ISSN 2786–6920
НАУКОВИЙ ВІСНИК КИЇВСЬКОГО ІНСТИТУТУ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ №2 2024

УДК 347.78.034:347.77.043
DOI 10.59226/2786-6920.2.2024.43-48

КОМІССАРОВА НАТАЛЯ ОЛЕКСАНДРІВНА

кандидат юридичних наук, доцент,
начальник кафедри державної безпеки
факультету забезпечення державної безпеки
Київського інституту Національної гвардії України
ORCID ID 0000-0001-6895-6891

КРУТІКОВ ПАВЛО ДМИТРОВИЧ

здобувач вищої освіти
факультету забезпечення державної безпеки
Київського інституту Національної гвардії України
ORCID ID 0009-0000-2041-1411

СИСТЕМА КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВЕДЕННЯ ВІЙНИ

У статті окреслено проблему впливу інформаційних загроз, кібератак, кібершпигунства на об'єкти критичної інфраструктури в умовах ведення війни.

Стаття дає змогу краще зрозуміти важливість захисту об'єктів критичної інфраструктури для забезпечення національної безпеки, а також ідентифікувати інформаційні загрози, кібератаки, виявляти операції кібершпигунства як потенційні загрози та ризики для об'єктів критичної інфраструктури, визначати недоліки в наявних системах захисту.

Описано основні типи інформаційних загроз, що охоплюють кібератаки та кібершпигунство. Значущим є виявлення цих загроз, які можуть серйозно пошкодити об'єкти критичної інфраструктури, як-от енергетичні системи, водопостачання, транспортні мережі та комунікації.

Запропоновані аналіз і рекомендації спрямовано на підвищення ефективності заходів захисту об'єктів критичної інфраструктури та зменшення ризиків їхнього негативного впливу на національну безпеку.

На основі цього аналізу можна розробляти конкретні рекомендації, які забезпечують підвищення ефективності заходів захисту. Зокрема, передбачити оновлення технологічної бази, проведення регулярних тренінгів для персоналу, вдосконалення законодавства та впровадження сучасних методів виявлення та нейтралізації загроз. Важливо створювати резервні копії даних та зберігати їх в офлайн-режимі. Це дозволить відновити їх у разі успішної кібератаки або інших непередбачуваних подій.

Загалом дослідження доводить важливість комплексного підходу щодо захисту критичної інфраструктури, що охоплює не лише технічні, а й організаційні та нормативні заходи. Це забезпечить надійніший захист національної безпеки в умовах сучасних загроз.

Ключові слова: *критична інфраструктура; інформаційна інфраструктура; кібератака; кібершпигунство; шпигун; інформаційна система; ведення війни; війна; кримінальне правопорушення; злочинність; протидія злочинності.*

Постановка проблеми. Сучасний світ стрімко розвивається в умовах диджиталізації всіх сфер суспільства. Інноваційні технології стали невід'ємною складовою нашого життя, відіграючи ключову роль в організації як роботи, так і відпочинку. Значна частина цих технологій базується на використанні

даних різного типу, які обробляються за допомогою спеціального програмного забезпечення та новітніх технологій. Інформація нині є не лише одним із основних ресурсів, від якого залежить існування та функціонування різних об'єктів, явищ та систем, а й ресурсом для їх оновлення, трансформації та розвитку.

Значущість інформації в нашому житті та в організації ефективного функціонування економічних об'єктів стимулює постійний пошук науковців у напрямі створення досконалих методів та механізмів роботи з даними. Це дозволяє максимально спростити процеси, які доцільно автоматизувати та уніфікувати. Інформація також є ресурсом для змін та управління, оскільки її обіг усередині систем забезпечує їх розвиток, вдосконалення та адаптацію до змін зовнішнього середовища, що дозволяє їм виконувати необхідні функції і забезпечувати постійний розвиток.

Під час військової агресії російської федерації проти України ворог активно використовує комп'ютерні технології для вчинення воєнних злочинів шляхом кібератак на об'єкти критичної інфраструктури.

