DOI: https://doi.org/10.36910/6775-2524-0560-2021-45-12
УДК 343.9:004.056.5
Міскевич Оксана Іванівна, асистент
https://orcid.org/0000-0002-5009-2391
Луцький національний технічний університет

ДОСЛІДЖЕННЯ ЗАГРОЗ ВІД КІБЕРАТАК ТА ЗАХИСТ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ

Міскевич О. І. Дослідження загроз від кібератак та захист персональної інформації. У даній статті представлено основні групи для отримання кібердоступу до засобів обчислювальної техніки. Детально розглянуто безпосереднє, електромагнітне, аудіо та відео перехоплення. Досліджено куб кібербезпеки та недавні кібератаки а також безпеку інфраструктури Google для нашої персональної інформації.
Ключові слова: кібератака, цілісність, доступність, конфеденційність, аутентифікація, Куб Мак-Камбера, CIA Triad, Атака TalkTalk.

Мискевич О. И. Исследование угроз от кибератак и защита персональной информации.В данной статье представлены основные группы для получения кибердоступа к средствам вычислительной техники. Рассмотрены непосредственное, электромагнитное, аудио и видео перехваты. Исследованы куб кибербезопасности и недавние кибератаки а также безопасность инфраструктуры Google для нашей персональной информации.
Ключевые слова: кибератака, целостность, доступность, конфиденциальность, аутентификация, Куб Мак-Камбер, CIA Triad, Атака TalkTalk.

Miskevich O. Cyberattack threat research and protection of personal information. This article presents the main groups for obtaining cyber access to computer equipment. Direct, electromagnetic, audio and video interception are considered in detail. We've explored the cybersecurity cube and recent cyberattacks, as well as the security of Google's infrastructure for our personal information.
Keywords: cyberattack, integrity, availability, confidentiality, authentication, McCumber Cube, CIA Triad, TalkTalk Attack.

Постановка наукової проблеми: Незалежно від нашої сфери діяльності кібербезпека на сьогодні займає головне місце, а основна задача, яка стоїть перед кожним – це як захистити себе від кіберзлочинців та атак, які так стрімко зростають не тільки в Україні, а й у світі та проаналізувати як впливають атаки та збої соціальних мереж на суспільство.

Аналіз досліджень. На сьогоднішній день комп'ютери, смартфони та інша техніка та програми стають більш поширеними і застосовуються не тільки для особистого користування – а й на державному рівні. Тому чим більше ми оцифровуємо дані та завантажуємо у мережу, тим більший ризик витоків інформації на зовні для зловмисників.

Досліджуючи тріаду CIA (КЦЦ-тріада) можна впевнено сказати - конфіденційною інформацією є інформація, доступ до якої обмежено фізичною або юридичною особою та може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Першим експертом, який широко працював над захистом Інтернет, мереж, доменів та розробив конструкцію у вигляді Куба (кубик Рубик) був Джон Мак-Камбер.[1]. За його кубиком інформаційна безпека має три виміри. Перший – це конфіденційність, цілісність, доступність. Другий - це три стани інформації. Третій – це основні дії для захисту. Усі ці три виміри і є майже гарантією кібербезпеки.

Наприклад, якщо взяти цілісність та ії порушення. Це означає видалення даних сторонньою особою, додавання нових бітів (зокрема абсолютно нових даних) третьою стороною, інверсія бітів та ін. Якщо розглядати доступність - це можливість за прийнятний час одержати необхідну інформаційну послугу. Якщо критично важлива комп'ютерна система стане недоступною – користувачі не зможуть отримувати особисті дані, для того, щоб оперувати ними у реальному житті чи при використанні певних додатків, які залежить від інформації користувача: банки, лікарні і т.д. Конфіденційність (приватність) гарантує, що інформація не буде доступна і розкрита тим людям, які є не авторизовані. [2]

Якщо розглядати другий простір, а саме стан інформації – то він базується на проблемах захисту інформації та даних у кіберпросторі. Це дані, які передаються, обробляються та зберігаються. Третій простір – це як кожен з нас, як фахівець може захищати свої дані, використовуючи набуті знання під час навчання та навички під час роботи. І тому дуже важливо для захисту своїх конфіденційних даних включати контроль та аутентифікацію.

