щодо забезпечення інформаційної безпеки є особливо актуальними. Інформаційна війна, на думку американських експертів, належить до одного із новітніх факторів, що має комплексний та динамічний характер і здійснює все більш значущий вплив на інфраструктуру держави. Це по суті новий вид війни, а це, відповідно, потребує системних заходів на рівні державної політики:

– вдосконалення правового забезпечення інформаційної безпеки;

– актуалізації системи ліцензування організацій, які працюють з інформацією чи здійснюють її захист;

– розвиток систем і засобів контролю;

– підготовки кадрів у сфері захисту інформації, крім того, одним із найважливіших напрямів є розширення міжнародної співпраці, участь в міжнародних системах сертифікації.

Отож, швидше за все, питання інформаційної безпеки в майбутньому вирішуватиметься
в комплексі нових проблем, що лежать і в площині високих технологій, і в логіці всього світового розвитку.

1. Кодинець А. О. Інформація як об'єкт цивільно-правової охорони. Науковий вісник Ужгородського національного університету. 2016. Вип. 39. С. 59.

2. Кодинець А. О. Цивільно-правове регулювання зобов'язальних інформаційних відносин. К. : Алерта, 2016. 582 с.

3. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12/ed20101013.

4. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. URL: https:// ips.ligazakon.net/document/T030435?an=14.

УДК 342.95+004
DOI: 10.31733/17-03-2023-526-528

Володимир ПЯДИШЕВ
професор кафедри кібербезпеки
та інформаційного забезпечення
Одеського державного
університету внутрішніх справ,
доктор юридичних наук, професор

СУЧАСНІ АСПЕКТИ КІБЕРЗАХИСТУ КРИТИЧНИХ ІНФРАСТРУКТУР: ЗАРУБІЖНИЙ ДОСВІД

Можна без перебільшення стверджувати, що сьогодні увага світової спільноти прикута до подій в Україні, де тривають постійні атаки на критичні інфраструктури з боку російської федерації. Згідно зі звітом Microsoft про цифровий захист за 2022 рік, кібератаки, спрямовані на критичну інфраструктуру в усьому світі, становили до 40 % усіх атак на національні держави. Це сталося в основному через те, що російські хакери атакували українську інфраструктуру та союзників України у триваючій війні [1].

Сьогодні Україна стоїть на передовій лінії, і колись у всьому світі будуть ретельно вивчатися саме її передові практики щодо протистояння кібератакам на критичні інфраструктури. Але ми вважаємо, що наразі нам слід знати та ефективно впроваджувати увесь накопичений у світі досвід боротьби з кібератаками на критичні інфраструктури.

За даними Агентства з кібербезпеки та безпеки інфраструктури США [2], у державі розрізняють 16 секторів критичної інфраструктури:

– хімічний сектор;
– сектор комерційних об'єктів;
– сектор зв'язку;
– критичний виробничий сектор;
– сектор дамб;
– сектор оборонно-промислової бази;

- сектор екстрених служб;
- енергетичний сектор;
- сектор фінансових послуг;
- харчовий та сільськогосподарський сектор;
- сектор державних установ;
- сектор охорони здоров'я;
- сектор інформаційних технологій;
- сектор ядерних реакторів, матеріалів і відходів;
- сектор транспортних систем;
- сектор систем водопостачання та водовідведення.

Оскільки інформаційні технології все більше інтегруються в усі аспекти нашого суспільства, зростає ризик серйозних широкомасштабних подій, які можуть завдати шкоди або порушити послуги, від яких залежить економіка держави та повсякденне життя мільйонів американців [3].

За словами колишнього генерального директора Cisco Джона Чемберса, «є два типи компаній: ті, які були зламані, і ті, які ще не знають, що їх зламали» [4].

Незважаючи на безліч можливих точок входу та безліч типів експлойтів, які можна використовувати, більшість авторів поділяє найпоширеніші вектори кіберзагроз на три основні категорії [5]:

- Підключені системи управління процесами;
- Зовнішні підключення;
- Внутрішні загрози та викрадені облікові дані.

Фахівці з США висвітлюють п'ять напрямів, що роблять операційні технології вразливими:

Старіння технологій. Більшість систем ОТ було створено за роки до того, як кібербезпека стала проблемою. Більше того, за оцінками Microsoft, 71 % систем все ще працюють на застарілих системах, які не перевіряють нові вразливості чи нові загрози кібербезпеці.

Обмежена можливість виправлення. Оскільки критичні сектори інфраструктури та середовища промислових систем управління працюють цілодобово, тривалі періоди простою не є варіантом. Це надзвичайно ускладнює регулярне оновлення систем.

Слабкі паролі. Пристроям ОТ бракує надійної автентифікації та шифрування. У результаті досвідчені хакери можуть легко отримати доступ за допомогою грубої атаки.

Обмежені ресурси безпеки. 47 % організацій промислових систем управління не мають внутрішньої команди (групи), яка пропонувала б цілодобову підтримку під час інцидентів кібербезпеки.

Порт 5900 (порт, прийнятий за замовчуванням для ОВМ). З 9 липня по 9 серпня 2022 року на Порт 5900 спостерігався сплеск кібератак.

Більшість авторів вважає за найважливіші три практики для посилення кібербезпеки критичних інфраструктур [6]:

- Інтегрувати кібербезпеку зі штучним інтелектом і машинним навчанням;
- Збільшити видимість промислових мереж і їхнього ризику;
- Мати ретельно розроблений і добре відрепетований план реагування на кризу.

