УДК 004.056.5

ВПЛИВ РІЗНИХ ФОРМ КІБЕРЗАГРОЗ НА СТІЙКІСТЬ ІНФОРМАЦІЙНИХ СИСТЕМ: АНАЛІЗ ТА СТРАТЕГІЇ ЗАХИСТУ

Євгеній Осадчий[1], Марина Єсіна[1,2], Віктор Онопрієнко[2]

[1] Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
xa12850357@student.karazin.ua, m.v.yesina@karazin.ua
[2] АТ «Інститут Інформаційних технологій», вул. Коломенська 15, Харків, 61166, Україна
v25258@gmail.com

Надійшла: Листопад 2023. Прийнята: Грудень 2023.

***Анотація**: Дана робота присвячена дослідженню проблематики кібербезпеки в контексті сталого розвитку сучасного інформаційного суспільства. Починаючи з огляду різноманітних форм кіберзагроз, у статті запропоновано аналіз їхнього впливу на конфіденційність, цілісність та доступність інформації. Критична залежність сучасного суспільства від інформаційних технологій, робить тематику захисту від кіберзагроз надзвичайно актуальною. В межах роботи запропоновано аналіз зростання кількості та складності кіберзагроз, що вимагає постійного удосконалення та оновлення стратегій захисту від них. Важливим етапом висвітлення теми є аналіз впливу різних форм кіберзагроз на сучасні інформаційні системи. Розглянуто основні різновиди фішингу та соціальної інженерії, а також наслідки впливу вірусів, троянських програм та інших шкідливих програм. Детальний огляд цих аспектів дозволяє визначити ключові питання та небезпеки, які виникають в контексті проблематики кіберзагроз. Також, стаття містить матеріали, присвячені різним стратегіям захисту. Вона розглядає існуючи стратегії для захисту інформаційних систем, включаючи виявлення вразливостей, використання багатофакторної автентифікації та заходи для забезпечення стійкості. Загальні висновки даної роботи підсумовують необхідність постійного оновлення та адаптації стратегій захисту, щодо зростаючої складності кіберзагроз у світі швидкого технологічного розвитку. В цілому, дана робота є ще одним кроком у розумінні сутності викликів, які пов'язані із проблематикою забезпечення кібербезпеки в сучасному інформаційному суспільстві.*

***Ключові слова:** кіберзагроза, аналіз та захист, стійкість інформаційних систем, стратегії захисту.*

1. Вступ

У сучасному інформаційному суспільстві питання кібербезпеки стають надзвичайно актуальними, оскільки з кожним днем зростає обсяг цифрової активності та залежність від інформаційних технологій. Разом із швидким розвитком технологій зростає і рівень кіберзагроз, які стають важливим аспектом забезпечення безпеки в Інтернет просторі. Ці загрози викликають серйозні проблеми, а також стають причиною порушення конфіденційності, цілісності та доступності інформації. У межах цієї роботи в стислому вигляді розглянуті різноманітні форми кіберзагроз та їхній вплив на сучасні інформаційні системи (ІС), а також можливі заходи для захисту від них в умовах постійно зростаючого цифрового середовища.

Актуальність теми зумовлена впливом відразу кількох ключових аспектів. По-перше, інформаційні технології стали не тільки необхідною частиною повсякденного життя, але і критично важливим ресурсом для функціонування великої кількості суспільних, комерційних та господарських процесів. По-друге, зростання залежності від цих технологій відкриває нові можливості для кіберзлочинців, які використовують різноманітні та вдосконалені методи для атак на ІС. Забезпечення надійності і безпеки ІС стає надзвичайно важливим завданням, оскільки кіберзагрози, такі як атаки на мережеві структури, витоки конфіденційної інформації та шкідливі програми, можуть мати серйозні наслідки для економіки, політики та суспільної безпеки. У цьому контексті розуміння різних форм кіберзагроз та їхнього впливу стає стратегічно важливим для розробки ефективних заходів захисту, що відповідають викликам сучасного інформаційного простору.

