлення, щоб запобігти втраті конфіденційних даних.

Антивірусне програмне забезпечення та захист від шкідливих програм: «Шкідливе програмне забезпечення» (скорочено від «зловмисне програмне забезпечення») – це віруси, інтернет-черв’яки, троянські програми, програми-вимагачі та шпигунські програми. Іноді шкідливе програмне забезпечення може заражати мережу днями або навіть тижнями, не проявляючи себе.

Найкраще антивірусне програмне забезпечення не лише сканує вхідний трафік для виявлення шкідливого програмного забезпечення, але й безперервно

контролює файли після цього, щоб виявити аномалії, видалити шкідливе програмне забезпечення та усунути пошкодження.

Сегментація мережі: програмна сегментація класифікує мережевий трафік і спрощує застосування політик безпеки. Класифікація в ідеалі базується на ідентифікації кінцевих точок, а не лише на IP-адресах. Призначення прав доступу на основі ролі, місцезнаходження та інших факторів гарантує, що потрібні користувачі отримають потрібний рівень доступу, підозрілі пристрої будуть поміщені в карантин, а загрози будуть усунені.

Контроль доступу: не всі користувачі мають доступ до мережі. Щоб захиститися від потенційних хакерів, кожен користувач і кожен пристрій повинен бути розпізнаний. Тільки тоді можна забезпечити дотримання політик безпеки. Кінцеві точки, які не відповідають вимогам, можна заблокувати або надати обмежений доступ. Цей процес називається контролем доступу до мережі (NAC).

Безпека додатків: все програмне забезпечення, що використовується в організації, незалежно від того, чи створене IT-персоналом організації, чи придбане у третьої сторони, має бути захищене. На жаль, будь-яка програма може містити лазівки (або вразливості), якими хакери можуть скористатися для проникнення в мережу [3].

Система безпеки додатків включає в себе апаратне, програмне забезпечення та процеси, що використовуються для усунення цих вразливостей.

Поведінковий аналіз: з метою виявлення аномальної поведінки в мережі, необхідно знати, як виглядає нормальна поведінка. Інструменти поведінкового аналізу автоматично виявляють незвичну поведінку. Це дозволяє відділам інформаційної безпеки ефективніше виявляти ознаки потенційного порушення, яке може спричинити проблеми, і швидко блокувати загрози.

Запобігання витоку даних: організаціям необхідно забезпечити, щоб співробітники не ділилися конфіденційною інформацією за межами мережі. Технологія запобігання витоку даних може перешкодити користувачам безпечно завантажувати, передавати або друкувати конфіденційну інформацію.

Безпека мобільних пристроїв: мобільні пристрої та додатки все частіше стають мішенню для кіберзлочинців. Протягом наступних трьох років дев'яносто відсотків IT-організацій можуть підтримувати корпоративні додатки на персональних мобільних пристроях. У цьому випадку необхідно контролювати доступ різних пристроїв до мережі. Крім того їм необхідно налаштувати свої з'єднання, щоб зберегти конфіденційність мережевого трафіку [5].

Віртуальні приватні мережі (VPN): віртуальна приватна мережа шифрує з'єднання кінцевого пристрою з мережею. Зазвичай VPN для віддаленого доступу використовують IPsec або SSL для автентифікації взаємодії між пристроєм і мережею.

Безпека вебтрафіку: рішення для захисту вебтрафіку контролюють використання Інтернету співробітниками, блокують веб-загрози та запобігають доступу до шкідливих вебсайтів. Вони захищають вебшлюзи в локальній мережі або в хмарі. Безпека вебтрафіку включає в себе заходи для захисту вебсайту.

1.3 Захист інформації

Згідно із Законом України «Про захист інформації в автоматизованих системах» захист інформації – це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованих систем та осіб, які користуються інформацією [7].

Забезпечення безпеки інформаційних технологій є комплексним питанням. Це комплексна проблема, що включає в себе правове регулювання використання інформаційних технологій, вдосконалення технологій, розробку, розвиток систем сертифікації та забезпечення належних організаційно-технічних умов експлуатації. Вирішення цієї проблеми вимагає значних витрат.

Перша проблема полягає в тому, щоб співвіднести необхідний рівень безпеки з витратами на його підтримку. Для цього необхідно визначити потенційні загрози, ймовірність їх виникнення та можливі наслідки, вибрати і

побудувати відповідні заходи. Також потрібно вибрати відповідні заходи і побудувати надійні системи захисту [6].

Основними принципами інформаційної безпеки є цілісність інформації, конфіденційність і, водночас, доступ до неї всіх авторизованих користувачів. У зв'язку з цим, основними випадками порушення інформаційної безпеки є наступними: несанкціонований доступ – доступ до інформації з порушенням правил розмежування доступу; порушення доступу до інформації; втрата інформації; фальсифікація інформації; перехоплення інформації; спотворення процесу обробки інформації тощо.

Загалом, найбільшою загрозою для інформаційної безпеки є люди. При побудові систем захисту необхідно передбачати навмисну або випадкову поведінку особи [8].

Інформаційна безпека охоплює захист конфіденційності, забезпечення захисту конституційних прав і свобод людини і громадянина, надання можливості доступу до інформації та її використання, а також порушує питання захисту інформації. Захист інформації гарантує цілісність, достовірність, точність і повноту інформації [9].

Нормативно-правова база захисту інформації включає норми, що регулюють суспільні відносини, які виникають у процесі інформаційної взаємодії між фізичними та юридичними особами і державою. Автор зазначає, що розвиток цифрової економіки зумовив необхідність внесення змін до нормативно-правової бази захисту інформації, але не встиг адекватно врахувати мінливі технологічні та соціальні аспекти життя суспільства. Автор наголошує на необхідності захисту комерційної та професійної таємниці, державної таємниці, інсайдерської інформації та персональних даних. На основі аналізу реалізації захисту інформації в контексті інформаційної безпеки для забезпечення конфіденційності інформації з обмеженим доступом виявлено низку закономірностей, які враховуються при визначенні тенденцій розвитку захисту інформації. Захист інформації має бути закріплений на законодавчому рівні щодо всіх видів інформації з обмеженим доступом [9].

