УДК 004.056.5:338.49(045)

Д. Ю. Радзіховський

ОСОБЛИВОСТІ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вінницький національний технічний університет

Анотація. *В статті акцентовано увагу на актуальності проблеми кіберзахисту підприємств критичної інфраструктури у період війни. Розглянуто особливості інформаційної безпеки вказаних підприємств. Наголошено на необхідності запровадження надійних засобів контролю безпеки підприємств критичної інфраструктури, а також впровадження міжнародних стандартів і врахування передового досвіду*.

Ключові слова. Підприємства критичної інфраструктури, кіберзахист, інформмаційна безпека, кібератака.

Abstract. *The article focuses on the relevance of the problem of cyber protection of critical infrastructure enterprises during the war. The peculiarities of information security of the specified enterprises are considered. It was emphasized the need to introduce reliable means of monitoring the safety of critical infrastructure enterprises, as well as the implementation of international standards and consideration of best practices*.

Keywords. Enterprises of critical infrastructure, cyber protection, information security, cyber-attack.

Нині питання безпеки інформаційних ресурсів, технологій захисту інформації є досить важливим. Особливої актуальності проблеми кіберзахисту набувають у військовий період, коли на інформаційні ресурси країни щоденно здійснюється сотні атак. Кібербезпека є критичною проблемою для організацій будь-якого розміру та типу. Із зростанням залежності від технологій та Інтернету загроза кібератак стає більшою, ніж будь-коли. Найбільшу зацікавленість ворог проявляє до об'єктів критичної інфраструктури: застосовуються як фізичні атаки ракетами та дронами, так і кібератаки.

Загальна кількість кібератак за 9 місяців війни складає понад 1 200 000 випадків. Кількість DDos-атак на сайти ключових енергетичних компаній і Міністерства – більше 50, для порівняння з початку фіксації такого типу атак з 2019 року їх було тільки 5. Україна щодня набуває нового унікального досвіду у протидії кіберзагрозам, і після перемоги у війні з Росією буде готова розкрити всі деталі щодо інструментарію хакерських атак, які використовує агресор. Динаміка та інтенсивність блокування тих чи інших ресурсів кіберспеціалістами збільшилася в сотні разів та за час війни досягла цифри +20 000 [1].

Проблеми кіберзахисту підприємств, організацій розглянуто у працях багатьох вітчизняних та зарубіжних дослідників, зокрема П. Жаркова, Р. Калюжного, Б. Кормич, , Н. Ткачук та інших. Проте в умовах війни це питання потребує постійного удосконалення, зокрема, посиленої уваги потребують питання кіберзахисту об'єктів критичної інфрастрккктури. Розглянемо особливості розв'язання вказаного питання.

Відповідно до чинного законодавства, об’єктами критичної інфраструктури є підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей [2]. Отже, об’єкти критичної інфраструктури – електростанції, водоочисні споруди, транспортні системи, які необхідні для функціонування суспільства. Проте ці об’єкти також є серйозною мішенню для кібератак у період війни, оскільки порушення їх роботи може мати серйозні наслідки для громадського здоров’я, безпеки загалом та економічної безпеки. Як наслідок, інформаційний захист об’єктів критичної інфраструктури є критичною проблемою для країн, їх урядів, організацій, окремих осіб, особливо у військовий період.

19 червня 2019 р. вийшла постанова кабінету міністрів України №м 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури», в якій передбачається, що

кіберзахист об’єкта критичної інфраструктури забезпечується шляхом впровадження на об’єкті критичної інформаційної інфраструктури комплексної системи захисту інформації. Об’єкт критичної інфраструктури повинен мати у своєму складі підрозділ або посадову особу з інформаційної безпеки, що відповідають за політику інформаційної безпеки, прийняту на об’єкті критичної інфраструктури, та контроль за її дотриманням. На об’єкті критичної інфраструктури повинно бути затверджено політику управління ризиками інформаційної безпеки і методику їх оцінювання та оброблення. В додатку до вказаної постанови сформульовано вимоги щодо ідентифікації та автентифікації користувачів та адміністраторів об’єкта критичної інформаційної інфраструктури, реєстрації подій компонентами об’єкта критичної інформаційної інфраструктури та їх періодичний аудит, забезпечення мережевого захисту компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури, умов використання програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури [3].

