9. Закон України «Про телекомунікації». URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text
10. Закон України «Про електронні документи та електронний документообіг». URL: https://zakon.rada.gov.ua/laws/show/851-15#Text
11. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
12. Закон України «Про електронну ідентифікацію та електронні довірчі послуги». URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text
13. Указ Президента «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні». URL: https://zakon.rada.gov.ua/laws/show/928/2000#Text

DOI https://doi.org/10.36059/978-966-397-444-6-58

Омецинська Н. В.,
кандидат технічних наук, доцент,
завідувачка кафедри інженерних систем та технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

Дроменко В. Б.,
кандидат технічних наук, доцент,
доцент кафедри інженерних систем та технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

КІБЕРЗАХИСТ В ІНФОРМАЦІЙНИХ СИСТЕМАХ: ПРИНЦИПИ ТА ПІДХОДИ

Від початку військових дій, які розпочалися після 2014 року, і значно загострилися з повномасштабним вторгненням Росії в 2022 році Україна зіткнулася з безпрецедентною хвилею кібератак. Кібератаки стали невід'ємною частиною російської агресії, націленої на критичні інфраструктури: енергетичний сектор, телекомунікації, банківську систему, державні сайти та сервіси.

Основними загрозами кібербезпеки під час війни стають: *кібератаки на критичну інфраструктуру*, які можуть виводити з ладу електромережі, телекомунікаційні системи або банківські сервіси, що паралізує економіку та управління державою; *фішингові атаки*, коли противник використовує кампанії для отримання доступу до

персональних даних українських громадян, військових та державних службовців; *злам інформаційних систем*, при яких російські хакери постійно намагаються отримати доступ до секретної інформації, зламують урядові сервіси для дестабілізації управління країною.

Наведемо ключові приклади кібератак за цей період:

1. Атака на енергетичну інфраструктуру (грудень 2015 року). Хакери атакували електричні компанії, що призвело до масштабного відключення електрики у Західній Україні. Було знеструмлено близько 230 тисяч споживачів на кілька годин. Атака була здійснена через злам SCADA-систем, що керують енергетичною мережею. Ця атака стала першим задокументованим випадком, коли кібератака спричинила відключення енергосистеми.

2. Кібератака NotPetya (червень 2017 року). Атака була спрямована на українські компанії, державні установи, банки, транспортні системи та енергетичні підприємства, але незабаром вірус поширився по всьому світу, завдавши збитків на мільярди доларів. NotPetya атакував системи через українське бухгалтерське програмне забезпечення M.E.Doc і, хоча виглядав як програмне забезпечення для шифрування даних з метою викупу, його основною метою було знищення даних. Атаку пов'язують із російськими хакерами.

3. Атака на державні вебсайти та банківські системи (лютий 2022 року). За кілька днів до початку повномасштабного вторгнення Україна зіткнулася з серією потужних кібератак на урядові вебсайти та фінансові інституції. В результаті атаки були тимчасово виведені з ладу вебсайти Міністерства оборони, Збройних сил України та деяких великих банків, таких як ПриватБанк і Ощадбанк. Атака була реалізована через метод DDoS (розподілена атака на відмову в обслуговуванні), яка переповнювала сервери і тимчасово виводила їх з ладу.

4. Кібератака на Viasat (лютий 2022 року). Хакери атакували європейський супутниковий інтернет-сервіс Viasat, який забезпечував зв'язок для військових та цивільних користувачів в Україні. Атака вивела з ладу тисячі супутникових модемів, які використовувалися для забезпечення зв'язку на місцях бойових дій, а також у цивільному секторі. Вважається, що метою цієї атаки було порушення комунікацій в перші години війни.

5. Кібератака на українські медіа та телеканали (липень 2022 року). В результаті атаки в ефірі каналу Україна 24 було показано фальшиве звернення президента України Володимира Зеленського, в якому він нібито закликав українців здатися. Ця інформаційна атака мала на меті деморалізувати українське населення, але була швидко викрита як фейк.

6. Кібератака на українські урядові структури (січень 2022 року). Було атаковано офіційні сайти Міністерства закордонних справ, Кабінету Міністрів, Міністерства освіти і науки та інші. На деяких

з них з'явилися погрозливі повідомлення з вимогою «боятися і чекати найгіршого». Експерти відзначили, що ця атака, ймовірно, була підготовкою до початку військової агресії.