2 ЗАГРОЗИ ТА ПОПЕРЕДЖЕННЯ АТАК НА МЕРЕЖЕВУ СИСТЕМУ

2.1 Методи криптографічного захисту інформації

Криптографічні методи захисту інформації – це спеціальні способи шифрування, кодування або іншого перетворення інформації таким чином, що доступ до її вмісту неможливий без пред’явлення та зворотного перетворення ключа шифрування [10].

Криптографічні методи захисту є, мабуть, одними з найнадійніших методів захисту, оскільки вони захищають саму інформацію, а не доступ до неї (наприклад, зашифровані файли неможливо прочитати, навіть якщо носій інформації викрадено). Цей метод захисту реалізується у вигляді програм і програмних пакетів.

Сучасні системи захисту зашифрованої інформації мають такі вимоги: зашифровані повідомлення можуть бути прочитані лише за наявності ключа; кількість операцій, необхідних для визначення ключа шифрування за фрагментом зашифрованого повідомлення та відповідного йому відкритого тексту, має бути не меншою за загальну кількість можливих ключів; кількість операцій, необхідних для отримання ключа та розшифрування інформації, повинна мати визначену нижню межу і бути поза можливостями сучасних комп’ютерів (з урахуванням можливості використання мережевих обчислень); знання алгоритму шифрування не повинно впливати на надійність захисту; незначні зміни в ключі, навіть при використанні одного і того ж ключа, не повинні призводити до суттєвих змін у вигляді зашифрованого повідомлення; ; структурні елементи алгоритму шифрування повинні бути інваріантними; будь-які додаткові біти, введені в повідомлення в процесі шифрування, повинні бути повністю і надійно приховані в шифротексті; довжина зашифрованого тексту повинна дорівнювати довжині відкритого тексту; між ключами, що використовуються в процесі шифрування, не повинно бути простих (легко встановлюваних) залежностей;

повинна бути можливість забезпечити надійний захист інформації з будь-яким з можливих наборів ключів [10].

Алгоритм повинен бути придатним як для програмної, так і для апаратної реалізації, а зміна довжини ключа не повинна призводити до якісної деградації алгоритму шифрування.

Алгоритми шифрування, які називаються алгоритмами шифрування, представлені певними математичними функціями, що використовуються для шифрування та дешифрування. Точніше, є дві такі функції, одна з яких використовується для шифрування, а інша – для розшифрування [11].

При симетричному шифруванні створюється ключ, файл з цим ключем пропускається через програму шифрування і результат надсилається до місця призначення, тоді як сам ключ надсилається до місця призначення окремо, використовуючи інший (безпечний або дуже безпечний) канал зв’язку.

Асиметричне шифрування складніше, але й надійніше. Воно вимагає двох незалежних один від одного ключів: відкритого і закритого.

Одержувач повідомляє всім свій відкритий ключ, який потім може бути використаний для шифрування повідомлення. Закритий ключ відомий тільки одержувачу повідомлення. Якщо комусь потрібно надіслати зашифроване повідомлення, він шифрує його за допомогою відкритого ключа одержувача. Після отримання повідомлення одержувач розшифровує його за допомогою свого приватного ключа. Підвищена безпека асиметричного шифрування досягається ціною більш тривалої процедури дешифрування через підвищену обчислювальну складність.

У сучасному світі найнадійнішими методами захисту інформації є криптографічні алгоритми та засновані на них протоколи безпечного обміну інформацією і цифрові підписи. Загалом, криптографія – це наука про математичні методи захисту цілісності та автентичності інформації. До основних алгоритмів криптографічного захисту належать: DES, AES, Camellia, Twofish, Blowfish, IDEA, RC4, RSA, Elgamal тощо. Хешування, асиметричне шифрування, симетричне шифрування та електронний цифровий підпис (ЕЦП) [11].

Хешування – це метод криптографічного захисту, який полягає в контрольованому перетворенні інформації. Хеш-значення фіксованої довжини обчислюється з даних необмеженого розміру шляхом виконання криптографічного перетворення і однозначно відповідає вихідним даним.

2.2 Методи автентифікації та авторизації в мережах

Автентифікація – це процес перевірки особи користувача. Він визначає, хто намагається отримати доступ до системи або програми. Зазвичай процес автентифікації передбачає введення імені користувача та пароля. Однак він може бути складнішим, наприклад, з використанням біометричних даних (відбитки пальців, розпізнавання обличчя) або двофакторної автентифікації (пароль і код, отриманий на мобільний телефон) [12].

Автентифікація гарантує, що тільки власник облікового запису може отримати доступ до нього. Правильно налаштована автентифікація запобігає несанкціонованому доступу до системи та захищає персональні дані користувача. Техніки автентифікацію бувають різні, але нижче розглянемо основні з них: автентифікація на основі пароля – це простий і широко використовуваний метод, за допомогою якого користувач надає ім’я користувача або адресу електронної пошти та пароль для доступу до системи або програми. Пароль порівнюється з хеш-значенням, що зберігається в системі, для перевірки того, що користувач має право доступу до системи; безпарольна автентифікація дозволяє отримати доступ до систем і додатків без необхідності вводити пароль, що позбавляє користувачів необхідності створювати і запам’ятовувати складні паролі. Замість цього користувач автентифікується за допомогою інших засобів, таких як біометричні дані, токени або смарт-карти; 2FA/MFA (двофакторна/багатофакторна автентифікація) – це метод, який вимагає від користувачів надання двох або більше форм автентифікації для доступу до системи або програми. Це включає введення пароля та сканування відбитків пальців; єдиний вхід (SSO) дозволяє користувачам отримувати доступ до декількох додатків або систем за допомогою