Зростання кількості та складності кіберзагроз стає серйозним викликом для сфери кібербезпеки. Різноманітність атак, включаючи витончені техніки фішингу, атаки з використанням шкідливого програмного забезпечення (ПЗ) та атаки на інфраструктуру, свідчать, що кі-

 © Осадчий Є., Єсіна М., Онопрієнко В., 2023

берзлочинці постійно вдосконалюють свої методи, адаптуючись до новітніх технологій та змін у сфері кібербезпеки [1]. Неперервний розвиток кіберзагроз вимагає не лише реактивних, але й проактивних стратегій захисту. Організації та індивіди, що прагнуть залишатися попереду, повинні не лише оновлювати свої системи та ПЗ, але й розвивати нові методи виявлення та запобігання кібератак. Важливість цього завдання зумовлена тим, що відповідальність за захист ІС стає не тільки завданням технічних спеціалістів, але й ключовою складовою стратегічного управління будь-якою організацією чи державною установою. У цьому контексті огляд різних форм кіберзагроз та їхнього впливу стає невід'ємною частиною ефективного й безпечного управління, спрямованого на забезпечення стабільності та надійності функціонування сучасних ІС.

Проведення аналізу впливу кіберзагроз на стійкість ІС є невід'ємною частиною вдосконалення стратегій кібербезпеки в умовах постійного еволюційного середовища [2]. З урахуванням стрімкого розвитку технологій та збільшення кількості цифрових аспектів нашого життя, зростає і сфера кіберзагроз, що накладає серйозний вплив на ІС.

Ця стаття має на меті розглянути проблематику кібербезпеки в контексті сучасних реалій й пропонує оглядовий аналіз різноманітних різновидів кіберзагроз, який охоплює їх вплив на конфіденційність, цілісність та доступність інформації. Зокрема, надаючи огляд найновіших тенденцій у сфері кібербезпеки, автори роботи мають на меті виокремити ключові аспекти безпеки, що піддаються ризику внаслідок сучасних кібератак.

Важливим етапом у запропонованому аналізі є визначення різних стратегій захисту, які спроможні ефективно відповідати викликам безпеки сучасного кіберпростору. Слід під креслити, що розглянуті стратегії враховують, як технічні, так і стратегічні аспекти, котрі спрямовані на удосконалення стійкості сучасних ІС та забезпечення їхньої функціональності в умовах постійного впливу широкого спектру загрози інформаційної безпеки (ІБ).

2. Різновиди кіберзагроз та їх вплив на ІС

2.1 Фішинг та соціальна інженерія

Фішинг та соціальна інженерія стали неодмінною частиною сучасного цифрового простору, ставши важливими елементами кібербезпеки. Ці методи атак, спрямовані на отримання конфіденційної інформації через маніпулювання психологією користувачів, стали більш витонченими та поширеними, викликаючи серйозні загрози для особистої та корпоративної безпеки. Цей розділ розглядає методи фішингу та соціальної інженерії, їх вплив на користувачів та пропонує практичні підходи до захисту від цих загроз [1].

2.1.1 Фішинг: відомі методи та їх варіації

Фішинг – це один із найбільш поширених методів атак в сфері кібербезпеки, який використовує соціальні інженерні техніки для отримання конфіденційної інформації, такої як паролі, номери банківських карт або особисті дані, від користувачів. Нижче наведено узагальнений перелік найбільш поширених методів і варіацій фішингу, наслідків їх впливу на користувачів та можливих стратегій захисту.

Основні методи фішингу:

- *Електронна пошта (E-mail): підступні листи, що виглядають як від відомих вам компаній чи сервісів, які закликають вас ввести конфіденційні дані на фіктивних веб-сайтах.*
- *Соціальні мережі та месенджери: фішингові атаки через популярні соціальні мережі та месенджери, де атакуючі видають себе за знайомих чи колег.*
- *Веб-сайти: створення фішингових веб-сайтів, які імітують офіційні ресурси для отримання особистої інформації.*

Варіації фішингу:

- *Розмовний фішинг – вішинг (Vishing): фішинг через телефонні дзвінки, де атакуючий намагається отримати конфіденційну інформацію від потенційної жертви.*
- *Смішинг (Smishing): атаки через SMS-повідомлення, де у користувачів намагаються виманити особисті дані через текстові повідомлення.*
- *Spear Phishing або таргетований фішинг: атаки, де зловмисники висококваліфіковано атакують конкретні цілі - фізичні особи та/чи організації.*
- *Соціальна інженерія: використовує психологічні аспекти впливу на свідомість персоналу сучасних ІС. Як метод атаки, не лише спрямований на експлуатацію технічних й організаційних вразливостей діючої системи захисту, але й ефективно використовує психологічні прийоми для масштабування наслідків атаки. Розгляд впливу соціальної інженерії на психологічний стан користувачів ІС та їх вразливість, є ключовим аспектом безпеки в онлайн середовищі. Зловмисники використовують такі методи, як створення терміновості, виклик емоцій, та швидкі перевтілення в авторитетність, щоб викликати потрібну реакцію у потенційної жертви.*

2.1.2 Ефективні стратегії захисту від загроз фішингу.