Виклад основного матеріалу й обґрунтування отриманих результатів.

Можна виділити п'ять основних груп для отримання доступу до засобів обчислювальної техніки:

вилучення засобів комп'ютерної техніки; перехоплення інформації; несанкціонований доступ; маніпулювання даними та керуючими командами; комплексні методи.[4]

Перехоплення зазвичай здійснюється коли відбувається підключення до телекомунікаційного обладнання мережі, системи або самого комп'ютера. Це може бути: принтер, телефонний провід, який застосовують для передачі інформації. Ці методи допомагають підключати з головною метою, а саме отримати пароль або важливу секретну інформацію за допомогою телекомунікаційних систем. Це відбувається різноманітними шляхами - підключення до кабелю або перехват мікрохвиль.

Електромагнітне перехоплення працює наступним чином - сигнали з дисплея можна як і приймати, так і записувати, а також проводити аналіз на великій відстані (більше 1000 метрів) за допомогою відповідного устаткування, яке знаходиться, для прикладу в будь-якому автотранспорті.

Аудіоперехоплення – спосіб, який на даний час є найбільш небезпечним та розповсюдженим. Захист інформації є дуже складним. Аудіоперехоплення можна реалізувати за допомогою підслуховуючого пристрою - "таблетки", "клопа", "жучка" і т. п. Часто злочинці можуть використовувати спеціальні датчики :акустичні та вібраційні. Основна задача яких має знімати інформацію, не проникаючи до потрібного приміщення.

Відеоперехоплення – спосіб, який отримує необхідну інформацію, використовуючи відеотехніку. В деяких випадках це також може бути: пристрій нічного бачення, підзорна труба, бінокль та багато іншої спеціальної відеоапаратури.

Реальні кіберзлочини та атаки, які відбуваються у світі

Перший приклад, крадіжка даних в історії урядової системи США, яка полягала насамперед в крадіжці інформації, як і фінансової так і медичної даних 19,7 мільйона людей, які проходили перевірки уряду.

Другий приклад, одна із великих компаній, яка мала глобальні проблеми через хакерів це ліцензована медична страхова некомерційна компанія - Premera Blue Cross. Хакери могли забрати до 11 мільйонів записів клієнтів. Ці записи включають номери кредитних карток, номери соціального страхування та медичну інформацію.

Третій приклад, атака TalkTalk. Це була крадіжка інформації - банківські дані, електронні адреси та номери мобільних телефонів. . В результаті цієї атаки у 2015 року були доступні особисті дані більше 157000 клієнтів. Після розслідування цього порушення було виявлено багато помилок в процесах безпеки самої компанії TalkTalk, яка заплатила рекордний штраф у 400000 фунтів стерлінгів.

Наступним прикладом є атака у понеділок 4 жовтня 2021 року, яка відбулася з найвідвідуванішим сайтом Facebook. Facebook та її дочірні компанії стали недосяжними на сім годин для всього світу. Звичайно це призвело до збитків у мільйони доларів. За словами Цукрберга – це були «зміни конфігурації на магістральних маршрутизаторах, які координують мережевий трафік між центрами обробки даних». Хоча в Інтернеті було багато інформації, що під час збою постраждали дані користувачів. Сама компанія та її керівництво все це заперечила.

Можливості функцій безпеки, які використовує Google для захисту персональних даних

Сервіс Google надає кожному користувачу безпечно спілкуватися через Інтернет та зберігати свої дані із захистом конфіденційності. Усі дані в системах Google зашифровані та зберігаються у кількох місцях. Google також використовує рандомізацію даних, щоб ускладнити пошук даних. Усі жорсткі диски регулярно контролюються та перевіряються. Якщо диск вказує на ознаки потенційної несправності, його замінюють до того, як він вийшов з ладу. Усі вилучені диски фізично знищені. Дані, які зберігаються на вашому локальному комп'ютері (ноутбуці, планшеті або смартфоні) також повинні бути захищені. Потрібно використовувати надійні паролі та/або двоетапний логін, очищати історію свого браузера або файли cookie. [4,5]

Двоетапна перевірка - це покращення звичайного входу в обліковий запис Google. Користувачі можуть створити спеціальний ідентифікаційний номер або свій ключ безпеки. Якщо ключа безпеки немає тоді працює код підтвердження.