одного набору облікових даних для входу. Цей метод зменшує необхідність користувачам запам’ятовувати кілька паролів і спрощує процес входу в систему. SSO зазвичай використовується в корпоративному середовищі, де співробітникам потрібно отримати доступ до різних систем і додатків; соціальна автентифікація дозволяє користувачам отримувати доступ до систем і додатків за допомогою облікових даних соціальних мереж, таких як акаунти Facebook або Google. Ця технологія спрощує процес автентифікації користувачів і може бути більш безпечною, ніж автентифікація на основі пароля, оскільки платформи соціальних мереж часто мають вдосконалені заходи безпеки [13].

Авторизація – це процес визначення того, до яких ресурсів або функцій користувач може отримати доступ після успішної автентифікації. Після встановлення особи користувача система визначає, які дії він може виконувати і які ресурси може переглядати або редагувати. Наприклад, системні адміністратори мають більше прав доступу, ніж звичайні користувачі.

Авторізація – це механізм, який гарантує, що користувачі мають доступ лише до того, до чого вони мають право доступу, і не можуть виконувати дії, на які вони не уповноважені [13].

Існують різні типи авторизації, кожен з яких має свої переваги та недоліки: контроль доступу на основі ролей (RBAC) – цей тип авторизації надає доступ до ресурсів на основі ролі користувача в організації; контроль доступу на основі атрибутів (ABAC) –цей тип авторизації надає доступ до ресурсів на основі атрибутів користувача, таких як посада, відділ, місцезнаходження тощо; обов’язковий контроль доступу (MAC) – цей тип авторизації ґрунтується на загальносистемних політиках, які визначають, які користувачі або процеси можуть отримати доступ до певних ресурсів; дискреційний контроль доступу (DAC) – цей тип авторизації дозволяє окремим користувачам контролювати доступ до ресурсів, якими вони володіють або якими керують; контроль доступу на основі правил (RBAC) – цей тип авторизації надає доступ до ресурсів на основі набору заздалегідь визначених правил, які можуть створювати адміністратори або самі користувачі.

Основна відмінність між цими двома процесами полягає в тому, що перший перевіряє особу користувача, тоді як другий визначає, що користувач може робити після того, як його особу перевірено. Важливо розуміти цю відмінність, оскільки саме другий процес є більш важливим, ніж перший, оскільки саме він є більш важливим. Це пов’язано з тим, що без належної авторизації авторизація не має сенсу. Система не може перевірити, що користувач з правильними повноваженнями - це дійсно він/вона [14].

Автентифікація та авторизація можуть звучати схоже, але насправді це різні процеси, які слугують різним цілям у забезпеченні безпечного доступу до ресурсів. Автентифікація полягає у перевірці особи користувача, тоді як авторизація у прийнятті рішення про те, що дозволити користувачеві робити після того, як його особу перевірено.

Іншими словами, автентифікація – це встановлення довіри, а авторизація - управління цією довірою. Наприклад, коли користувач вводить ім’я користувача та пароль для входу на вебсайт, він проходить процес автентифікації. Після входу сайт використовує автентифікацію, щоб визначити, які дії користувач має право виконувати, наприклад, переглядати певні сторінки або надсилати форми [13].

Контроль доступу є важливим елементом процесу автентифікації та авторизації. Контроль доступу гарантує, що тільки авторизовані користувачі можуть отримати доступ до ресурсів, і що вони можуть отримати доступ тільки до тих ресурсів, на використання яких вони уповноважені. При впровадженні контролю доступу дуже важливо розуміти різницю між автентифікацією та авторизацією. Автентифікація перевіряє особу користувача, тоді як авторизація визначає, які дії користувач може виконувати після автентифікації.

Інформаційна безпека є ще одним важливим аспектом автентифікації та авторизації. Надійні протоколи автентифікації та авторизації допомагають забезпечити конфіденційність, цілісність і доступність інформації. Захищаючи конфіденційні дані та системи від кіберзагроз, належні протоколи автентифікації та авторизації можуть допомогти запобігти витоку даних та іншим інцидентам безпеки [14].

Недостатня автентифікація та авторизація може мати серйозні наслідки. Без належної автентифікації та авторизації неавторизовані користувачі можуть отримати доступ до конфіденційних даних і систем, що призведе до витоку даних і збоїв у роботі системи. Такі інциденти можуть призвести до фінансових втрат, шкоди репутації та юридичної відповідальності.

Щоб уникнути таких інцидентів, необхідно впровадити надійні протоколи автентифікації та авторизації. Ці протоколи повинні включати кілька факторів автентифікації, таких як паролі, біометричні дані та токени. Крім того, контроль доступу має ґрунтуватися на принципі найменших привілеїв і гарантувати, що користувачі мають доступ лише до тих ресурсів, які їм потрібні для роботи.

2.3 Розгляд методів захисту від розподілених атак

Останнім часом з’являється все більше повідомлень про хакерів і злом програмного забезпечення, часто без жодних пояснень, що таке DDoS-атака і яку небезпеку вона становить для серверів.

DDoS-атака – це абревіатура від «Distributed Denial of Service», що означає розподілену атаку на відмову в обслуговуванні; мета DDoS-атаки - порушити і зупинити нормальну роботу сервера, сервісу або локальної мережі, або унеможливити доступ до них добросовісних користувачів ускладнити доступ до них добросовісним користувачам. Це досягається шляхом генерування інтернет-трафіку, для обробки якого комп’ютерна система не має достатніх ресурсів [15].

