Економічні науки

УДК 004.056

Ярема Олег Романович

кандидат економічних наук,

доцент кафедри цифрової економіки та бізнес-аналітики

Львівський національний університет імені Івана Франка

Yarema Oleg

PhD in Economics,

Associate Professor of the Department of Economic Cybernetics

Ivan Franko National University of Lviv

Тимчишин Софія Орестівна

студентка

Львівського національного університету імені Івана Франка

Tymchyshyn Sofiia

Student of the

Ivan Franko National University of Lviv

Книш Олег Григорович

студент

Львівського національного університету імені Івана Франка

Knysh Oleh

Student of the

Ivan Franko National University of Lviv

КІБЕРАТАКИ В СУЧАСНОМУ СВІТІ: НАВІЩО ТА ЯК ЗАХИСТИТИСЯ

CYBER ATTACKS IN THE MODERN WORLD: WHY AND HOW TO PROTECT YOURSELF

Анотація. *Дане дослідження розглядає загрози кібербезпеки, що стали необхідністю у цифровій епохі. У контексті зростаючого числа кіберзлочинів, автор розкриває мотивації за атаками, включаючи економічні вигоди, політичний вплив та порушення конфіденційності.*

У статті ретельно проаналізовано різноманітні методи та техніки, що використовуються зловмисниками, включаючи фішинг, атаки з використанням шкідливого програмного забезпечення та витіснення даних. Зокрема, надається узагальнення найбільш поширених загроз і їх можливих наслідків.

Також особлива увага приділяється заходам безпеки та стратегіям захисту від кібератак. Автори розглядають питання виявлення інцидентів, впровадження систем двофакторної аутентифікації, шифрування даних та регулярне оновлення програмного забезпечення. Звертається увага на важливість кібергігієни та освіти для користувачів як ефективного заходу проти атак.

Стаття завершується рекомендаціями щодо комплексного підходу до кібербезпеки, підкреслюючи важливість постійного моніторингу та адаптації заходів безпеки до постійно загроз, які постійно змінюються. Загальною метою є підвищення свідомості про кібербезпеку та надання конкретних порад для ефективного захисту від кібератак у сучасному світі.

Ключові слова: *кібербезпека, кібератака, кіберзагроза, кіберзлочинність, хакерство.*

Summary. *This study examines the cyber security threats that have become a necessity in the digital age. In the context of the growing number of cybercrimes, the author reveals the motivations behind the attacks, including economic gain, political influence and privacy violations.*

The article thoroughly analyzes the various methods and techniques used by attackers, including phishing, malware attacks, and data exfiltration. In particular, a summary of the most common threats and their possible consequences is provided.

Special attention is also paid to security measures and strategies to protect against cyber attacks. The authors consider the issues of incident detection, implementation of two-factor authentication systems, data encryption and regular software updates. Attention is drawn to the importance of cyber hygiene and user education as an effective measure against attacks.

The article concludes with recommendations for an integrated approach to cyber security, emphasizing the importance of constant monitoring and adaptation of security measures to constantly changing threats. The overall goal is to raise awareness of cyber security and provide concrete advice to effectively defend against cyber attacks in today's world.

Keywords: *cyber security, cyber attack, cyber threat, cyber crime, hacking.*

Постановка проблеми. В сучасному інформаційному суспільстві кібератаки стали однією з головних загроз безпеці як на національному, так і на особистому рівнях. Актуальність дослідження способів захисту та боротьби з комп'ютерними правопорушеннями в Україні – безсумнівна, адже на даний момент Росія веде повномасштабну інформаційну та кібер-війну з Україною, тож можливість захиститися від ворожих атак є справді начасною. До того ж, і в мирний час комп'ютерні правопорушення – не рідкість, тож необхідно вивчати й розробляти способи боротьби з ними. Ця стаття спрямована на розгляд причин та механізмів кібератак, а також надання рекомендацій для захисту в цьому цифровому ландшафті.