Більш детальний підхід дає вісім рекомендацій [7]:

- Тримайте критично важливі активи в середовищі інформаційних та операційних технологій за брандмауерам. Незалежно від того, чи потрібно вам надати легший доступ співробітникам чи партнерам, критичні активи повинні залишатися захищеними;
- Обмежте доступ до ОВМ через Інтернет. Якщо можливо, використовуйте стратегії сегментації для подальшої ізоляції критичної інфраструктури від виробничих мереж, ІТ-пристроїв і автоматизації офісу;
- Регулярно оновлюйте пристрої. Переконайтеся, що всі пристрої в середовищі промислових систем управління мають останні оновлення;
- Застосуйте політику надійних паролів. Усі в організації повинні дотримуватися обов'язкових параметрів для створення надійних складних паролів на всіх пристроях;
- Встановіть розширений контроль доступу. Завдяки двофакторній автентифікації та біометрії ви можете запровадити рольове управління ідентифікацією та доступом для всіх співробітників;
- Надайте пріоритет активам для реєстрації та моніторингу. Постійне ведення

журналів і аналіз мережевого трафіку допоможуть виявити аномалії та потенційні загрози на ранній стадії;

– Увімкніть усі необхідні заходи безпеки для ОВМ. Враховуючи чутливу природу мереж критичної інфраструктури, найкраще централізувати керування пристроями та шифрувати весь трафік і дані. Ви також можете встановити жорсткіші засоби контролю безпеки мережі в середовищі ОТ, включаючи пісочницю (організація процесів, при якій середовище тестування ізольоване від середовища виробництва) та брандмауери нового покоління;

– Надайте персоналу доступ до програм інформування та навчання з кібербезпеки. Ви можете культивувати сильнішу культуру безпеки, пропонуючи постійну освіту для співробітників, наприклад, зосереджуючись на політиці нульової довіри.

Важливість зазначених рекомендацій зростає у сучасних умовах, які характеризуються наступними чинниками. У минулому середовища ОТ рідко підключалися до Інтернету. Але коли цифровий світ перервав світ фізичний, уявні проміжки між ІТ і ОТ почали закриватися. Загроза операційним технологіям в системах комунального господарства зростає. Це підтверджує факт, що 80 % організацій ОТ та промислових систем управління мали інциденти за останній рік. Зрозуміло, що компанії повинні діяти, але перегляд найкращих практик і процесів у ОТ – це складний шлях уперед.

Сьогодні середня вартість витоку даних у Сполучених Штатах становить 9,44 мільйона доларів, що вдвічі перевищує середній світовий показник. Окрім фінансових витрат, коли стабільність країни знаходиться під загрозою, компанії повинні докладати більше зусиль для захисту критично важливих активів.

Однією з найбільших проблем із захистом середовищ критичної інфраструктури є поширене хибне уявлення про те, що мережі промислових систем управління відокремлені від традиційних ІТ-мереж надійним так званим «повітряним зазором». Однак у зв'язку з пандемією COVID-19, 65 % фахівців із безпеки IT/OT у США кажуть, що їхні ІТ- та ОТ-мережі тепер більш взаємопов'язані. Оскільки все більше ОТ з'являється в Інтернеті, зростає ймовірність кібератак, що просочуються через ІТ-середовища.

Згодом команди корпоративної безпеки повинні між інформацій ними та операційними технологіями знайти певний баланс, який захищатиме та оптимізуватиме обидва середовища. Наприклад, незважаючи на те, що засоби виявлення кінцевих точок і реагування добре підходять для ІТ-систем, вони громіздкі в ОТ. Кожне виявлення може бути виснаженням для ЦП, оскільки система надсилає дані в хмару.

1. Panez R. Analyzing major attacks in 2022: Lessons Learned from Critical Infrastructure Risks. Compuquip. January 18, 2023. URL: https://www.compuquip.com/blog/analyzing-major-attacks-in-2022-lessons-learned-from-critical-infrastructure-risks#:~:text=According%20to%20Microsoft's%202022%20Digital,allies%20in%20the%20ongoing%20war.

2. Cybersecurity Essentials for Critical Infrastructure. Dell. Technologies. Intel. URL: https://www.techtarget.com/searchsecurity/CyberResiliency/Cybersecurity-Essentials-for-Critical-Infrastructure.

3. Cybersecurity Best Practices. Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov/topics/cybersecurity-best-practices.

4. Ways to Prevent Cyberattacks on Critical Infrastructure. Unearth labs. URL: https://www.unearthlabs.com/blogs/cybersecurity-critical-infrastructure.

5. Coleman S. Five Cybersecurity Best Practices for Critical Infrastructure. Risk Management Magazine. March 2, 2023. URL: https://www.rmmagazine.com/articles/article/2023/03/02/five-cybersecurity-best-practices-for-critical-infrastructure.

6. Capdevielle E. Three Best Practices to Secure Critical Infrastructure. Nozomi Networks. September 6, 2018. URL: https://www.linkedin.com/pulse/three-best-practices-secure-critical-infrastructure-capdevielle.

7. Panez R. Analyzing major attacks in 2022: Lessons Learned from Critical Infrastructure Risks. Compuquip. January 18. 2023. URL: https://www.compuquip.com/blog/analyzing-major-attacks-in-2022-lessons-learned-from-critical-infrastructure-risks#:~:text=According%20to%20Microsoft's%202022%20Digital,allies%20in%20the%20ongoing%20war.