Атакуючий трафік генерується декількома комп’ютерами або локальними мережами, включаючи пристрої Інтернету речей. В результаті зловмисних дій окремої особи або групи хакерів генерується низка запитів до атакованої комп’ютерної системи, що дозволяє зловмиснику отримати несанкціонований доступ до цінної інформації. Це можуть бути конфіденційні бази даних, програмний код, версії програмного забезпечення тощо.

До DDoS-атак вразливі лише комп’ютерні системи, підключені до Інтернету. Глобальна мережа складається з безлічі комп’ютерів та інших

пристроїв, підключених до Інтернету, частина з яких у різний спосіб заражена шкідливим програмним забезпеченням. Фахівці називають останніх ботами , а групу – ботнетом [15].

Одразу після створення такої системи хакери можуть організовувати DDoS-атаки:

Вони створюють спеціальні інструкції для окремих роботів і розсилають їх мережею. Отримавши їх, керований комп’ютер або система починає генерувати та надсилати запити на IP-адресу локальної мережі або сервера, що атакується. Спочатку це уповільнює трафік і перевантажене обладнання починає давати збої. В результаті весь трафік, включаючи трафік звичайних користувачів, виявляється заблокованим. Основна проблема протидії розподіленим атакам на відмову в обслуговуванні полягає в тому, що вкрай складно відрізнити атакуючий трафік від звичайного. Кожен бот, який використовують хакери, є легітимним інтернет-пристроєм, і відрізнити зловмисні запити від нормальних вкрай складно.

Основними ознаками DDoS-атаки на сервер є раптове уповільнення роботи сервера або відсутність доступу до сервісу чи іншого вебсайту. Водночас труднощі можуть бути викликані природними причинами, наприклад, раптовим збільшенням нормального трафіку. Загальнодоступні сервіси аналізу можуть виявити DDoS-атаки за низкою характерних ознак: великі обсяги трафіку з однієї або декількох IP-адрес, що належать до одного діапазону; єдиний поведінковий профіль (геолокація, версія браузера або тип пристрою) великої кількості користувачів, які запитують доступ до аналізованої вебсторінки; сплески трафіку через певні проміжки часу, наприклад, кожні дві-три години або за різними графіками; вибухове зростання кількості запитів до одного з інтернет-сервісів або вебсторінок [16].

Існують і інші ознаки, притаманні певним видам розподілених атак типу «відмова в обслуговуванні». У таких випадках можливостей традиційних інструментів інтернет-аналізу може бути недостатньо, і для виявлення потрібно спеціальне програмне забезпечення.

Найбільшою проблемою в захисті від хакерських атак є визначення різниці між атакуючим трафіком і звичайним трафіком. Під час рекламної кампанії нового продукту багато користувачів можуть відвідати вебсайт розробника. Це призводить до аварійного відключення трафіку, що є помилкою: якщо вебсайт отримує сплеск трафіку від відомої хакерської групи, слід вжити заходів для пом’якшення наслідків розподіленої атаки на відмову в обслуговуванні.

Спроби зламу вебресурсів можуть приймати різні форми, від простого джерела підозрілого трафіку до найскладніших багатовекторних атак. В останньому випадку використовується відразу кілька типів DDoS-атак, що розподіляють сили і ресурси захисника в різних напрямках [16].

Прикладом такого багатовекторного впливу є комбінована DDoS-атака відразу на декількох рівнях: поєднання DNS-ампліфікації і великої кількості HTTP-запитів. Запобігання таким атакам вимагає одночасного застосування декількох контрзаходів.

Складність протидії зростає, коли зловмисники об’єднують різні методи атаки в розподілену DoS-атаку. Хакери намагаються максимально змішати атакуючий трафік зі звичайним, зводячи ефективність захисних заходів до нуля.

Спроби просто відключити або обмежити трафік без фільтрації рідко дають хороші результати. У цьому випадку DDoS-атака адаптується і шукає шляхи обходу контрзаходів. У цьому випадку найкращим рішенням є використання багаторівневих стратегій захисту.

3 ВІДБИТКИ БРАУЗЕРІВ

3.1 Методи збору та використання відбитків браузерів

Збір і використання відбитків пальців браузера – одна з найактуальніших тем у сфері інформаційної безпеки та конфіденційності в Інтернеті на сьогоднішній день. З розвитком технологій і поширенням онлайн-сервісів відбитки пальців браузера стають все більш важливим джерелом інформації для рекламодавців, маркетологів і кіберзлочинців.

Фінгерпринтинг (або ж відбитки браузерів) – це унікальний ідентифікатор, створений за допомогою технології, яка створює цифровий «відбиток» комунікаційного пристрою користувача. Технологія базується на аналізі інформації, що надсилається веббраузером на інтернет-ресурси, які відвідує користувач. Вона ідентифікує користувача за унікальними особливостями веббраузера, системи та комунікаційного пристрою, а не за спеціальною міткою, що зберігається на комунікаційному пристрої [18].

Відбитки браузера – це необов’язковий оригінальний зліпок вашого персонального комп’ютера, але спеціальні механізми вебсайтів мають можливість здійснювати спостереження за вами. Фінгерпринтинг є альтернативою файлам cookie, але мають ряд переваг.

Відбитки пальців іноді порівнюють з браузерними файлами cookie, але хоча вони служать одній меті, вони працюють зовсім по-різному. Файли cookie більше схожі на пристрій відстеження, який, потрапляючи на ваш комп’ютер, дозволяє вебсайту знати, де ви знаходитесь і що робите. Відбитки пальців браузера більш статичні. Відбитки пальців браузера більш статичні і використовують встановлені дані про вас і ваш пристрій, щоб точно визначити, хто ви, і записати інформацію про те, коли ви відвідуєте сайт, але не можуть відстежувати вас.