- *Навчання та професійна відповідальність:* завчасне передбачення фішингових атак розуміє під собою безперервне навчання користувачів сучасних ІС, розпізнавати характерні ознаки шахрайства. Тому, регулярні тренінги та інструкції персоналу, можуть значно підвищити рівень їх профільних компетенцій.
- *Використання антивірусних програм:* встановлення та регулярне оновлення антивірусних програм є ефективним заходом захисту від фішингу. Вони виявляють та блокують шкідливі віруси та веб-сайти.
- *Багатофакторна автентифікація:* використання багатофакторної автентифікації додає додатковий шар захисту, оскільки для входу необхідні два чи більше види автентифікації. Багатофакторна автентифікація дедалі стає необхідністю в умовах постійного зростання фішингових атак. Аналіз відомих інцидентів безпеки показує, що використання не лише паролів, але й інших методів ідентифікації, таких як біометричні дані чи одноразові коди, робить процес автентифікації значно більш надійним. Це зменшує ймовірність «успіху» атак та робить доступ до особистих облікових записів складнішим для зловмисників.
- *Управління паролями:* широке застосування бездротових мереж підвищує ризик несанкціонованого доступу до особистої (приватної) та/чи корпоративної інформації. В цьому сенсі одним із найважливіших заходів безпеки є коректне адміністрування паролями. Користувачі мають створювати складні та унікальні паролі для кожного облікового запису і регулярно їх змінювати.
- *Впровадження механізмів багатофакторної автентифікації:* додатково зміцнює захист доступу до особистих/корпоративних даних [3].
- *Оновлення ПЗ та операційних систем:* є ключовим аспектом безпеки. Своєчасне встановлення оновлень та патчів безпеки дозволяє виправляти виявлені уразливості та запобігати можливим атакам зловмисників.
- *Використання шифрування* даних на пристроях та під час обміну інформацією через бездротові мережі є також невід'ємною частиною захисту чутливих даних від фішингу. Шифрування забезпечує конфіденційність та цілісність інформації під час передачі її через мережі, в т.ч. незахищені.
- *Обмеження доступу до інформації.* є додатковим кроком з протидії фішингу, тому користувачі ІС повинні ретельно контролювати, кому та за яких умов нада-

ють (делегують) доступ до своїх особистих даних та/чи службових повноважень при роботі з ПЗ та/чи мережевим устаткуванням корпоративної ІС.

Інтеграція зазначених стратегій сприятиме підвищенню поточного рівню захисту інформаційних ресурсів від загроз фішингових атак та покращити безпеку особистих та/чи конфіденційних корпоративних даних при їх зберіганні й циркуляції між користувачів в онлайн середовищі.

2.2 Віруси та шкідливе ПЗ

Шкідливе ПЗ є важливою складовою у загальному спектрі загроз ІБ. В загальному випадку її основною метою є завдання шкоди інформаційним і апаратним ресурсам сучасних ІС. Нижче наведено перелік найбільш характерних (часто використовуваних) різновидів шкідливих програм та їх способи їх поширення:

- *Комп'ютерні черв'яки (або трояни): самостійні програми, які розповсюджуються через носії даних та/чи мережеву взаємодію без необхідності подальшого мануального втручання (супроводження) з боку їх розробника.*
- *Рекламні віруси: програми, що намагаються розповсюджувати рекламу або навіть змінюють (підмінюють) сторінки веб-сайтів.*
- *Шпигунське ПЗ: програми, які збирають конфіденційну, в тому числі, технологічну інформацію, без відома її користувачів.*

Вплив на інформаційні системи: наслідки використання шкідливого ПЗ для інформаційних систем можуть передбачати втрату конфіденційності, порушення цілісності даних та обмеження доступу до важливих ресурсів.