Мета дослідження полягає в тому, щоб надати комплексне розуміння проблематики кібербезпеки критичної інфраструктури, а також запропонувати ефективні рішення для поліпшеня захисту та зменшення ризиків, пов'язаних з інформаційними загрозами.

Важливим є визначення та класифікування основних видів інформаційних загроз, кібератак та кібершпигунства, які можуть вплинути на критичну інфраструктуру. Вивчення різних технік та інструментів, що використовують зловмисники, а також аналіз їхньої еволюції у контексті сучасних технологічних досягнень допоможе виявити нові вектори атак, кіберзагроз у реаліях сучасної війни.

Необхідно також провести детальне оцінювання потенційних ризиків та наслідків для об'єктів критичної інфраструктури у випадку успішних кібератак чи актів кібершпигунства. У полі зору дослідження – аналіз імовірних сценаріїв розвитку подій та їхнього впливу на функціонування життєво важливих систем і забезпечення неперервності їхньої роботи

Аналіз останніх досліджень і публікацій. Згідно з аналізом останніх досліджень і публікацій Держспецзв'язку, кількість кібератак у 2022 році становила 2194, з яких – 1048 кіберінцидентів мали високий або критичний рівень. У 2023 році загальна кількість кіберінцидентів – 2554, із них лише 367 серйозні [9].

Перші місяці цього року демонструють збільшення кількості кібератак, які здійснюють російські хакери на українські інформаційні системи. Тому варто очікувати, що 2024 рік для нашої країни буде важчим з погляду ведення кібервійни. У першому кварталі 2024 року Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, серед іншого, вжила заходи з недопущення реалізації зловмисного задуму, який полягав у проведенні деструктивного впливу щодо трьох українських організацій урядового та енергетичного секторів.

Однією з найактивніших загроз є угруповання найманців UAC-0050, пов'язаних із російськими правоохоронними органами. Вони оголосили про завершення своєї «професійної» діяльності під назвою DaVinci Group за кілька днів до російського вторгнення у 2022 році, але останнім часом знову активно нагадують про себе.

Станом на 22 лютого 2024 року було виявлено і досліджено щонайменше 15 кампаній, під час яких зловмисники використовували п'ять видів шкідливих програм: REMCOS RAT, QUASAR RAT, VENOM RAT, REMOTE UTILITIES та LUMMASTEALER. Попри те, що лише незначна частина їхньої діяльності оприлюднюється в Telegram-каналі, їх тактика нагадує діяльність брокерів первинного доступу.

Зважаючи на масовість атак і використання програм, призначених для викрадення автентифікаційних даних, скомпрометовані логіни, паролі та сертифікати можуть створювати технічні передумови для несанкціонованого доступу до інформаційно-комунікаційних систем організацій, що дозволить розвивати атаки на їхні внутрішні ресурси.

Також команда реагування на комп'ютерні надзвичайні події України CERT-UA, згідно із Законом України «Про основні засади забезпечення кібербезпеки України», виявила, що однією з найбільших «кіберзагроз» є UAC-0010 (Armageddon). Ця загроза походить від колишніх «офіцерів» ГУ СБУ в АР Крим, які у 2014 році зрадили військовій присязі і стали служити ФСБ російської федерації. Головною метою цієї групи є кібершпигунство стосовно безпеки та оборони України. Згідно з наявною інформацією, кількість одночасно інфікованих комп'ютерів, переважно у системах державних органів, може сягати кількох тисяч.

Виклад основного матеріалу. Своєю чергою кібератаки спрямовано на об'єкт інформаційної інфраструктури, що стає безпосередньою мішенню для нанесення шкоди або виступають як система керування іншим об'єктом критичної інфраструктури. Об'єкти критичної інфраструктури охоплюють системи, їх компоненти та сукупності, які є важливими для економіки, національної безпеки та оборони.

Порушення їх функціонування може завдати шкоди життєво важливим національним інтересам.