З цієї причини, незважаючи на те, що ви можете відключити файли cookie, дані, які вони збирають, мають велику цінність. Крім того, браузери все частіше блокують сторонні файли cookie, щоб запобігти відстеженню користувачів. Відбитки пальців є майже повною протилежністю, оскільки більшість даних, які

вони передають, необхідні для інтернет-серфінгу, тому їх неможливо відключити. Відбитки пальців менш вразливі, але майже невидимі, і тому їх практично неможливо вимкнути.

Для зняття відбитків браузера використовується великий список точок даних, які створюють відбиток вашого браузера. Відбиток, ймовірно, буде надзвичайно унікальним [18].

Збір та використання відбитків браузерів викликає все більше занепокоєння з точки зору конфіденційності та безпеки в Інтернеті. Ці дані можуть бути використані для створення детальних профілів користувачів, що порушує конфіденційність. Крім того, зловмисники можуть використовувати ці дані для відстеження, розсилки спаму або кібератак.

Розуміючи основні способи збору відбитків пальців браузера, користувачі можуть усвідомлювати ризики і вживати заходів для захисту своєї приватності в Інтернеті. Важливою частиною захисту є використання інструментів анонімізації та безпеки, таких як використання VPN, блокування відстеження та використання розширень конфіденційності.

Збереження конфіденційності в Інтернеті вимагає постійної уваги до технологій і здатності виявляти потенційні загрози. Поінформованість і заходи безпеки є ключовими для збереження особистої конфіденційності та безпеки в цифровому світі [17].

3.2 Оцінка приватності та безпеки зібраних відбитків браузерів

Оцінка приватності та безпеки зібраних відбитків пальців браузера стає все більш важливою в епоху цифрової взаємодії. З кожним кліком ми залишаємо слід в інтернеті, і ці сліди, зібрані браузерами, можуть містити велику кількість персональних даних.

Для запобігання унікальності цифрових відбитків пристроїв комунікації за рахунок веббраузерів необхідно використовувати частіше оновлення

веббраузерів, застосовувати плагини для блокування запуску JavaScript та Flash, видалити нестандартні шрифти з операційної системи тощо.

Також існує спосіб завдання недостовірних даних для спеціалізованих інтернет-сервісів, що формують цифрові відбитки пристроїв комунікації. Наприклад, можна змінити вручну такі дані:

- змінити часовий пояс;
- встановити «зайві» плагіни в веббраузер;
- відвідувати безліч інтернет-ресурсів у випадковому порядку за допомогою спеціалізованих плагінів;
- змінити базову (англійську) мову веббраузера;
- не відкривати «на весь екран» веббраузер;
- змінити масштаб відображення веб-сторінок на екрані і так далі.

Використання такого способу, дозволить внести у цифровий відбиток пристрою комунікації забагато надлишкової інформації, що приведе до його спотворення і як наслідок зниження його унікальності [19].

Крім того, слід відзначити, що спеціалізовані інтернет-ресурси можуть «забувати» про веббраузери окремої конфігурації. Це показує тест, в якому користувач відвідує експериментальний інтернет-ресурс декілька разів, а потім повертається на нього через деякий час. Результати цього тесту не є надто точними. Унікальність цифрових відбитків веббраузерів, з яких заходили на інтернет-ресурс повторно через 2-2,5 тижні, знижувалась на 30% та більше. Таким чином, можна умовно вважати, що зміни наступають вже після 5 днів відсутності активності пристрою комунікації у цифровому просторі.

Ще кращий результат можна отримати при зміні часового поясу. Користувачі, які мешкають у різних часових поясах, виставляли неправильний час, а після відвідування інтернет-ресурсу змінювали його на правильний. У користувача з найбільш віддаленим (від початкового показника) часовим відрізком унікальність знижувалась максимально.

Досить ефективно знижує створення цифрових відбитків відключення виконання Flash, JavaScript та WebGL без посередньо у самих веббраузерах.

Якщо це не можливо, то необхідно скористатися спеціалізованими плагінами для блокування запуску JavaScript та Flash сценаріїв. Це набагато ускладнює визначення унікальності веббраузера та пристрою комунікації.

3.3 Дослідження різних браузерів за рівнем захисту

Сьогодні такі веббраузери, як Google Chrome, Opera, Microsoft Internet Explorer, Mozilla Firefox та Apple Safari встановлені майже на всіх комп'ютерах. Оскільки веббраузери використовуються часто, налаштування безпеки є важливими [19].

Однак веббраузери, які постачаються разом з операційною системою (ОС), часто не мають таких налаштувань за замовчуванням.

Якщо не налаштувати параметри безпеки веббраузера, це може призвести до різноманітних проблем з комп'ютером, наприклад, до встановлення шпигунського програмного забезпечення без відома користувача або до отримання зловмисниками контролю над комп'ютером.

Мета веббраузера – отримувати вміст з Інтернету і відображати його на пристрої користувача.

У 2020 році дослідники інтернет-безпеки підготували звіт про стан сучасних веббраузерів на основі дослідження використання основних браузерів 1,4 мільйонами користувачів по всьому світу. Основним висновком стало те, що майже третина всіх веббраузерів містять критичні вразливості:

– Microsoft Internet Explorer і Edge – понад 40%;

– Google Chrome – трохи менше 40%;

– Mozilla Firefox – 35%;

– Opera – 34%;

– Safari менше – 30%

У 2024 році існує безліч браузерів, деякі з яких вирізняються особливими перевагами. Нижче наведено список найпоширеніших браузерів та їхніх основних переваг:

– Google Chrome: надійний, швидкий і багатий на розширення;

– Mozilla Firefox: з відкритим вихідним кодом, має потужні інструменти для розробників і добре захищений;

– Microsoft Edge: інтегрований у Windows 10, працює швидко та ефективно;

– Safari: оптимізований для використання на пристроях Apple, швидкий та з унікальними функціями;

– Opera: має вбудовану VPN, працює швидко навіть при слабкому з'єднанні та має розширений набір інструментів.