Рисунок 1 - Шари безпеки інфраструктури Google

Google гарантує, що сервери, які вони встановлюють у своїх центрах обробки даних (ЦОД) є безпечними для користувачів. Сервери періодично перевіряють на зміну даних, порівнюють їх. Контейнери автоматично скануються на наявність шкідливого програмного забезпечення (ПЗ), при наявності ураженого контейнера буде відповідне позначеннння. За цей процес відповідає менеджер тегів Google, який не запустить теги зі зловмисним ПЗ. А власник отримає сповіщення на електронну пошту. Цей тег буду позначено як зловмисний . Це повідомлення дублюється в історії версій.

ЦОД Google розташовані по всьому світу але без доступу третім особам. Географічне розташування таких центрів ретельно обирається, щоб було безпечним від будь-яких катастрофічних наслідків. Відповідальні за це співробітники компанії, які мають доступ до ЦОД та серверів. Контроль стану безпеки здійснюється дуже ретельно. Це відбувається і на місцях, і в контрольних центрах безпеки в цілому світі. [5]

Основна задача компанії– це охорона від зловмисних атак; наявності вірусів та спамів. А головна задача хакерів - пошкодження або проникнення мережних прикладних програм. Типи атак, які часто використовують хакери - міжсайтовий скриптинг, IP-спуфінг, фальсифікація пакетів даних.

Чи вразливі наші дані та де їх можна знайти під час пошуку в системі? Звичайно, пошукові запити та дії зберігаються у обліковому записі. При активності в Інтернеті кожен має швидший пошук та корисні рекомендації. Якщо вимкнути історію активності - то видаляється попередня активність. Нам відомо, що Google вони збирає такі дані:

- IP -адреса та дані cookie
- Місцезнаходження
- Інформація про пристрій
- Веб-сайти, які переглядалися
- Відео, які переглядалися
- Оголошення, які переглядалися

Google постійно відстежує діяльність кожного користувача, збирає про вас багато інформації. Наприклад, за допомогою файлів cookie, які відповідають на їх рекламний код та ідентифікують вас та особистий ваш пристрій. [9]

Як захистити наші дані?

Перший захист – паролі. Надійний пароль - це найкращий вибір та дія. Не можна користуватися досить простими паролями та використовувати один і той же як на декількох пристроях так і на сайтах. При необхідності є онлайн-генератора паролей, які допоможуть створити безпечний та надійний пароль. Ніколи не варто прив'язуватися до особистих даних. На телефоні бажано користуватися додатково і відбитком пальця або Touch ID.

Другий захист – правильний пошук. Найбезпечнішим є використання віртуальної приватної мережі (VPN) у громадських місцях, де безкоштовна точка Wi-Fi. VPN приховує від інших особисту інформацію.

Третій захист – шифрування, адже для того щоб зрозуміти іншим особам необхідно мати ключ. І тому це дуже корисно при захисті інформації як на персональному комп'ютері так і на телефоні, щоб ваші електронні листи та повідомлення не підлягали стороннім очам.

Важливим для кожного є налаштування, які можна змінювати в Google Chrome, адже їх є велика кількість. Бажано вмикати тільки ті функції, які потрібні в даний момент, оскільки зловмисники можуть цим скористатися. У розділі Конфіденційність є захист від фішингу та шкідливих програм. Chrome попереджає про сайт підозрілий у фішингу або зловмисних програм.