Аналіз останніх досліджень і публікацій. У зв'язку з актуальністю теми кібербезпеки в даний час багато науковців приділили свою увагу дослідженню різноманітних видів кіберзагроз та способів протидії їм.

Дослідження О. Трофименко показало, що проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора і громадянського суспільства [6].

Ю. Міхєєв поглиблює розуміння стану захищеності кіберпростору держави, вказуючи на взаємозв'язок з інформаційно-аналітичним забезпеченням Збройних сил України. Він підкреслює, що для ефективного забезпечення кібербезпеки необхідно удосконалити систему інформаційно-аналітичного забезпечення. Автор визначає основні напрямки удосконалення, які включають в себе використання сучасного програмного забезпечення на основі сучасних технологій та розробку системи інформаційно-аналітичного забезпечення з оцінкою її спроможності [4].

І. Пулеко в своєму дослідженні фокусується на захисті систем Інтернету Речей (IoT). Він визначає відсутність єдиної і повністю надійної системи захисту для IoT систем з бездротовими мережами. Автор рекомендує дотримуватися простих правил для зменшення ризиків, зазначаючи важливість використання фільтрації за MAC-адресою, хования SSID, обмеження доступу та оновлення мікропрограм [5].

І. Діордіца підкреслює, що система забезпечення кібербезпеки є єдиним державно-правовим механізмом. Він визначає основні суб'єкти системи – державні органи, органи місцевого самоврядування та підприємства, які забезпечують кіберзахист. Діордіца стверджує, що система забезпечення кібербезпеки має сприяти збалансованому існуванню інтересів особи, суспільства і держави, здійснюючи виявлення, запобігання та припинення загроз [2].

Загалом, проведений аналіз досліджень підкреслює необхідність комплексного та системного підходу до забезпечення кібербезпеки, залучення різних суб'єктів та використання сучасних технологій у цьому

процесі. Однак в своїх дослідженнях науковці зосереджуються здебільшого на кібербезпеці національного рівня, не акцентуючи увагу на способах захисту від кібератак конкретних індивідуумів.

Формулювання цілей статті. Мета даної статті — проаналізувати сучасні кіберзагрози та запропонувати конкретні заходи для захисту пересічних користувачів нових технологій від потенційних кібератак.

Виклад основного матеріалу. У наші дні використання інформаційних технологій не має меж. Віртуальний простір переймає від реального все, у тому числі й злочинність у її нових формах і проявах. Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектору. Таким чином, зіштовхнутися з комп'ютерними правопорушеннями може кожен користувач мережі. До того ж, під час війни кількість кібератак тільки зростає і носить все більш руйнівний характер.

Кіберзлочинність визначається як злочинні дії або активності, які здійснюються в інтернеті або через комп'ютерні системи та мережі. Це включає в себе різні види діяльності, що мають кіберпризначення і можуть завдати шкоди системам, даним, інфраструктурі та іншим цифровим активам. Щодо тих видів кіберзлочинів, що спрямовані переважно на пересічних громадян і з якими може зіткнутися кожен, то до них відносять:

Кардинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «трояни», «боти»).

Фішинг – вид шахрайства, відповідно до якого клієнтам платіжних систем надсилають повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі. Цей тип шахрайства різко зріс за останні кілька років, оскільки це легко зробити, але важко відстежити злочинця.

Вішинг – вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки.

Онлайн-шахрайство – несправжні інтернет-аукціони, інтернетмагазини, сайти та телекомунікаційні засоби зв'язку.

Піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті.

Кард-шарінг – надання незаконного доступу до перегляду супутникового та кабельного TV.

Соціальна інженерія – мистецтво маніпулювання людьми, щоб вони відмовилися від конфіденційної інформації або доступу до облікових даних. Соціальна інженерія здійснюється шляхом видавання себе за колегу, здійснення телефонних дзвінків, надсилання електронних листів і використання служб обміну миттєвими повідомленнями, щоб завоювати довіру жертви.

Мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення. Зловмисне програмне забезпечення – це програми або програмне забезпечення, призначені для порушення роботи комп'ютера, збору конфіденційної інформації з комп'ютерних систем або отримання дистанційного керування комп'ютером. Зловмисне програмне забезпечення часто залишається непоміченим, його важко видалити та може завдати значної шкоди комп'ютерним системам, заражаючи файли, змінюючи дані та руйнуючи системні утиліти. Важливо також зазначити, що зловмисне програмне забезпечення може маскуватися під законне програмне забезпечення, щоб користувачам було легше встановити його на свої комп'ютери. Прикладами є віруси, хробаки, трояни, шпигунське та рекламне ПЗ.

Злом Інтернету речей – є однією з найпоширеніших форм кіберзлочинності та може призвести до фізичної шкоди. Цей злом

відбувається, коли хакер використовує пристрій, підключений до Інтернету, наприклад розумний термостат або холодильник. Вони зламують пристрій і заражають його шкідливим програмним забезпеченням, яке поширюється по всій мережі. Потім хакери використовують цю інфіковану систему для атаки на інші системи в мережі.

Протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.

Прослуховування – це таємне прослуховування або запис розмов без відома та/або згоди всіх сторін. Це може відбуватися по телефону, за допомогою прихованої камери або навіть через віддалений доступ. Прослуховування є незаконним і може поставити вас під загрозу шахрайства та крадіжки особистих даних.

Рефайлінг – незаконна підміна телефонного трафіку.

Спуфінг – це кіберзлочин, коли хтось приховує свою особу в Інтернеті, щоб обдурити або ошукати іншого. Ці злочини можуть включати підробку електронної пошти, підробку телефону, підроблені профілі в соціальних мережах і підроблені оголошення. Одним із прикладів є те, що особа надсилає електронний лист, який, здається, надійшов від колеги по роботі, із запитом на конфіденційну інформацію від імені генерального директора компанії.

Криптоджекінг — це кіберзлочин, у якому хакери незаконно використовують комп'ютери та мережі людей для видобутку криптовалюти. Характеризується надмірним навантаження на ЦП.

Black Hat SEO — це різновид спаму, коли маркетологи використовують неетичні методи для підвищення рейтингу в результатах пошукової системи. Тактика Black Hat може включати перенасичення ключовими словами, невидимий текст і маскування, що змушує алгоритм пошукової системи вважати сторінку релевантною, хоча це не так [1].

Переважна більшість наведених вище кіберзлочинів спрямована на викрадення персональних даних і подальше їх незаконне використання з метою отримання вигоди (переважно фінансової). З кожним роком все більше персональної інформації ми розміщуємо в інтернеті (при реєстрації на численних сайтах, проходячи онлайн-опитування чи просто публікуємо у вільному доступі в соціальних мережах), відповідно, зростає загроза що ці дані зловмисник захоче роздобути й скористатися ними в злочинних цілях. Для того щоб цього уникнути необхідно дотримуватися кількох правил:

1. Створювати сильні паролі. Для цього можна скористатися спеціальними сайтами, або ж скласти складний пароль самотужки. Такий пароль повинен містити малі та великі літери, числа та спеціальні символи, розміщені в випадковому порядку, найкращий варіант коли вони не складаються в слова та дати. До того ж, пароль варто час від часу змінювати. Для кожного облікового запису пароль повинен бути іншим.

2. Використовувати двофакторну аутентифікацію (2FA). Використання двох «факторів» (звичайний пароль та код підтвердження, отриманий від окремої програми) допомагає надійно захистити обліковий запис, слугуючи додатковим рівнем безпеки.

3. Використовувати антивірусне програмне забезпечення та мережевий брандмауер. Завдяки цьому можна вберегтись від мальваре (вірусів та шкідливого ПЗ).