Кожен з цих браузерів має свої недоліки, але їхні переваги роблять їх найпопулярнішими серед користувачів 2024 року [19].

Однією з найважливіших характеристик найпопулярніших браузерів у 2024 році є їхня здатність забезпечувати безпеку під час перегляду вебсторінок. У цьому відношенні кожен з цих браузерів має свої сильні та слабкі сторони.

Одним з найбільш використовуваних браузерів цього року є Google Chrome. Його безпека базується на низці розширень, які можуть блокувати небажані завантаження файлів і рекламу. Крім того, Chrome має вбудований захист від шкідливих вебсайтів, які можуть завдати шкоди комп'ютеру користувача. Однак цей браузер має той недолік, що він використовує багато пам'яті і сповільнює роботу комп'ютера.

Іншим популярним браузером є Mozilla Firefox. Безпека цього браузера базується на використанні відкритих технологій, що дозволяє швидше виявляти та усувати вразливості; Firefox також пропонує можливість блокувати сторінки зі шкідливим програмним забезпеченням та рекламою. Однак недоліком Firefox є те, що багато розширень можуть призвести до вразливостей у безпеці.

Це може призвести до вразливостей у системі безпеки.

Microsoft Edge, один з найпопулярніших браузерів у 2024 році, також має один недолік з точки зору безпеки. Він заснований на технології Windows Defender SmartScreen, яка блокує шкідливе програмне забезпечення та фішингові сайти. Крім того, Edge також пропонує анти-трекінг і вбудований менеджер

паролів. Однак недоліком Edge є його обмежені можливості розширення порівняно з іншими браузерами.

Загалом, найпопулярніші браузери 2024 року мають різні сильні та слабкі сторони з точки зору безпеки. Вибір того, якому браузеру віддати перевагу, залежить від особистих уподобань користувача та його потреб у безпеці під час перегляду вебсторінок [19].

3.4 Аналіз браузеру Mozilla Firefox на створення цифрового відбитку

З метою оцінки можливості створення цифрового відбитка пристрою комунікації веббраузера та визначення ступеню його унікальності було використано спеціалізований інтернет-ресурс *panopticlick.eff.org*, який дозволяє здійснювати перевірку унікальності цифрового відбитку поточного веббраузеру, інформуючи користувача про ступінь його унікальності [18].

У випадку, якщо отримані результати перевірки незадовільні, необхідно виконувати конфігурування веббраузеру та здійснювати тестування доти, поки його унікальність веббраузера не знизиться до припустимих показників.

Для постановки експерименту з визначення цифрового відбитка в якості пристрою комунікації був обраний стаціонарний персональний комп’ютер з операційною системою Windows 7, версія 64 біт, веббраузер Mozilla Firefox, версія 93, 64 біта з встановленим плагіном Umatrix.

Особливістю цього плагіна є те, що він дозволяє здійснювати перегляд, і вибіркове блокування структурних елементів, що завантажуються з інтернет-сторінок з розкладкою по їх доменах і піддоменах, з яких здійснюються запити, що посилаються у веббраузер (рисунок 3.1).

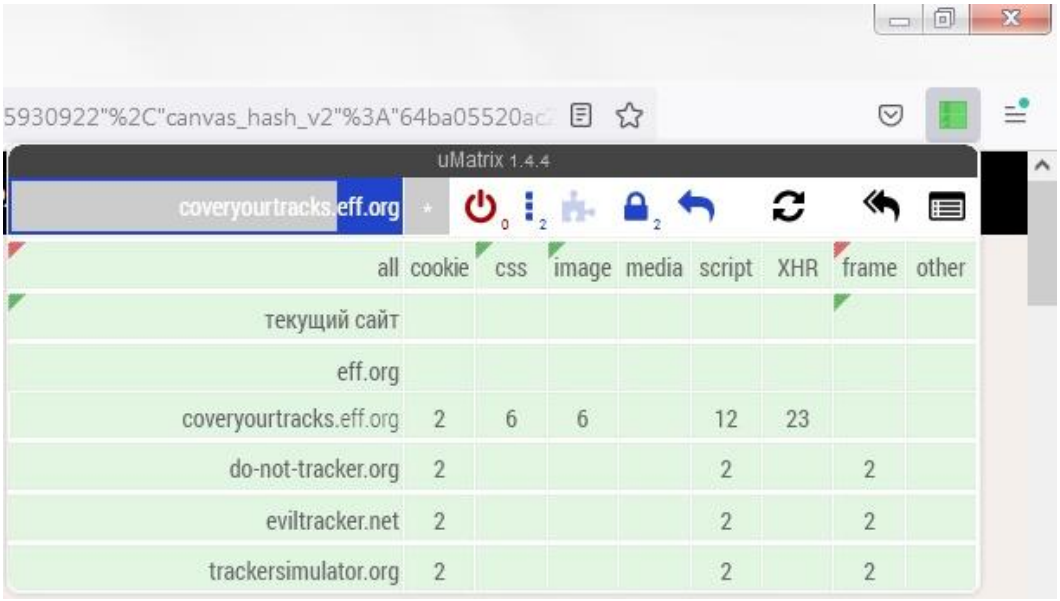

Рисунок. 3.1 – Робота плагіну Umatrix на інтернет-ресурсі *panopticlick.eff.org*.

До елементів, що приймають участь у створенні цифрового відбитку пристрою комунікації за допомогою веббраузерів відносяться:

Cookie – невеликий фрагмент даних, що відправляється інтернет-ресурсам на веббраузер, який може зберігатися і відсилатися на інтернет-ресурс з новим запитом.