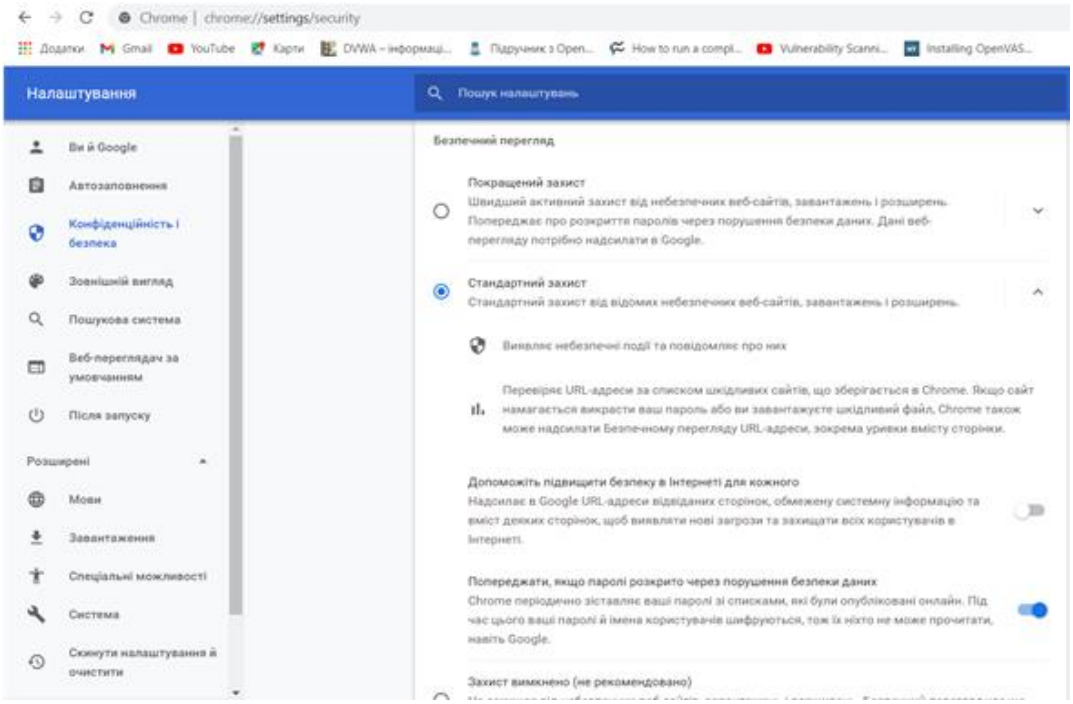

Рисунок 2 — Функція для безпечного використання сайтів

У розділі HTTPS/SSL - Керування сертифікатами встановлені сертифікати. Дані SSL сертифікати використовуються для шифрування інформації під час передачі її по інтернету від точки А в точку Б. Тобто, всі дані – будь-то особиста інформація, банківські координації, геолокація, зображення та інші важливі відомості, які можуть використовувати зловмисники, буде шифруватися і доставлятися до одержувачу в безпеці, без втручання з боку.