Протидія шкідливим програмам: використання антивірусного ПЗ, засобів міжмережевого екранування, систем виявлення вторгнень тощо. Також треба акцентувати увагу на важливості своєчасного оновлення ПЗ та вдосконалення кіберграмотності користувачів ІС.

2.3 Відмова в обслуговуванні та DDoS атаки

2.3.1 DDoS атаки

DDoS (*Distributed Denial of Service - розподілені атаки з відмовою в обслуговуванні*) є серйозною загрозою для сучасних ІС, що здатна призводити до великих збоїв у роботі веб-серверів та мережевої інфраструктури. Цей розділ присвячений аналізу різних типів DDoS атак, їх впливу та ефективним заходам для запобігання відмові в обслуговуванні. На сьогоднішній день ці атаки досі залишаються однією з найбільш поширених та руйнівних форм реалізації деструктивного впливу на функціонування сучасних ІС. Вони спрямовані на перевантаження ресурсів цільового сервера, мережі чи програми (програмного додатку), шляхом навмисного відправлення надмірного злочинного трафіку. Розгляд цієї теми є надзвичайно важливий, оскільки *DDoS* атаки можуть призвести до відмови в обслуговуванні та серйозно зашкодити бізнес та чи промисловим/технологічним процесам. За останні роки збільшилась частота та підвищилась складність реалізації *DDoS*.

Так, наприклад, зловмисники додатково використовують атаки підсилення (як своєрідний різновид забезпечення, або каталізатор цих атак) та синтез ботнетів, для максимізації впливу й наслідків основної атаки. Зокрема, атаки підсилення, такі як *DNS Amplification* та *NTP Amplification*, дозволяють помітно збільшити обсяг надлишкового (постановочного) трафіку і тим самим відчутно перевантажити мережеві з’єднання цільового об’єкту-жертви.

- *Відмова в обслуговуванні та її вплив на систему*

DDoS атаки можуть призвести до відмови в обслуговуванні, зробивши ресурси недоступними для легітимних користувачів. Це може викликати серйозні фінансові втрати, погіршення репутації компанії та втрату клієнтів.

- *Захист від DDoS атак*

Захист від *DDoS* атак вимагає комплексного підходу. В цьому сенсі важливо мати системи моніторингу трафіку, які виявлятимуть аномальні патерни, що можуть бути характерними для *DDoS* атак. Використання *CDN* (*Content Delivery Network*) може розподіляти трафік та мінімізувати вплив атак. Також, вкрай важливо мати системи фільтрації та обробки трафіку, які можуть відокремити легітимний трафік від атак.

2.3.2 Особливості реалізації атак підсилення

DNS Amplification

- *Збільшення обсягу відповідей:* атакуючі використовують *DNS*-сервери як посередників для збільшення обсягу трафіку. Вони відправляють запити до DNS-серверів з підробленими адресами цільової жертви. *DNS Amplification* базується на тому, що DNS-запити можуть бути короткими, але відповіді можуть бути значно більшими. Атакуючі використовують це, щоб збільшити обсяг зловмисного/паразитного трафіку, використовуючи ресурси легальних *DNS*-серверів.
- *Відсилання запитів у великому масштабі:* атакуючі відправляють велику кількість підроблених DNS-запитів відразу до великої кількості DNS-серверів, збільшуючи тим самим відповіді, які спрямовані на жертву атаки.

NTP Amplification

- *Використання NTP-серверів:* ці атаки використовують *Network Time Protocol (NTP)* для збільшення обсягу паразитного трафіку. Атакуючі відправляють підроблені запити відразу до великої кількості діючих *NTP*-серверів.

Провокування значної сукупності *DNS* та *NTP* серверів до одночасного формування ними відповідей на масштабні короткі злочинні запити, котрі формуються в межах *атак підсилення,* ґрунтується на тому, що такі відповіді можуть бути значно більшими чим запити, що й дозволяє атакуючим збільшити паразитний трафік.

2.3.3 Синтез та використання ботнетів (Botnet-based DDoS)

Синтез та наступне використання ботнетів у *DDoS* атаках є ефективним та небезпечним методом перевантаження мережевих ресурсів цільового об’єкта. Розглянемо деякі основні особливості цього процесу.