CSS (Cascading Style Sheets) – код, який використовується для стилізації інтернет-сторінок (завдання кольорів, шрифтів, стилів, розташування окремих блоків та інших аспектів представлення зовнішнього вигляду).

Image – вносить зміни в графічні образи, присутні на інтернет-сторінці.

Media – запити, що виявляють мобільні пристрої комунікації; створюють адаптивний макет проглядається ресурсу, який підлаштовується під дозвіл монітора і вікна веббраузера, змінюючи при необхідності ширину макета, число колонок, розміри зображень і тексту.

Script (JavaScript) – забезпечує: перевірку правильності заповнення форм на інтернет-ресурсі; відправку статистичної та аналітичної інформації в спеціалізовані інтернет-ресурси; різні візуальні ефекти.

XHR (XMLHttpRequest) – вбудований в веббраузер об’єкт, який дає можливість робити HTTP-запити до інтернет-ресурсу без перезавантаження

інтернет-сторінки. Він використовує запити HTTP або HTTPS безпосередньо до вебсервера і завантажує дані відповіді сервера безпосередньо в викликає скрипт.

Frame – окремий закінчений HTML-документ, який разом з іншими HTML-документами може бути відображений у вікні браузера.

Other – інші елементи інтернет-сторінок.

Гнучкість налаштувань цього плагіну дозволяє отримати користувачу повний контроль над відгуками його веббраузера на всі запити, що надходять від всіх доменів, що пов’язані з поточним інтернет-ресурсом. Користувач сам вирішує, з якими доменами здійснювати обмін даними – тим самим він повністю контролює створення цифрового відбитку пристрою комунікації [21].

Результати експериментальних досліджень формування цифрових відбитків пристрою комунікації за допомогою веббраузеру та встановленим плагіном Umatrix наведені у таблиці 3.1.

Таблиця 3.1 - Результати повного дослідження для веббраузера на можливість створення цифрового відбитку

Признаки ідентифікації	Веббраузер	Наявність створеного цифрового відбитка при блокуванні елементів (+/-)							
		Cookie	Css	Image	Media	Script	XHR	Frame	other
User Agent	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0	+	+	+	+	-	+	+	+
HTTP_ACCEPT Headers	text/html, */*; q=0.01 gzip, deflate, br ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3	+	+	+	+	-	+	+	+
Browser Plugin Details	undefined	+	+	+	+	-	+	+	+
Time Zone Offset	-120	+	+	+	+	-	+	+	+

Продовження таблиці 3.1

Time Zone	Europe/Kiev	+	+	+	+	-	+	+	+
Screen Size and Color Depth	1920x1080x24	+	+	+	+	-	+	+	+
System Fonts	Arial, Arial Black, Arial Narrow, Arial Rounded MT Bold, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New, Georgia, Helvetica, Impact, Lucida Console, Lucida Sans, Lucida Sans Typewriter, Lucida Sans Unicode, Microsoft Sans Serif, Monotype Corsiva, MS Gothic, MS PGothic, MS Reference Sans Serif, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Light, Segoe UI Semibold, Segoe UI Symbol, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript)	+	+	+	+	-	+	+	+
Are Cookies Enabled?	Yes	+	+	+	+	-	+	+	+
Limited supercookie test	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No, openDatabase: false, indexed db: true	+	+	+	+	-	+	+	+
Hash of canvas fingerprint	64ba05520ac2959d29b1a88cf185dafd	+	+	+	+	-	+	+	+
Hash of WebGL fingerprint	87456eae57dba74c1cf4d1b5f4212e11	+	+	+	+	-	+	+	+
WebGL Vendor & Renderer	Google Inc.~ANGLE (NVIDIA GeForce GTX 480 Direct3D11 vs_5_0 ps_5_0)	+	+	+	+	-	+	+	+

Продовження таблиці 3.1

DNT Header Enabled?	True	+	+	+	+	-	+	+	+
Language	ru-RU	+	+	+	+	-	+	+	+
Platform	Win32	+	+	+	+	-	+	+	+
Touch Support	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false	+	+	+	+	-	+	+	+
Ad Blocker Used	False	+	+	+	+	-	+	+	+
AudioContext fingerprint	35.7383295930922	+	+	+	+	-	+	+	+
CPU Class	N/A	+	+	+	+	-	+	+	+
Hardware Concurrency	4	+	+	+	+	-	+	+	+
Device Memory (GB)	N/A	+	+	+	+	-	+	+	+

Аналіз отриманих даних (див. таблицю 3.1) показує, що створення цифрових відбитків здійснюється з обов’язковим використанням елемента *Script* за умови його наявності в коді завантажуваних інтернет-сторінок. Більш того, при здійсненні блокування виконання будь-яких елементів *Script* було встановлено, що це призводить до неможливості створення цифрових відбитків веббраузера і як наслідок до неможливості ідентифікації пристрою комунікації користувача [18].

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було проведено пошук та аналіз різноманітної інформації про сучасні підходи та методи захисту інформації – одне із завдань та завдань даної роботи.

Більше мільярда людей активно користуються Інтернетом, при цьому їхній онлайн-захист в значній мірі залежить від програмного забезпечення, що використовується для доступу до вебсайтів та їх перегляду у веббраузері. Проте багато користувачів часто не приділяють уваги налаштуванням безпеки, що створює серйозні ризики в обличчі зростаючої загрози атак. Вразливості веббраузерів стали популярним методом для зловмисників, що дозволяє їм скомпрометувати комп’ютерні системи.

Однією з найбільш критичних вразливостей браузера, яка була розглянута, є зчитування відбитків браузера. Загроза порушення конфіденційності стоїть за цим, що робить користувача уважним. Відбиток браузера майже не змінюється з часом, що робить ідентифікацію майже недвозначною, а також він містить значну кількість інформації. Крім того, налаштування захисту від інших вразливостей також включається до відбитка веббраузера.