Відповідно до Постави Кабінету Міністрів України наявні 25 секторів, які належать до критичної інфраструктури: паливно-енергетичний сектор; цифрові технології; захист інформації; системи життєзабезпечення; харчова промисловість та агропромисловий комплекс; державний матеріальний резерв; охорона здоров'я; ринки капіталу та організовані товарні ринки; фінансовий сектор; транспорт і пошта; промисловість; сектор громадської безпеки; цивільний захист населення і територій; міграція (імміграція та еміграція); охорона навколишнього природного середовища; сектор оборони; національна безпека; правосуддя; тримання під вартою; наукові дослідження та розробки; фінансовий сектор; вибори та референдуми; соціальний захист; інформаційні послуги; державна влада та місцеве самоврядування [2].

Кібератака (кібернетична атака, хакерська атака) – це навмисні дії в кіберпросторі, що здійснюються за допомогою електронних комунікаційних засобів (зокрема інформаційно-комунікаційних технологій, програмних та апаратних засобів, іншого технічного та технологічного обладнання). Такі атаки спрямовано на досягнення кількох основних цілей: порушення конфіденційності, цілісності та доступності електронних інформаційних ресурсів, які обробляються, передаються або зберігаються в комунікаційних та технологічних системах; отримання несанкціонованого доступу до цих ресурсів; порушення безпеки, стабільного та надійного функціонування комунікаційних та технологічних систем; використання комунікаційної системи та її ресурсів для проведення кібератак на інші об'єкти кіберзахисту.

Із цим пов'язано таке поняття у сфері кібербезпеки як «кіберзагроза» – наявні або потенційно можливі явища та фактори, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі та мають негативний вплив на її стан. Хакерська атака (кібератака) – це спроба реалізації кіберзагрози, тобто дії кіберзловмисників (хакерів) або шкідливих програм, спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над його ресурсами або виведення системи з ладу.

Отже, кібератака – це напад на інформаційну інфраструктуру, який охоплює сукупність взаємопов'язаних дій порушника (ініційованих ним процесів), що призводять до реалізації загроз інформаційним ресурсам шляхом використання вразливостей певної інформаційної системи як частини цієї інфраструктури.

Умовно можна розрізняти два типи кібератак, залежно від місця перебування зловмисника під час атаки, що має значення для виявлення осіб, відповідальних за атаку, та ступеня їх дії:

Локальне проникнення (local penetration) – зловмисник перебуває всередині об'єкта та використовує прямий доступ до інформаційної системи.

Віддалене проникнення (remote penetration) – зловмисник перебуває поза системою та використовує віддалений доступ для здійснення атаки на інформаційні ресурси.

Найбільш поширеними видами є віддалені (зовнішні) кібератаки до яких належать:

Фішинг – відправлення підроблених електронних листів від імені довірених компаній або інших надійних джерел. Зловмисники використовують фішинг для того, щоб отримати доступ до особистих даних у корпоративних або особистих мережах.

SQL-ін'єкції – це метод поширення шкідливого програмного забезпечення через вразливості програм, таких як LinkedIn або Target, що дозволяє кіберзловмисникам викрасти або видалити дані, а також отримувати контроль над ними.

Міжсайтові сценарії (XSS) – це атаки, під час яких кіберзловмисники відправляють зловісні або заражені сценарії поштою чи іншими каналами комунікації. Після того, як їх відкрито, зловмисник отримує доступ до вашої особистої інформації [7].

Для пошуку способів вторгнення в інформаційну систему широко використовують спеціальні програмно-технічні засоби: мережеві сканери, сканери вразливостей, зламувачі паролів, аналізатори протоколів тощо.

Аналізатори протоколів – метод отримання інформації, що базується на роботі мережевої карти в спеціальному режимі, що дозволяє отримати значну кількість службової інформації. Найбільшою небезпекою такої атаки є отримання логінів і паролів, які можна використовувати для незаконного доступу.