Синтез ботнетів DDoS:

- *Створення ботнетів:* зловмисники використовують різноманітні методи для зараження тисяч або навіть мільйонів пристроїв, перетворюючи їх на боти.
- *Координовані атаки:* дозволяє атакуючим синхронізувати дії ботів, направляючи трафік на цільовий сервер одночасно, збільшуючи таким чином вплив атаки.
- *Розподілена відмова в обслуговуванні:* ботнет *DDoS* атаки призводять до розподіленої відмови в обслуговуванні, внаслідок чого цільовий об’єкт стає недоступним для легітимних користувачів.

Особливості DDoS ботнетів:

- *Інфікування:* зараження пристроїв шляхом використання шкідливого ПЗ, експлуатації вразливостей та/або методів соціальної інженерії.
- *Приховане управління:* зловмисники використовують різноманітні методи для прихованого управління ботами, уникнення їх виявлення та блокування.
- *Збільшення ресурсів атаки:* використання ботнетів для збільшення (посилення) обсягу нелегітимного злочинного трафіку та «силового» впливу на цільовий сервер.

Заходи захисту:

- *Мережевий моніторинг: п*остійний моніторинг мережі для виявлення аномалій та надмірного трафіку, які можуть вказувати на DDoS атаку.

- *Виявлення та блокування ботів:* використання систем виявлення ботів для ідентифікації та блокування зламаних пристроїв у ботнеті.
- *Системи фільтрації трафіку:* впровадження швидкодіючих (хмарних) систем фільтрації трафіку, які блокують надмірний трафік та «відсікають» шкідливий.
- *Захист Інтернету речей (IoT):* збільшення поточного рівня безпеки пристроїв IoT, щоб унеможливити їх використання в якості ботів.

2.4 Інші типи кіберзагроз та їхні методи впливу на системи

У світі кібербезпеки існує розмаїття кіберзагроз, які відображаються у різних формах та методах впливу на ІС. Тому приділимо увагу й іншим типам загроз ІБ, зокрема атакам на безпеку мережі та застосунків, уточнюючи їх методи впливу та заходи із захисту.

Атаки на безпеку мережі:

- *Перехоплення трафіку (Man-in-the-Middle):* тип атаки, при якому зловмисники здійснюють перехоплення трафіку між взаємодіючими сторонами, що може призвести до доступу до конфіденційної інформації.
- *Атаки на DNS (Domain Name System):* методи атак на інфраструктуру *DNS* з метою спрямовування трафіку на злочинний ресурс та/чи посилення атак (*див. вище*).

Атаки на застосунки:

- *Хакерські атаки на вразливості коду (SQL Injection, XSS):* техніки використання вразливостей коду для впровадження зловмисного коду або отримання несанкціонованого доступу.
- *Атаки на автентифікацію та онлайн сесії*: методи обходу механізмів автентифікації та зловживання сесій для несанкціонованого доступу.

Вплив на інформаційні системи:

- *Втрата конфіденційності та цілісності даних:* можливі наслідки атак на безпеку мережі і додатків, зокрема, втрати конфіденційності та порушення цілісності даних.
- *Втрата доступності сервісів:* ці атаки можуть впливати на доступність інформаційних систем та відповідних онлайн послуг/сервісів.

Заходи для захисту:

- *Шифрування та/чи приховування (стеганографія) трафіку.*
- *Постійний моніторинг мережі, виявлення вторгнень та/чи припинення недекларованої мережевої активності.*

3. Аналіз вразливостей і можливих стратегії захисту

3.1 Виявлення вразливостей ІС

Виявлення вразливостей ІС, це ключовий етап в забезпеченні їхньої стійкості та захисту від кібератак. У світі, де загрози зростають щодня, ефективні методи виявлення вразливостей стають їх обов'язковою необхідністю [3]. Виявлення цих вразливостей у власних інформаційних системах – перший крок до їхнього ефективного захисту. Тому коротко розглянемо деякі з нових підходів, щодо виявлення вразливостей і розробці стратегій для їхнього негайного парирування.

Методи виявлення вразливостей:

- *Сканування портів та аналіз вразливостей:* автоматизовані засоби можуть проаналізувати «відкриті порти» та визначити потенційні точки входу для атак.
- *Статичний та динамічний аналіз коду:* виявлення вразливостей використовуваного ПЗ, через аналіз вихідного коду, дозволяє виявити вразливості, які можуть бути використані для вторгнень/атаки/витоку даних.