7. Атаки на поштові сервіси (2023 рік). Хакери намагалися виманити облікові дані українських урядовців і військових через підроблені електронні листи, маскуючи їх під офіційну кореспонденцію. Це було частиною стратегії збору розвідувальної інформації.

Інформаційні системи можуть бути піддані різним видам атак, кожна з яких має свої особливості і потребує окремих підходів до захисту:

1. Зловмисне програмне забезпечення (шкідливе ПЗ): Віруси, трояни, шпигунське ПЗ та інші типи шкідливого програмного забезпечення, які можуть красти або знищувати дані, поширюватися через мережу або використовувати ресурси системи для здійснення подальших атак.

2. Фішинг: Атаки, спрямовані на викрадення персональних даних користувачів шляхом обману (наприклад, через підроблені електронні листи чи вебсайти).

3. DDoS-атаки: Розподілені атаки на відмову в обслуговуванні, метою яких є перевантаження системи запитами з багатьох джерел, що робить її недоступною для користувачів.

4. Атаки зловмисників зсередини: Це загрози, які походять від співробітників або інших людей, що мають доступ до інформаційних систем, і можуть навмисно чи ненавмисно порушувати безпеку даних.

5. Експлойти уразливостей: Використання вразливих місць у програмному забезпеченні або мережевих протоколах для несанкціонованого доступу до систем.

Для захисту інформаційних систем від вищезазначених загроз використовуються різноманітні технології та методи кібербезпеки. Впровадження технічних рішень дозволять зміцнити кіберзахист в інформаційних системах:

1. Мережева безпека:

– Фаєрволи: Встановлення між мережею підприємства і зовнішнім світом для фільтрації трафіку та блокування несанкціонованих доступів.

– Віртуальні приватні мережі (VPN): Забезпечують безпечний доступ до мережі через зашифровані канали, що особливо важливо для віддалених співробітників.

2. Шифрування даних:

– Шифрування на рівні зберігання: Захист даних під час зберігання на серверах або у хмарних сховищах.

– Шифрування під час передачі: Захист даних під час передачі через мережу за допомогою таких протоколів, як TLS (Transport Layer Security).

3. Система виявлення та запобігання вторгнень (IDS/IPS):

– IDS/IPS системи використовуються для виявлення підозрілої активності в мережі та автоматичного блокування потенційних загроз. Вони допомагають у швидкому виявленні атак та зменшують ризик їх розвитку.

4. Багатофакторна аутентифікація (MFA):

– Використання декількох факторів перевірки при доступі до систем, таких як комбінація пароля та одноразового коду або біометрії, значно підвищує безпеку.

5. Антивірусні програми та засоби захисту від шкідливого ПЗ:

– Використання сучасного антивірусного програмного забезпечення, яке забезпечує захист від шкідливого програмного забезпечення, вчасно оновлюється і може запобігти зараженню системи.

6. Резервне копіювання даних:

– Регулярне створення резервних копій даних для забезпечення їх відновлення у випадку кібератаки або інших інцидентів, таких як відмова обладнання.

Кіберзахист в інформаційних системах – це багаторівневий процес, який вимагає комплексного підходу з використанням як технічних рішень, так і організаційних заходів. Сучасні загрози постійно змінюються, тому інформаційні системи повинні бути гнучкими, здатними до адаптації та швидкого реагування на нові виклики. Забезпечення конфіденційності, цілісності та доступності інформації є ключовими елементами кібербезпеки, і тільки системний підхід до її реалізації може ефективно захистити критичні активи від кіберзагроз.

Список використаних джерел:

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. / Інформаційна та кібербезпека: соціотехнічний аспект : [підручник]. Б 91 / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С. В. Толюпа. Львів : «Магнолія 2006», 2024. 320 с.

2. Кібербезпека бізнесу під час війни. Мінфін. URL: https://www.project.minfin.com.ua/kiberbezpekabiznesu-pid-chas-vijny

3. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам (2024). Європейська Бізнес-асоціація. URL: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannyaatakam/

4. Жарикова А. Держспецзв'язку. Економічна правда. URL: https://www.epravda.com.ua/news/2024/01/31/709355/