Перехоплення каналу зв'язку (Man-in-the-Middle) – атака, коли зловмисник перехоплює зв'язок між двома системами і отримує доступ до переданої інформації. Це може дозволити зловмиснику модифікувати передану інформацію або отримати доступ до ресурсів мережі. Ці атаки важко виявити, оскільки зловмисник зазвичай перебуває всередині мережі і може діяти анонімно.

Атака на відмову в обслуговуванні (denial of service або DoS) – атака, що має на меті змусити сервер не відповідати на запити. Такий вид атаки не передбачає отримання деякої секретної інформації, але іноді буває підмогою в ініціалізації інших атак. Наприклад, деякі програми через помилки в своєму коді можуть викликати виняткові ситуації і при від'єднанні

сервісів здатні виконувати код, наданий зловмисником або атаки лавинного типу, коли сервер не може обробити величезну кількість вхідних пакетів. DDoS (від англ. Distributed Denial of Service – Розподілена DoS) – підтип DoS-атаки, що має ту саме мету, що і DoS, але вони проводяться не з одного комп'ютера, а з декількох комп'ютерів у мережі [3].

У таких типах атак використовується або виникнення помилок, що призводять до відмови сервісу, або спрацьовування захисту, що приводить до блокування роботи сервісу, а в результаті також до відмови в обслуговуванні. DDoS використовується там, де звичайний DoS неефективний. Для цього кілька комп'ютерів об'єднуються, і кожен виробляє DoS-атаку на систему жертви. Разом це називається DDoS-атака.

Будь-яка атака є спробою використовувати недосконаліть системи безпеки жертви або для отримання інформації, або для нанесення шкоди системі, тому причиною будь-якої вдалої атаки є професіоналізм крекерів і цінність інформації, а також недостатня компетенція адміністратора системи безпеки, зокрема, недосконаліть програмного забезпечення та недостатня увага до питань безпеки в компанії у цілому.

Спам e-mail (Mailbombing) вважають найстарішим методом атак, хоча за змістом він простий і примітивний: значна кількість поштових повідомлень унеможливлює роботу з поштовими скриньками, а іноді і з цілими поштовими серверами. Було розроблено безліч програм, і навіть недосвідчений користувач може зробити атаку, вказавши всього лише e-mail жертви, текст повідомлення, кількість необхідних повідомлень. Такі програми дозволяють ховати реальний IP-адрес відправника, використовуючи для розсилки анонімний поштовий сервер [3].

Статистика кіберзлочинності показує зростання використання різних інструментів для шпигунства, які охоплють як спеціалізовані пристрої, так і програмне забезпечення. Порівняно з традиційними методами розвідки та шпигунства, нові технології значно модифікували ці практики. Часто вже неможливо визначити, хто саме створив певне програмне забезпечення для проведення розвідувальних або шпигунських операцій у високих технологіях. Такі програми можуть розробляти як приватні особи, так і організації з різними джерелами фінансування, зокрема державними коштами.

Як зазначає директор з розвідки компанії з кібербезпеки бізнесу Red Canary, та старший науковий співробітник програми Cyber Statecraft Initiative Атлантичної ради Кеті Нікелс, «кібершпигунство» є характерним для російських розвідувальних служб, які фінансуються державою-противником. Вони прагнуть здобути інформацію про урядові та пов'язані з урядом об'єкти. Це вимагає іншої політичної реакції, ніж щодо російських кіберзлочинців, які стоять за більшістю атак вимагачів. За її словами, державні структури російської федерації здійснюють шпигунство повністю під контролем уряду, тоді як оператори програм викупів, можливо, не мають прямого контролю російського уряду [7].

Висновки та перспективи подальших досліджень. Отже, протидія кібератакам на об'єкти критичної інфраструктури є надзвичайно важливою для забезпечення безпеки суспільства та ефективного функціонування економіки.