- *Системи виявлення Інтранет-загроз:* моніторинг внутрішнього сегменту мережі для виявлення аномальної мережевої активності та потенційних загроз безпеки.
- *Ethical hacking та Penetration testing:* етичний хакінг (пентестінг) для виявлення існуючих вразливостей з метою їх подальшого усунення (в межах аудиту ІБ).

3.2 Стратегії захисту від різних типів кіберзагроз

Багатошаровий підхід до захисту:

- *Системи виявлення та захисту:* встановлення інтегрованих систем безпеки для виявлення та блокування атак в реальному часі (*IDS/IPS/DLP/HoneyNet* тощо).
- *Фільтрація трафіку:* використання систем фільтрації для блокування небезпечних пакетів трафіку на різних рівнях/сегментах мережі (*proxy, firewall, IPS* тощо).

Сегментація та ізоляція ресурсів:

- *Делегування прав доступу:* обмеження доступу до важливих ресурсів за допомогою делегування прав (*firewalls, біометричні системи, системи захисту від несанкціонованих дій, впровадження алгоритмів виконання сумісних дій та ін.*).

3.3 Заходи із забезпечення стійкості ІС до кібератак

Забезпечення стійкості ІС до кібератак – це необхідна передумова для збереження конфіденційності, цілісності та доступності даних. Сучасний кіберпростір вимагає від організацій постійно вдосконалювати свої стратегії захисту та вживати комплексних заходів для завчасного парирування існуючих загроз ІБ.

- *Захист від внутрішніх загроз.* Розробка та впровадження ефективної корпоративної політики ІБ (ПІБ), включаючи обмеження доступу та моніторинг внутрішніх користувачів, стає важливим етапом у попередженні можливих загроз зсередини.
- *Використання сучасних систем виявлення загроз.* Системи виявлення вторгнень та аномалій дозволяють вчасно виявляти та реагувати на небезпечні активності. Використання штучного інтелекту та машинного навчання (AI/LM) дозволяє автоматизувати процес виявлення навіть найскладніших кіберзагроз.
- *Захист мережі та захист умовного «периметру» безпеки.* Міжмережеві бар'єри та захист «зовнішнього» периметру безпеки, визначають умовну першу лінію захисту. Вони включають в себе використання *firewalls*, систем виявлення вторгнень (*IDS*) та засоби фільтрації трафіку (корпоративні *proxy* та *DLP* тощо) для блокування можливих атак/витоку даних на рівні мережі.
- *Управління доступом та автентифікація.* Забезпечення стійкості включає в себе також впровадження ефективної системи управління доступом та багатофакторної автентифікації. Це дозволяє обмежити доступ до чутливої інформації та ускладнює можливі атаки на облікові записи користувачів.
- *Регулярні аудити стану безпеки та оновлення ПЗ та ПІБ.* Проведення систематичних аудитів поточного стану ІБ для виявлення існуючих вразливостей та невикористаних можливостей є ключовим аспектом безпеки. Регулярне оновлення програмного та апаратного забезпечення дозволяє усувати виявлені вразливості та підтримувати систему в актуальному стані.

3.4 Вплив рівню технологічного розвитку у забезпеченні ІБ

Технологічний розвиток є неодмінним фактором впливу на рівень безпеки сучасних ІС. Постійний прогрес у галузі інформаційних технологій (ІТ) створює нові можливості для забезпечення ІБ та вимагає від організацій постійного адаптування до змін у кіберпросторі. Тож коротко розглянемо основні з найбільш перспективних технологій:

- *Штучний інтелект та машинне навчання (AI та LM)*

Застосування технологій *AI* та *LM* в галузі кібербезпеки дозволяє автоматизувати виявлення та аналіз аномалій в мережах. Алгоритми машинного навчання можуть швидко адаптуватися до нових типів загроз, забезпечуючи більш ефективний захист.

- *Блокчейн для забезпечення «імунітету» до змін*

Технологія блокчейн визначається своєю децентралізацією та непроникністю до змін. У сфері кібербезпеки, вона може служити основою для безпечного зберігання та обміну конфіденційної інформації, запобігаючи атакам на централізовані системи.