4. Регулярно оновлювати програмне забезпечення. Кожна нова версія ПЗ зазвичай краща за попередню, тож регулярне оновлення операційної системи та програмного забезпечення допоможе закрити можливі вразливості.

5. Проводити регулярне резервне копіювання даних. Резервні копії не вбережуть персональну інформацію, але дадуть можливість відновити її після можливої атаки.

6. Користуватися захищеними мережами. Virtual Private Network (VPN) забезпечує захист інформації що циркулює в ній, тож персональна інформація буде у безпеці.

7. Підвищувати свою освіченість у сфері кібербезпеки. Для того щоб захиститися від кіберзагрози потрібно знати про її існування – безліч людей навіть не знають про існування фішингу, мальваре, кард-шарінгу, рефайлінгу тощо. Обізнаність про розповсюджені прийоми значно підвищує шанси не попастися на вудку зловмисника. До того ж, злочинці намагаються покращувати свої навички, винаходять нові віруси, шкідливі програми та способи викрасти дані та гроші; відповідно необхідно підвищувати свою обізнаність, щоб могти розпізнати атаку та протидіяти їй.

8. Перевіряти свої облікові записи. Завдяки цьому можна вчасно помітити крадіжку облікового запису (зазвичай підбирають пароль до облікового запису, а тоді змінюють його) і звернутися до правоохоронних органів.

9. Намагатися не розповсюджувати свої персональні дані. За будь-якої можливості використовуйте псевдонім, а не справжнє ім'я. До того ж варто створити додаткову електронну пошту, не прив'язану до ваших основних облікових записів, і використовувати її разом з псевдонім там, де це можливо. Ніколи не публікуйте у відкритих джерелах разом із раніше поширеними частинами персональних даних (як правило, це ПІБ) адреси проживання, номери телефонів, номери або копії документів, реєстраційні номери автотранспорту (фото з авто, на якому видно номер) чи інші конкретні дані, через які вас можна однозначно ідентифікувати в реальному житті.

Завдяки всім правилам, що перечислені вище, можна вберегти свою персональну інформацію від «побутового» кібершахрайства – кіберзлочинів, що відбуваються регулярно та спрямовані на крадіжку даних з метою збагачення. Однак, в часі війни, терористи атакують Україну не

лише для викрадення грошей, а ще й для того щоб принести шкоду: перевантажити трафік, припинити роботу міської IT інфраструктури, завдати технічної шкоди, розповсюдити дезінформацію, а також задля шпигунства. Військовим кібератакам здебільшого піддаються великі, національно важливі сайти, мережі зв'язку, військові комп'ютерні системи, однак певні атаки можуть бути спрямовані й на пересічних українців.

Масштабні атаки на держоргани України зазвичай розпочинаються з розсилання інфікованих файлів електронною поштою або в месенджерах звичайним працівникам потрібної державної організації. Після того як комп'ютери будуть інфіковані зловмисники можуть викрасти потрібні їм файли. Для того щоб не допустити таких атак потрібно користуватися засобами шифрування електронної пошти, антивірусним програмним забезпеченням, налаштувати папку Спам на всі листи від невідомих отримувачів і обережно відкривати такі листи.

Російські хакери використовують й інші види кібератак для нанесення ударів по IT-інфраструктурі України, зокрема:

Хакерство — це акт отримання несанкціонованого доступу до комп'ютерної системи з метою зараження комп'ютерів своїх жертв або обходу заходів безпеки. Хакери створюють програми, призначені для проникнення в комп'ютери інших людей, крадіжки інформації та продажу її в темній мережі.

Програми-вимагачі – це форма зловмисного програмного забезпечення, яке атакує комп'ютерні системи, блокує дані та вимагає плату за розблокування даних. Після зараження комп'ютера програмою-вимагачем користувачеві зазвичай пропонується заплатити викуп за отримання ключа розшифровки, необхідного для відкриття комп'ютера та відновлення контролю над даними. Середня вартість атаки програм-вимагачів становить понад 4 мільйони доларів США, тоді як руйнівна атака в середньому становить понад 5 мільйонів доларів.