У цьому контексті визначено важливість розробляти та впроваджувати комплексні заходи кібербезпеки, що охоплюють моніторинг та виявлення потенційних загроз, вдосконалення технічних засобів захисту, а також навчання персоналу та своєчасну реакцію на виявлені загрози.

Регулярне створення резервних копій важливих даних та збереження їх в офлайн-режимі дозволить відновити дані у разі успішної кібератаки або інших непередбачуваних подій.

До того ж співпраця між урядовими органами, приватним сектором та міжнародними партнерами є ключовою для ефективної протидії кібератакам на об'єкти критичної інфраструктури. Лише завдяки взаємодії та обміну інформацією можна забезпечити високий рівень захисту та реагувати на кіберзагрози вчасно і ефективно. Важливо впроваджувати ефективні методи шифрування для захисту конфіденційної інформації. Шифрування або криптографічний захист бази даних є одним з найбільш ефективних методів забезпечення безпеки БД.

Алгоритм шифрування перетворює інформацію на незрозумілі символи за допомогою математичного процесу. У той час, як інші інструменти безпеки захищають систему від вторгнень або атак, шифрування є фундаментальною формою, яка стосується безпеки самих даних. Це означає, що навіть у разі злому системи інформація буде доступна для читання тільки авторизованим користувачам, які мають ключі шифрування. Розробіть суворі правила доступу до даних та мінімізуйти кількість працівників (співробітників), які мають повний доступ до цієї інформації.

Крім того, постійне вдосконалення заходів кібербезпеки та адаптація до нових викликів і загроз є необхідними для забезпечення стійкості об'єктів критичної інфраструктури до потенційних кібератак.

Список використаних джерел

1. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт.

нарад / Упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. Київ : НІСД, 2016, 176 с.

2. Указ Президента України від 15.03.2016 р. № 96/2016 «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року «Про Стратегію кібербезпеки України». Режим доступу: http://zakon2.rada.gov.ua/laws/show/96/2016.

3. Указ Президента України №189/2014 від 02.03.2014р. «Про рішення Ради національної безпеки і оборони України від 1 березня 2014 року «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України». Режим доступу: http://zakon2.rada.gov.ua/laws/show/189/2014

4. GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION. Retrieved from http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf.

5. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection. Retrieved from :// eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

6. A Communication on Protecting Europe's Critical Energy and Transport Infrastructure (цей документ містить чутливу інформацію, і тому не підлягає публікації).

7. COUNCIL DIRECTIVE 2008/114/EC of 8 December on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

8. Постанова Кабінету Міністрів України від 16 січня 2024 р. № 48 зі змінами, що вносяться до постанови Кабінету Міністрів України від 9 жовтня 2020 р. № 1109.

9. Державна служба спеціального зв'язку та захисту інформації України «Щодо обстановки в сфері кібер на 23-24 лютого 2024 року». Режим доступу: https://cert.gov.ua/article/6277822.

References

1. Green book on the protection of critical infrastructure in Ukraine: coll. materials of international expert. Meeting.,Arrangement D.S. & Biryukov, S.I. & Kondratov, Kyiv: NISD, 176p. [in Ukrainian]

2. Ukaz Prezydenta Ukrainy vid 15.03.2016 r. № 96/2016 «Pro rishennia Rady natsionalnoi bezpeky i oborony» [Decree of the President of Ukraine dated March 15, (2016), 96. *On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016*]. (15 March 2016) [in Ukrainian].

3. Ukaz Prezydenta Ukrainy №189/2014 vid 02.03.2014r. «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 1 bereznia 2014 roku «Pro nevidkladni zakhody shchodo zabezpechennia natsionalnoi bezpeky, suverenitetu i terytorialnoi tsilisnosti Ukrainy» [Decree of the President of Ukraine, dated March 2, (2014), 189. *«On the decision of the National Security and Defense Council of Ukraine dated March 1, 2014 «On urgent measures to ensure the national security, sovereignty and territorial integrity of Ukraine»*] (2 March 2014) [in Ukrainian].