- *Квантова обчислення та технології віртуалізації процесів (VR)*

З розвитком квантових технологій виникає можливість у нових методах аналізу мережевого трафіку, віртуалізації процесів, каскадування обчислювальних можливостей та криптографічного захисту даних. Квантові комп'ютери можуть «зламувати» традиційні криптографічні алгоритми, тому створення нових квантово-стійких захисних методів, дедалі стає все більш актуальним завданням ІБ.

- *Інтернет речей (IoT) та кіберфізичні системи*

Розширення Інтернету речей передбачає додавання та й маніпулювання величезними обсягами додаткових даних, що потребують їх ефективного захисту. Розвиток кіберфізичних систем дозволяє об'єднати в собі фізичний та кібер- світи, вимагаючи при цьому впровадження інноваційних технологій й методів безпеки.

- *Спрощення управління безпекою через Cloud Security*

Використання сукупності хмарних та *VR* технологій дозволяє компаніям зосередитися на вдосконаленні стратегій безпеки, адже адміністрування та оновлення захисних систем може бути здійснене централізовано [4].

4. Висновки

1. На сьогоднішній день кіберзагрози створюють загрози для конфіденційності, цілісності та доступності інформації. Зростання залежності суспільства від поточного рівня розвитку й впровадження ІТ підкреслює актуальність питання захисту ІС від кіберзагроз.

2. Проведено аналіз впливу різних типів кіберзагроз на ІС та розглянуті основні стратегії щодо їх захисту. Запропоновано огляд нових тенденцій у кібербезпеці і деяких інноваційних підходів з питань захисту від нових загроз. Підкреслено наявність нерозривного взаємозв'язку питань технологічного розвитку й фактичного стану можливостей із ІБ.

3. Підкреслено необхідність постійного оновлення й адаптації діючих стратегій захисту до зростаючої складності кіберзагроз. Звернено увагу, що захист ІС вимагає одночасного поєднання впровадження інноваційних технологій, глибокого розуміння сучасних тенденцій кібербезпеки та глобальної співпраці для ефективної протидії актуальним кіберзагрозам.

Список літератури

[1] Jon Erickson (2010). "Hacking: The Art of Exploitation"

[2] Edward Amoroso. (2010). "Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare"

[3] P.W. Singer та Allan Friedman (2014). "Cybersecurity and Cyberwar: What Everyone Needs to Know"

[4] International Journal of Computer Science and Information Technologies "Cybersecurity: A Journal of Technology, Society and Policy".

Received: on November 2023. **Accepted:** on December 2023.

Authors:
Osadchyi Yevhenii, CSD Student, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: xa12850357@student.karazin.ua
Yesina Maryna, Ph.D., Associate Professor, department of security of information systems and technologies, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine; research associate-consultant of JSC "IIT", Kharkiv, Ukraine.
E-mail: m.v.yesina@karazin.ua
ORCID: https://orcid.org/0000-0002-1252-7606

Victor Onoprienko, Ph.D., CEO of JSC "IIT", Kharkiv, Ukraine.
E-mail: v25258@gmail.com

The influence of different forms of cyber threats on the stability of information systems: analysis and protection strategies

Abstract. This work is dedicated to the further investigation of cybersecurity issues in the context of the ongoing development of the current information industry. Starting with an overview of various forms of cyber threats, the article examines the analysis of their impact on the privacy, integrity and availability of information. The critical dependence of modern society on information technology makes the topic of protection against cyber threats extremely relevant. This work offers an in-depth analysis of the growth in the number and complexity of cyber threats, which requires constant improvement and updating of protection strategies against them. An important stage of coverage of the topic is the analysis of the impact of various forms of cyber threats on information systems. The main types of phishing and social engineering are considered, as well as the consequences of exposure to viruses, Trojans and other malicious programs. A detailed review of these aspects allows us to highlight the key issues and dangers that arise in the context of cyber threats. Also, the article contains materials devoted to various protection strategies. It examines effective strategies for protecting information systems, including identifying vulnerabilities, using multi-factor authentication, and measures to ensure resilience. The general conclusions of this work summarize the need for constant updating and adaptation of protection strategies in relation to the growing complexity of cyber threats in the world of rapid technological development. In general, this work is another step in understanding the essence of the challenges associated with the issue of ensuring cyber security in the modern information society.

Keywords: Impact, Cyber Threat, Analysis And Protection, Resilience Of Information Systems, Protection Strategies.