Як відмічають науковці, на сьогодні єдиний перелік об’єктів критичної інфраструктури в Україні відсутній, а захист об’єктів, які згідно із світовою практикою відносять до категорії “критичної інфраструктури”, регламентується численними нормативно-правовими актами, що носять переважно відомчий характер .

Одна з головних проблем, з якою стикаються державні підприємства, коли йдеться про кіберзахист, полягає в величезному обсязі та різноманітності даних, які вони зберігають. Це може включати конфіденційну інформацію, особисті дані співробітників і клієнтів, а також інтелектуальну власність і комерційну таємницю. Як наслідок, на таких підприємствах повинні бути надійні стратегії захисту інформації, щоб захистити ці дані від несанкціонованого доступу, використання або розголошення.

Однією з базових проблем захисту об’єктів критичної інфраструктури є інтеграція систем інформаційних технологій (IT) і операційних технологій (OT). У той час як IT-системи призначені для підтримки бізнес-операцій, системи OT використовуються для контролю та моніторингу фізичних процесів. Інтеграція цих систем призвела до підвищення ефективності та економії коштів, але також створила нові вразливості, якими можуть скористатися кіберзлочинці.

Щоб захистити об’єкти критичної інфраструктури, необхідно впровадити надійні засоби контролю безпеки. Це включає використання брандмауерів, систем виявлення вторгнень та інших технологій безпеки для запобігання несанкціонованому доступу до мереж і систем організації. Крім того, важливу роль грає впровадження шифрування для конфіденційних даних і інформації, а також застосування контролю доступу, щоб гарантувати, що лише авторизовані особи мають доступ до конфіденційних даних. Брандмауери використовуються для контролю доступу до мережі шляхом блокування несанкціонованого трафіку, тоді як системи виявлення вторгнень відстежують мережеву активність на наявність ознак зловмисної діяльності. Обидві ці технології можуть мати вирішальне значення для виявлення та запобігання кібератакам.

Іншим важливим аспектом захисту інформації є реалізація політик і процедур безпеки. Це включає розробку планів реагування на інциденти, регулярні тренінги з питань безпеки для співробітників і регулярні аудити безпеки для виявлення й усунення потенційних вразливостей. Крім того, також потрібно мати програму управління даними, щоб забезпечити належну класифікацію, обробку та утилізацію конфіденційних даних відповідно до норм і законів.

Окрім впровадження заходів безпеки та політики, потрібно знати про потенційні загрози, з якими вони можуть зіткнутися на вказаних об’єктах. Це включає моніторинг ознак кібератак, таких як незвичайна мережева активність або спроби неавторизованого доступу, а також отримання інформації про останні вразливості та загрози. На нинішньому етапі варто налагодити співпрацю із зовнішніми експертами, консультантами з безпеки, щоб допомогти виявити й усунути потенційні інформаційні ризики об’єктів критичної інфраструктури.

Іншим важливим аспектом кібербезпеки є використання надійних паролів та інших методів автентифікації. Надійні паролі необхідні для захисту від атак грубої сили, які передбачають використання автоматизованого програмного забезпечення для вгадування та перевірки великої кількості комбінацій паролів, щоб отримати доступ до облікового запису. Окрім використання надійних паролів, також слід розглянути впровадження двофакторної автентифікації, яка передбачає використання другої форми ідентифікації, наприклад відбитка пальця або маркера безпеки, на додаток до пароля.