Зловмисник може використовувати ці дані для створення експлойтів або «цифрових двійників», що може завдати значної шкоди користувачеві. На сьогоднішній день не існує гарантовано ефективних методів та засобів захисту від технології зчитування відбитка браузера, проте після аналізу заходів, спрямованих на зниження унікальності веббраузера, одним з найефективніших виявилося застосування спеціалізованих розширень.

У кваліфікаційній роботі було відображено як саме зловмисники можуть зчитувати відбитки браузерів та використовувати їх у своїх цілях. Також були наведені деякі алгоритми як забезпечити себе від легкого зчитування цифрових відбитків веббраузерів зловмисниками, такі як зміна часового поясу, встановлення «зайвих» плагінів на комп’ютер тощо.

Таким чином, можна сказати, що технологія створення відбитків веббраузерів базується на зборі великої кількості даних про комунікаційні пристрої користувачів. Повністю запобігти фінгерпрінтингу неможливо, але можливість ідентифікації користувача можна звести до мінімуму, встановивши спеціалізовані плагіни, які дозволяють контролювати виконання скриптів (найбільше це стосується Java і Flesh), доступ до яких здійснюється на сторінках Інтернет-ресурсів.

На сьогоднішній день існує багато методів захисту інформації в мережі, але жоден з ним не може гарантувати безпеку на 100 відсотків.

Тому актуальним на сьогоднішній день є розширення комплексу методів та підходів із мережевого захисту системи, які допоможуть зменшити ризики зчитування приватних даних користувачів та мінімізувати їх вразливості.

ПЕРЕЛІК ПОСИЛАНЬ

1. Організація комп’ютерних мереж. URL: https://marytisna.blogspot.com/2017/12/blog-post.html
2. З.Б. Живко, М.О. Живко. Тези доповідей ІІ міжнародної НПК «Безпека та захист інформації в інформаційних системах» URL: https://core.ac.uk/download/pdf/232881194.pdf
3. Загрози інформаційної безпеки. Матеріал з вікіпедії – вільної енциклопедії. URL: https://uk.wikipedia.org/wiki/Загрози_інформаційної_безпеки
4. Про основні засади забезпечення кібербезпеку України : Закон України від 05.10.2017р. № 2163-VIII. Дата оновлення 21.06.2018р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19
5. Система мережевої безпеки, її значення для розвитку бізнесу. URL: https://vikna.if.ua/cikavo/129634/view
6. Технології захисту інформації. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186
7. Про захист інформації в автоматизованих системах : Закон України від 31.05.2005р. № 2594-V URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text
8. Захист інформації у контексті забезпечення інформаційної безпеки. URL: http://surl.li/tpqjr
9. Захист інформації. Енциклопедія сучасної України. URL: https://esu.com.ua/article-15872
10. Криптографічні методи захисту інформації. URL: https://classmill.com/659/112/m/xnb7A
11. Класифікація криптографічних алгоритмів. URL: http://ypn.ru/228/classification-of-cryptographic-algorithms/.
12. Автентифікація та авторізація даних. URL: https://it-rating.ua/autentifikatsiya-ta-avtorizatsiya-zahist-danih-koristuvachiv
13. Різниця між автентифікацію та авторизацією. URL: https://foxminded.ua/riznytsia-mizh-avtentyfikatsiieiu-ta-avtoryzatsiieiu/

14. Різниця між автентифікацію та авторизацією.URL: https://goo.su/D26g1
15. DDoS атака – що це таке та в чому небезпека для серверу? URL: https://goo.su/QmgmMl
16. Distributed Denial of Service. URL: https://stormwall.pro/knowledgebase/termin/ddos-protection
17. Табала К. А. Сучасні напрями забезпечення кіберзахисту та удосконалення інформаційних технологій. Суспільство та держава в умовах воєнного стану: виклики та перспективи, 27 квітня 2024 р. Одеса, 2024.
18. Табала К. А. Цифрові відбитки веббраузерів. Кібербезпека в сучасному світі : матеріали III Всеукраїнської науково-практичної конференції, 19 листопада 2021 р. Одеса, 2021. С. 77-80.
19. Переваги та недоліки найпопулярніших браузерів 2024 року. URL: https://mediacom.com.ua/perevagi-ta-nedoliki-najpopulyarnishix-brauzeriv-2024-roku-oglyad-ta-porivnyannya/
20. Securing Your Web Browser. URL: https://us-cert.cisa.gov/publications/securingyour-web-browser
21. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 1999.04.28]. Київ, 1999. 60с. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf
22. Mozilla. What is a browser? URL: https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/
23. What is a web browser? // Mozilla. URL: https://www.mozilla.org/enUS/firefox/browsers/what-is-a-browser/
24. Simon Kemp. Digital 2021: Global Overview Report. URL: https://datareportal.com/reports/digital-2021-global-overview-report.
25. Jan Teichmann. Single UserID Matching for Anonymous Users Across Devices with GraphX. URL: https://cutt.ly/iHbrAcT
26. Positive Technologies. Виявлено спосіб деанонімізації користувачів за допомогою «звукових відбитків» SecurityLab, URL: http://www.securitylab.ua/news/482344.php

27. What Is Browser Fingerprinting & How Does It Work? Seon, 2023. URL: http://surl.li/hfscp.
28. Doty N. Mitigating Browser Fingerprinting in Web Specifications. W3C: World Wide Web Consortium, URL: https://w3c.github.io/fingerprinting-guidance
29. Каланча А. А., Світличний В. А. Засоби забезпечення анонімності в мережі. URL: http://surl.li/hfqqh.
30. Когут Ю.І. «Кібербезпека та ризики цифрової трансформації компаній», Київ, 2021. – 370 с.