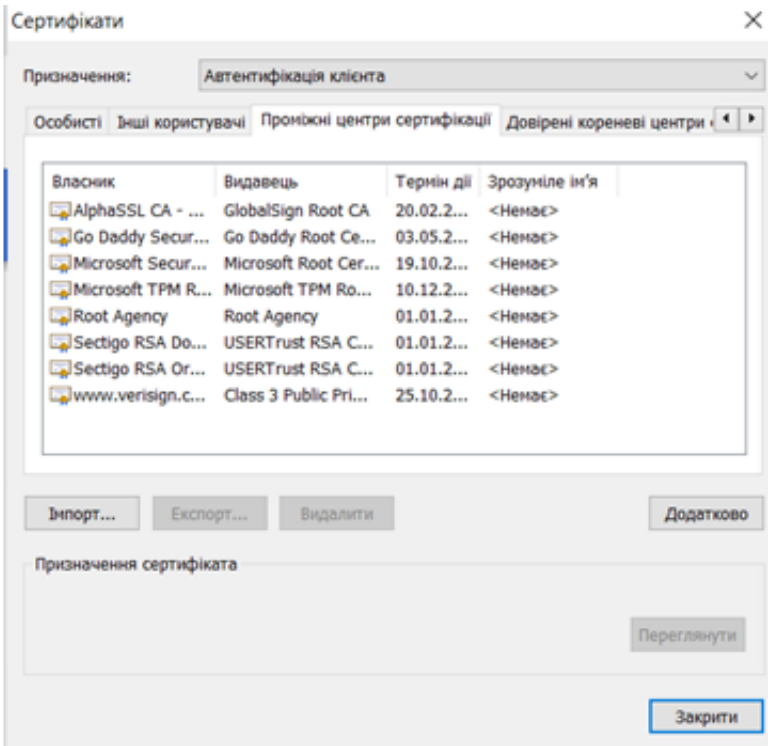

Рисунок 3 — Сертифікати безпеки

Щоб браузер Google Chrome автоматично видаляв файли cookie при закритті усіх вікон необхідно у налаштуваннях встановити - Зберігати локальні дані лише до закриття веб-оглядача. Якщо заблокувати всі файли cookie встановити - Не дозволяти сайтам зберігати дані. Якщо необхідно швидко видалити всі файли cookie - натиснути кнопку Видалити все. Якщо є винятки - натиснути Керувати винятками, вказавши ім'я домену, наприклад улюблений сайт або вказати його IP-адресу,

IPv6-адресу або URL. Параметр - Очищати під час виходу- файли cookie видаляються під час закриття браузера.

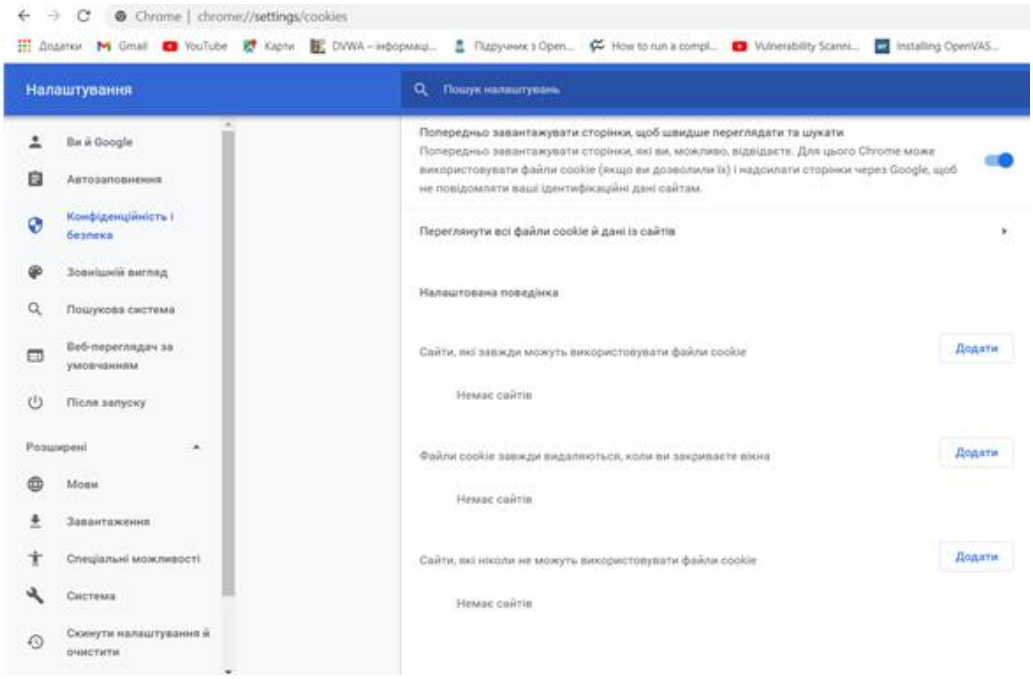

Рисунок 4 — Налаштування файлів cookie для безпечного використання

Висновки та перспективи подальшого дослідження. Провівши аналіз наймасштабніших атак та збоїв соціальних мереж прийшли до висновку – суспільство стало набагато залежніше від соціальних мереж, як приклад є недавній збій 4 жовтня 2021 року у Facebook, основні атаки проводяться вночі, де відбувається крадіжка інформації - банківські дані, електронні адреси та номери мобільних телефонів.

Провели аналіз функцій безпеки, які використовує Google для захисту персональних даних. Досліджувалися функції по забезпеченню безпечного використання сайтів, та SSL сертифікати, які використовуються для шифрування інформації від зловмисників.