Міжсайтовий сценарій (XSS) — це вразливість веб-безпеки, яка виникає, коли зловмисник впроваджує шкідливі сценарії в надійний веб-сайт або веб-програму. XSS може дозволити зловмисникам отримати контроль над сеансом користувача, викрасти його облікові дані та отримати цінні дані. Наприклад, зловмисники можуть розмістити шкідливий код на скомпрометованому сайті, який чекає, поки нічого не підозрюючий користувач увійде в систему, перш ніж виконувати команди, які можуть розкрити інформацію з комп'ютера жертви [3].

Розподілена відмова в обслуговуванні (DDoS) атакує службу або систему, яка заповнює ціль більшою кількістю запитів, ніж вона може обробити. Ця атака націлена на веб-сайт організації та намагається знищити його, надсилаючи численні запити одночасно. Потік запитів змушує сервери вимикатися, порушуючи доступність інформації для користувачів, які намагаються отримати до неї доступ.

Розширені стійкі загрози (APT) – це тип кібератак, які є чітко цілеспрямованими, стійкими, складними та забезпеченими ресурсами. Кібератаки APT можуть тривати місяцями або роками. Вони проникають у мережі, витягують дані, а потім викрадають їх непомітно. Типовими цілями є державні установи, університети, виробничі фірми, високотехнологічні галузі та оборонні підрядники.

Для захисту від таких атак важливо дотримуватися всіх правил захисту персональних даних, зазначених вище, а також можна вжити додаткових заходів (серйозніших), таких як:

1. Інтеграція технологій штучного інтелекту та машинного навчання. Штучний інтелект можна використати для виявлення та блокування аномальних патернів поведінки системи чи користувача, які можуть свідчити про кіберзагрозу. ШІ також може аналізувати великі обсяги даних для визначення можливих майбутніх кібератак на основі попередніх патернів. Завдяки тому, що штучний інтелект не потребуватиме залучення

людини для спрацювання алгоритмів, відповідь на атаку буде миттєвою. Також ШІ може аналізувати програмний код для виявлення шкідливих програм та коду, навіть якщо вони раніше не були відомі. Ще штучний інтелект можна використовувати для активного пошуку слабких місць в системах безпеки та виявлення потенційних точок атак. А також задіяти в розробці систем, які можуть виявляти можливі кіберзагрози до їх виникнення та уразливості. Завдяки здатності штучного інтелекту до самонавчання з його використанням можна організувати складну адаптивну систему ефективного захисту від кібератак.

2. Використання блокчейн-технологій. Завдяки блокчейну можна надійно захистити дані, адже без ключа доступ до даних, що зберігаються в блоці, отримати неможливо. Блокчейн працює на принципі розподіленого реєстру, що означає, що кожен вузол в мережі має однаковий запис. Це ускладнює атаки, оскільки зловмисники повинні взяти під контроль більшість вузлів, щоб внести зміни в існуючий блокчейн. Блокчейн може використовуватися для створення децентралізованих систем авторизації та ідентифікації, де кожен користувач має унікальний ключ, який не зберігається централізовано. Це зробило б атаки на централізовані системи менш ефективними. Розподілений характер блокчейн-технологій полегшує моніторинг та аудит дій у мережі. Кожна транзакція, яка додається до блокчейну, стає частиною незмінного журналу, що полегшує виявлення аномальних активностей. До того ж, використання блокчейн-технологій може ускладнити DDoS-атаки, оскільки мережа розподілена та менше уразлива до централізованих атак.