4. Zelena knyha pro yevropeisku prohramu zakhystu krytychnoi infrastruktury 2005 r. [Green paper on a european program for critical infrastructure protection 2005]. eur-lex.europa.eu. Retrieved from: http:// eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf. [in English].

5. Zasidannia komisii shchodo Yevropeiskoi prohramy zakhystu krytychnoi infrastruktury [Communication from the Commission of 12 December (2006) *«On a European Program for Critical Infrastructure Protection*] (12 December 2006) [in English].

6. Povidomlennia pro zakhyst krytychno vazhlyvoi enerhetychnoi ta transportnoi infrastruktury Yevropy (*tsei dokument mistyt konfidentsiinu informatsiiu i tomu ne pidliahaie publikatsii*) [A Communication on Protecting Europe's Critical Energy and Transport Infrastructure (*this document contains sensitive information and is therefore not subject to publication*)] (27 September 2008) [in English].

7. Dyrektyva Rady EC /114 vid 8 hrudnia 2008 (*pro identyfikatsiiu ta poznachennia yevropeiskykh krytychnykh infrastruktur ta otsinku neobkhidnosti pokrashchennia yikh zakhystu*). [Council directive (2008) /114/EC of 8 December on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection]. eur-lex.europa.eu. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF. [in English].

8. Postanova Kabinetu Ministriv Ukrainy vid 16 sichnia 2024 r. № 48 zi zminamy shcho vnosiatsia do postanovy Kabinetu Ministriv Ukrainy vid 9 zhovtnia 2020 r. № 1109 [Resolution of the Cabinet of Ministers of Ukraine dated January 16, (2024), 48, *[with amendments to Resolution of the Cabinet of Ministers of Ukraine dated October 9, 2020]*, 1109. (16 January 2024). [in Ukrainian].

9. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy «Shchodo obstanovky v sferi kiber na 23-24 liutoho 2024 roku» [State Service of Special Communications and Information Protection of Ukraine (2024) «*Regarding the situation in the cyber sphere on February 23-24*»]. cert.gov.ua. Retrieved from: https:// /cert.gov.ua article/6277822.[in Ukrainian].

Komissarova Natalia
PhD in Law, Associate Professor,
Head of the Department of State Security
of the Faculty of State Security,
Kyiv Institute of the National Guard of Ukraine

Krutikov Pavlo
Graduate of the Faculty of State Security,
Kyiv Institute of the National Guard of Ukraine.

CYBER PROTECTION SYSTEM FOR CRITICAL INFRASTRUCTURE FACILITIES IN WARFARE CONDITIONS

The article outlines the problem of the impact of information threats, cyber attacks, and cyber espionage on critical infrastructure facilities in the context of warfare.

The work allows for a better understanding of the importance of protecting critical infrastructure facilities for ensuring national security.

To identify information threats, cyber attacks, manifestations of cyber espionage, which are potential threats and risks to critical infrastructure objects and to identify shortcomings in existing protection systems.

The main types of information threats are described, which include cyber attacks and cyber espionage. The importance of identifying these threats, which can seriously damage critical infrastructure facilities such as energy systems, water supply, transport networks and communications

The analysis and recommendations developed in the work can help increase the effectiveness of measures to protect critical infrastructure objects and reduce the risks of their negative impact on national security.

Based on this analysis, specific recommendations can be developed that can contribute to increasing the effectiveness of protection measures. This may include updating the technological base, conducting regular training for personnel, improving legislation, and implementing modern methods of detecting and neutralizing threats. Regularly back up important data and store it offline. This will allow data recovery in the event of a successful cyber attack or other unforeseen events.

In general, the study emphasizes the importance of a comprehensive approach to the protection of critical infrastructure, which includes not only technical, but also organizational and regulatory measures. This will ensure more reliable protection of national security in the face of modern threats.

Keywords: *critical infrastructure; information infrastructure; cyber attack; cyber espionage; sp; information system; warfare; war; criminal offense; crime; counter crime.*