Список бібліографічного опису

1. Забезпечення інформаційної безпеки держави. Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с.
2. Основи інформаційної безпеки : навч. пос. / Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. – Вінниця : ВНТУ, 2018. – 316 с.
3. Баглай Р. О. Загрози безпеки хмарних технологій для банків / Р. О. Баглай // Системи обробки інформації. 2018. Вип. 1. С. 127-135. – Режим доступу: http://nbuv.gov.ua/UJRN/soi_2018_1_20
4. Інформаційна безпека. Навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик. Львів : Видавництво Львівської політехніки, 2019. 580 с
5. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. — К.: Видавничий дім «Кондор», 2019. — 272 с.
6. Стратегічна безпека системи "об'єкт – інформаційна технологія" - Монографія. Львів : Видавництво Львівської політехніки, 2020. 260
7. Міскевич О. І., Кокоша М. С. Додаток «Системний монітор» засобами бібліотеки QT. // Науковий журнал "Комп'терно-інтегровані технології: освіта, наука, виробництво" – Луцьк: Видавництво ЛНТУ. – Вип. 26. – 2017. – С. 138-142.
8. S.V. Grynyuk, K.Ya. Bortnik, O.I. Miskevych, D.I. Palivoda An overview of tools for creating games on Android. / Computer-integrated technologies: education, science, production. No. 35, Art. 124-128, 2019.
9. N. A. Khrystynets, A. A. Sakhnyuk, E. A. Sviridyuk, O. I. Miskevich. Use of бем-blocks when creating a site. / Computer-integrated technologies: education, science, production. №35., Art. 206-210, 2019
10. Miskevich O., Bagniuk, N., Khrystynets, N., Marchevska O. Automation of detection of defective products by machine learning methods. Computer-integrated technologies: education, science, production, №39, 175-180. 2020

References

1. Ensuring information security of the state. Textbook / VB Dudykevych, IR Opirsky, PI Garanyuk, VS Zachepylo, AI Partyka. Lviv: Lviv Polytechnic Publishing House, 2017. 204 p.
2. Fundamentals of information security: textbook. pos. / Dudykevych VB, Khoroshko VO, Yaremchuk YE - Vinnytsia: VNTU, 2018. - 316 p.

3. Baglay RO Threats to the security of cloud technologies for banks / RO Baglay // Information processing systems. 2018. Vip. 1. pp. 127-135. - Access mode: http://nbuv.gov.ua/UJRN/soi_2018_1_20
4. Information security. Textbook / Yu. Ya. Bobalo, IV Gorbaty, MD Kiselychnyk, AP Bondarev, SS Voitusik, A. Ya. Gorpenyuk, OA Nemkova, IM Zhuravel , BM Berezyuk, EI Yakovenko, VI Otenko, IY Tyshyk. Lviv: Lviv Polytechnic Publishing House, 2019. 580 p
5. Lisovska Yu.P. Cybersecurity: risks and measures: textbook. manual. - Kyiv: Condor Publishing House, 2019. - 272 p.
6. Strategic security of the system "object - information technology" - Monograph. Lviv: Lviv Polytechnic Publishing House, 2020. 260
7. Miskevich OI, Kokosha MS Application "System Monitor" by means of the QT library. // Scientific journal "Computer-integrated technologies: education, science, production" - Lutsk: LNTU Publishing House. - Vip. 26. - 2017. - P. 138-142.
8. S.V. Grynyuk, K.Ya. Bortnik, O.I. Miskevych, D.I. Palivoda An overview of tools for creating games on Android. / Computer-integrated technologies: education, science, production. No. 35, Art. 124-128, 2019.
9. N. A. Khrystynets, A. A. Sakhnyuk, E. A. Sviridyuk, O. I. Miskevich. Use of бет-blocks when creating a site. / Computer-integrated technologies: education, science, production. №35., Art. 206-210, 2019
10. Miskevich O., Bagniuk, N., Khrystynets, N., Marchevska O. Automation of detection of defective products by machine learning methods. Computer-integrated technologies: education, science, production, №39, 175-180. 2020