3. Використання хмарних технологій. Хмарні сервіси надають можливості для шифрування даних під час їх передачі та зберігання, забезпечуючи конфіденційність інформації. Також хмарні платформи дозволяють автоматизоване резервне копіювання даних та швидке відновлення в разі кібератак чи втрати даних. До того ж хмарні платформи

можуть легко інтегруватися з іншими засобами безпеки, такими як антивірусне програмне забезпечення, моніторинг загроз тощо.

4. Шифрування даних. Однією з основних функцій шифрування є забезпечення конфіденційності даних. Завдяки шифруванню можна зберігати та передавати інформацію так, що тільки особи з відповідними ключами зможуть отримати до неї доступ. У випадку, коли комунікація між системами чи користувачами здійснюється через відкриті мережі, шифрування перешкоджатиме перехопленню чи радше читанню перехопленої інформації. Використання шифрування в електронній пошті (наприклад, засоби PGP або S/MIME) забезпечить конфіденційність та цілісність листування. До того ж, шифрування даних може знизити ризик втрати даних в результаті атаки програми-вимагача, оскільки навіть якщо дані стануть недоступними, вони залишаться зашифрованими.

Впровадження цих заходів безпеки в поєднанні з правилами збереження персональних даних допоможуть вберегтися від кібератак, однак важливим є використовувати комплексний підхід – обирати різні методи захисту, комбінувати їх, вдосконалювати та адаптувати відповідно до потреб [2].

Висновки та перспективи подальших досліджень. Кіберзлочинність в Україні стрімко розвивається, цьому сприяє як розвиток і поширення інформаційних технологій так і військова агресія Росії, тож, щоб уникнути кібератак в свою сторону, необхідно поглиблювати свої знання в сфері кібербезпеки (які види кібератак існують, як їх ідентифікувати та як їм протистояти), дотримуватися правил захисту персональних даних (як от використання сильних паролів, двофакторної аутентифікації, антивірусного ПЗ та захищених мереж, регулярне оновлення ПЗ та резервне копіювання даних), а також за можливості та потреби включити в свою систему безпеки блокчейн та хмарні технології,

шифрування даних та штучний інтелект. Ці заходи допоможуть уникнути кібератак, або ж зберегти свої дані, якщо атака все ж відбудеться.

Література

1. Гудмен М. Злочини майбутнього. Харків: Фабула. 2019. 592 с.
2. Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. Підприємництво, господарство і право. 2017. № 7. С. 109-116. URL: http://pgp-journal.kiev.ua/archive/2017/7/24.pdf (дата звернення: 03.12.2023).
3. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність. Концепції, Стратегії, технології. Київ: Сідком, 2022. 284 с.
4. Міхєєв Ю. І., Павленко М.М., Савчук В. С. Інформаційно-аналітичне забезпечення підрозділів Збройних сил України в національному сегменті кіберпростору. *Комп'ютерні технології: інновації, проблеми, рішення: тези доповідей III Всеукраїнської науково-технічної конференції* (м. Житомир, 26-27 листопада 2020 р.). Житомир: Житомирська політехніка, 2020. С. 31-32. URL: https://conf.ztu.edu.ua/wp-content/uploads/2021/01/tezy-dopovidej-kt2020_os-2.pdf (дата звернення: 03.12.2023).
5. Пулеко І. В., Росінський Ю. М. Рекомендації щодо забезпечення безпеки бездротових з'єднань Інтернету речей. *Комп'ютерні технології: інновації, проблеми, рішення: тези доповідей III Всеукраїнської науково-технічної конференції* (м. Житомир, 26-27 листопада 2020 р.). Житомир: Житомирська політехніка, 2020. С. 39-40. URL: https://conf.ztu.edu.ua/wp-content/uploads/2021/01/tezy-dopovidej-kt2020_os-2.pdf (дата звернення: 03.12.2023).
6. Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. Захист інформації. 2019. Том 21, № 3. С. 150-157. URL:

http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?Sequence=1&isallowed=y (дата звернення: 03.12.2023).