Державної прикордонної служби України. 2021. Вип. 3. С. 8–11.

3. Dobak I. Thoughts on the evolution of national security in cyberspace. *Security and Defence Quarterly.* 2021. № 33 (1). С. 75–85. URL : https://securityanddefence.pl/Thoughts-on-the-evolution-of-national-security-in-cyberspace,133154,0,2.html.

4. Holdsworth J., Kosinski M. What is information security? IBM. URL : https://www.ibm.com/think/topics/information-security.

Наталія ПРОТОПОПОВА
старший викладач кафедри
соціально-економічних дисциплін
Дніпровського державного
університету внутрішніх справ
(м. Дніпро, Україна)
https://orcid.org/0000-0002-0207-9301

ІНФОРМАЦІЙНА БЕЗПЕКА МАЛИХ ПІДПРИЄМСТВ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Інформаційна безпека є важливим аспектом діяльності будь-якого підприємства, особливо в умовах воєнного стану. Малі підприємства стають вразливими до кіберзагроз через обмежені ресурси та недостатню обізнаність у сфері кіберзахисту. В умовах війни в Україні зростає ризик кібератак, витоків конфіденційної інформації, фінансових шахрайств та інших загроз, що можуть паралізувати роботу бізнесу.

Основними загрозами інформаційній безпеці малих підприємств є:

1. Кібератаки – зловмисники можуть використовувати фішинг, віруси, шкідливе програмне забезпечення для доступу до корпоративних даних;
2. Соціальна інженерія – маніпулювання співробітниками для отримання важливої інформації або доступу до внутрішніх систем;
3. Витоки даних – ненавмисне або навмисне розголошення конфіденційної інформації через необережність персоналу чи недоліки в системах захисту;
4. Фізичні загрози – втрата або крадіжка носіїв інформації, руйнування серверів унаслідок бойових дій;
5. Несанкціонований доступ до хмарних сервісів – уразливість облікових записів у разі ненадійних паролів або недостатніх заходів безпеки;
6. Шахрайство та фінансові махінації – кібершахраї можуть створювати фальшиві рахунки та підробляти фінансові документи.

Основними методами забезпечення інформаційної безпеки можна визначити наступні:

1. Захист IT-інфраструктури:
   - використання оновлених антивірусних програм і брандмауерів;
   - регулярне оновлення програмного забезпечення та операційних систем;
   - налаштування багатофакторної автентифікації для всіх критичних систем;
2. Контроль доступу:
   - обмеження доступу співробітників до важливих даних;
   - використання VPN для захисту з'єднання під час віддаленої роботи;
   - створення резервних копій критично важливих даних;
3. Захист від соціальної інженерії:
   - навчання персоналу основам інформаційної безпеки та розпізнавання фішингових атак;
   - перевірка автентичності запитів, що стосуються фінансових операцій;
4. Захист фізичних носіїв інформації:
   - використання шифрування для захисту файлів і носіїв інформації;
   - організація безпечного зберігання паперових документів;
   - контроль над використанням особистих USB-носіїв у корпоративних мережах;
5. План дій у разі кіберінцидентів:
   - розробка алгоритму дій для відновлення роботи у разі кібератаки;
   - регулярне тестування систем безпеки та вразливостей;

– взаємодія з державними структурами кібербезпеки (наприклад, CERT-UA) для отримання актуальних рекомендацій.

В Україні діє низка ініціатив щодо підтримки бізнесу в сфері кібербезпеки:

1. Національний координаційний центр кібербезпеки при РНБО України;
2. Рекомендації Державної служби спеціального зв'язку та захисту інформації України;
3. Міжнародні програми підтримки кіберзахисту малого бізнесу.

Інформаційна безпека є критично важливою для збереження стабільності малих підприємств в умовах воєнного стану. Використання комплексного підходу до кіберзахисту, навчання персоналу, застосування сучасних технологій і дотримання рекомендацій державних структур допоможе підприємцям мінімізувати ризики та забезпечити безперебійну діяльність. Малі підприємства повинні усвідомлювати свою роль у загальній системі інформаційної безпеки та активно працювати над підвищенням рівня захисту своїх даних та активів.

Роман ШТОНДА
начальник науково-дослідного відділу
https://orcid.org/0000-0002-0207-9301
Ірина МАЛЬЦЕВА
старший науковий співробітник
Військового інституту телекомунікацій
та інформатизації імені Героїв Крут
(м. Київ, Україна)
https://orcid.org/0000-0001-6073-4637

ПІДХОДИ ЩОДО ПРОТИДІЇ ВИНИКНЕННЮ КІБЕРЗАГРОЗ В КРИТИЧНІЙ ІНФРАСТРУКТУРІ ДЕРЖАВИ

Інформаційна безпека та кібербезпека є невід'ємною складовою національної безпеки будь-якої держави. Потенційні кіберзагрози, що можуть виникнути на об'єктах критичної інфраструктури, несуть серйозні наслідки для всієї держави. Це пов'язане з тим, що будь-який об'єкт критичної інфраструктури залежить від інформаційних технологій [1].

Згідно із Річним аналітичним оглядом [2] глобальне протистояння в кіберпросторі набуває все більших обертів, залучаються нові учасники. Активність хакерів (далі – кіберзлочинці) в усьому світі зростає. З метою отримання інформації про зовнішньополітичні ініціативи та критичну інфраструктуру держав набуває широкого значення кібершпигунство. Відслідковується зростання тенденції кібервпливу на об'єкти критичної інфраструктури та особисті мобільні пристрої військовослужбовців і співробітників сектора безпеки. Кіберзлочинці в своїй діяльності активно використовують нові технології (штучний інтелект та машинне навчання) для розробки більш дієвих кібератак та кібероперацій, що дає можливість впливати на політичне, військове керівництво та критичну інфраструктуру держав.

Наслідки таких кібервпливів на критичну інфраструктуру держав можуть бути катастрофічними та призвести до:

– людських жертв – шляхом зламу електронних комунікаційних мереж, транспортних та медичних інформаційно-комунікаційних систем, інформаційно-комунікаційних систем енергетичних об'єктів тощо;

– виникнення паніки та соціальної напруги – шляхом обмеження електропостачання, збоїв в наданні послуг операторами Інтернет та зв'язку, відключення банківських систем;

– економічних втрат – шляхом завдання мільярдних збитків через втрати даних, зупинку підприємств, що належать до критичної інфраструктури, а також з огляду на необхідність відновлення критичної інфраструктури після цих кібервпливів;

– політичних наслідків, які спроможні будуть підірвати довіру до влади атакованих держав та дестабілізувати міжнародні відносини.

Для зменшення ризиків виникнення кібервпливів на критичну інфраструктуру слід