Одним із найпоширеніших способів кіберзлочинців отримати доступ до конфіденційної інформації є фішинг. Фішингове шахрайство зазвичай здійснюється через електронну пошту чи інший електронний зв'язок і передбачає використання тактики соціальної інженерії, щоб обманом змусити людей надати особисту або фінансову інформацію. Ці шахрайства можуть приймати різні форми, наприклад підроблені електронні листи або веб-сайти, які нібито належать законним організаціям, але насправді контролюються кіберзлочинцями. Щоб захиститися від фішингу, потрібно знати про загальні тактики та прийоми, які використовують кіберзлочинці. Наприклад, важливо остерігатися електронних листів або веб-сайтів, які просять надати особисту або фінансову інформацію, особливо якщо вони несподівані або небажані. Крім того, важливо бути обережним, натискаючи посилання або завантажуючи вкладені файли з невідомих джерел, оскільки вони часто можуть призвести до зловмисного або іншого шкідливого програмного забезпечення.

Також важливим аспектом захисту об'єктів критичної інфраструктури є розвиток міжнародних стандартів і врахування передового досвіду. Керівники та урядовці повинні працювати разом, щоб розробити та впровадити стандарти для захисту об'єктів критичної інфраструктури, наприклад NIST Cybersecurity Framework, який забезпечує основу для управління ризиками кібербезпеки. Крім того, організаціям також слід розглянути можливість участі в центрах обміну та аналізу інформації (ISAC) та інших форумах обміну інформацією, щоб бути в курсі останніх загроз і вразливостей.

Зауважимо, що нині на базі НЕК "Укренерго" та НАК "Нафтогаз України" створено кіберцентри, які займаються кіберзахистом об'єктів, що належать вказаним структурам.

Відмітимо також, що протягом грудня 2021 та січня-лютого 2022 росіяни багаторазово намагалися здійснити втручання в роботу ключових енергетичних компаній, зламати персональні кабінети клієнтів, а також втрутитися в роботу диспетчерських центрів. Водночас високий рівень кіберзахисту українського енергосектору не дозволив країні-агресору досягнути поставлених цілей [1].

Підсумовуючи вищесказане можна зробити висновок, що кібербезпека – це сфера, яка постійно розвивається, і вимагає пильності та уваги, а кіберзахист є надзвичайно важливою проблемою для підприємств критичної інфраструктури. Нині ці організації є основною мішенню для кіберзлочинців. Щоб здійснювати їх кіберзахист, необхідно запровадити надійні засоби контролю безпеки, політику та процедури, а також бути в курсі останніх загроз і вразливостей, важливим аспектом захисту об'єктів критичної інфраструктури є розвиток міжнародних стандартів і врахування передового досвіду. Керівники, урядовці повинні працювати разом над розробкою та впровадженням міжнародних стандартів і найкращих практик для захисту об'єктів критичної інфраструктури. Інтенсивні кібератаки на об'єкти критичної інфраструктури ворог почав ще до 24 лютого 2022 року, проте високий рівень кіберзахисту українського енергосектору не дозволив країні-агресору досягнути поставлених цілей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. З початку війни на енергосектор України було здійснено 1,2 млн кібератак: URL: https://lb.ua/society/2022/11/22/536658_z_pochatku_viyni_energosektor.html (Дата звернення 20.01.2023).
2. Ткачук Н.А. Організаційно-правові засади формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. *«Інформація та право»,* 2018. №1(24). С. 133-138.
3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.17 р. № 2163-19. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2163-19.

Радзіховський Дмитро Юрійович, студент, Вінницький національний технічний університет**,** факультет інформаційних технологій та комп'ютерної інженерії**,** м. Вінниця, dimaradvin@gmail.com

Науковий керівник: ***Шиян Анатолій Антонович***, кандидат фізико-математичних наук, доцент, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет**,** м. Вінниця.

Dmytro Yuriyovych Radzihovskyi, student, Vinnytsia National Technical University, faculty of information technologies and computer engineering, Vinnytsia.

Academic supervisor: ***Anatolii Shyian***, candidate of physical and mathematical sciences, associate professor, associate professor of the department of information systems management and security, Vinnytsia National Technical University, Vinnytsia.