Клименко Софія Павлівна
Студентка н.гр. 105_СПД ННІ права та психології НАВС

Науковий керівник:
Хахановський Валерій Георгійович
доктор юридичних наук, професор, професор кафедри інформаційних технологій ННІ права та психології НАВС

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В СУЧАСНИХ УМОВАХ

Сучасний світ дедалі більше залежить від цифрових технологій: нині всі працюють, навчаються, спілкуються та навіть зберігають власні гроші в електронному просторі. Разом із новими можливостями зростає й кількість ризиків, пов'язаних із кіберпростором. Кібератаки вже не є лише технічною проблемою – вони перетворилися на глобальний виклик, що впливає на економіку, політику та національну безпеку. Саме тому дослідження проблем кібербезпеки набуває особливого значення у XXI столітті.

Загальні тенденції впровадження цифрових технологій:

– цифровізація суспільства призводить до збільшення кількості пристроїв, що підключені до мережі, а отже – й точок потенційної атаки;

– зростання обсягів персональних даних робить користувачів більш вразливими до крадіжок інформації;

– гібридні війни активно використовують кіберінструменти як засіб впливу на супротивника.

Основними сучасними викликами кібербезпеки є:

1. Кіберзлочинність (хакерські атаки на банківські системи, крадіжка коштів і даних; використання шкідливого програмного забезпечення (вірусів, троянів, програм-вимагачів)).
2. Кібертероризм і кібервійни (атаки на критичну інфраструктуру: енергетичні системи, транспорт, медицину; використання кіберзасобів у збройних конфліктах, як це спостерігається нині під час агресії проти України).
3. Соціальна інженерія (фішинг; маніпуляції довірою користувачів, щоб отримати доступ до конфіденційної інформації).
4. Загрози для приватності (масове збирання й використання персональних даних великими корпораціями; проблеми захисту інформації у соціальних мережах).

5. Штучний інтелект та нові технології – з одного боку вони допомагають захищати дані, з іншого – створюють нові ризики (наприклад, deepfake, автоматизовані атаки).

В умовах війни Україна постійно зазнає масштабних кібератак з боку росії, метою яких є паралізація роботи державних органів, дезінформація, створення паніки серед населення. Це доводить, що кіберпростір став окремим фронтом сучасної війни.

Основні тренди кібербезпеки у 2025 році:

1. Штучний інтелект у захисті (використання AI для виявлення та блокування загроз у реальному часі; прогнозування потенційних атак за допомогою аналітики даних).

2. Мережна сегментація (розділення мережі на сегменти для мінімізації ризику поширення загроз; підвищення контролю над доступом до критичних систем).

3. Багатофакторна аутентифікація (активне впровадження додаткових рівнів безпеки; захист доступу до корпоративних систем і особистих даних).

4. Кібербезпека в хмарних середовищах (посилення захисту даних у хмарних платформах; використання спеціалізованих інструментів для моніторингу та захисту).

5. Навчання співробітників (підвищення рівня обізнаності працівників про сучасні загрози; регулярні тренінги для зменшення ризику людського фактору).

Сьогодні більшість речей навколо нас працює завдяки складним системам (електростанції, лікарні, транспорт, банки, водопостачання, зв'язок та Інтернет тощо). Усі ці об'єкти утворюють так звану критичну інфраструктуру. Якщо хоча б одна з цих систем перестане працювати, це може спричинити значні проблеми: зупиниться транспорт, зникне електроенергія, не буде доступу до грошей, може постраждати здоров'я людей. Через це питання захисту критичної інфраструктури стає одним із найважливіших у сучасному світі. З розвитком технологій з'являються і нові небезпеки: хакери можуть зламати комп'ютерні мережі, правопорушники – пошкодити обладнання, стихійні лиха – знищити важливі об'єкти. Завдання держави, бізнесу та суспільства – не допустити таких ситуацій або швидко реагувати, якщо вони трапляються.

Критична інфраструктура – це найважливіші системи та об'єкти, без яких не може нормально існувати суспільство й держава. Вона забезпечує життя людей, роботу економіки та безпеку країни. До неї належать:

- Енергетика – електростанції, газо- та нафтопроводи, теплопостачання.
- Транспорт – залізниці, метро, морські порти, авіаційні системи.
- Зв'язок і Інтернет – мобільні мережі, супутникові системи, пошта.
- Охорона здоров'я – лікарні, лабораторії, системи швидкої допомоги.
- Фінанси – банки, банкомати, системи оплати.
- Безпека держави – військові об'єкти, поліція тощо.

Якщо одна з цих сфер буде пошкоджена або знищена, це може спричинити серйозні наслідки для життя всієї країни.

Загроз для об'єктів критичної інфраструктури багато. Найпоширеніші з них:

• Кібератаки. Злочинці можуть зламати комп'ютерні мережі та паралізувати роботу електростанцій, банків чи транспорту.

• Фізичні напади. Терористи або зловмисники можуть пошкодити об'єкти інфраструктури.

• Технічні аварії. Іноді системи виходять з ладу через несправність або людську помилку.

• Природні катастрофи. Повені, землетруси, пожежі можуть знищити важливі об'єкти.

• Військові дії. Під час війни такі об'єкти стають однією з головних цілей ворога.

Відомі приклади атак на критичну інфраструктуру:

✓ Україна, 2015 рік. Кібератака на енергетичну систему призвела до відключення електроенергії в кількох регіонах країни.

✓ США, 2021 рік. Злочинці зламали систему нафтопроводу «Colonial Pipeline», через що постачання палива на східному узбережжі було зупинене на кілька днів.

✓ Україна, 2022 рік. Під час війни росія неодноразово атакувала енергетичні підприємства та Інтернет-мережі, намагаючись порушити роботу критичних систем.

Ці приклади доводять, що загроза реальна і може торкнутися кожної людини.

Захист таких об'єктів складається з багатьох заходів:

o Постійний нагляд і моніторинг. Фахівці відстежують роботу систем, щоб одразу помітити небезпеку.

o Резервні системи. Створюються запасні джерела енергії, копії даних та інші механізми на випадок аварій.

o Навчання персоналу. Людей навчають діяти в кризових ситуаціях та правильно реагувати на загрози.

o Законодавчий захист. Приймаються закони, які визначають правила безпеки та покарання за злочини проти критичних об'єктів.

o Міжнародна співпраця. Держави обмінюються досвідом і допомагають одна одній захищати важливі системи.

В Україні для цього діє Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони. Він координує роботу державних органів, приватних компаній і міжнародних партнерів.

Отже, критична інфраструктура – це серце сучасної держави. Без електрики, води, транспорту, зв'язку та лікарень життя людей зупинилося б. Тому її захист – це не просто технічне питання, а гарантія безпеки кожного громадянина.

Список використаних джерел:

1. Міністерство цифрової трансформації України. Офіційний сайт. – https://thedigital.gov.ua
2. Кіберполіція України. Аналітичні матеріали та новини. – https://cyberpolice.gov.ua
3. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Reports. – https://ccdcoe.org
4. Symantec. Internet Security Threat Report. – https://symantec.com
5. FireEye Mandiant. Cyber Security Reports. – https://www.mandiant.com
6. CERT-UA (Computer Emergency Response Team of Ukraine). Офіційні публікації. – https://cert.gov.ua
7. Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.).
8. Офіційний сайт Ради національної безпеки і оборони України – www.rnbo.gov.ua.
9. ENISA. Reports on Critical Infrastructure Protection.
10. Symantec. Internet Security Threat Report.
11. Zetter K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* – 2014.

Стрельцова Кіра Юріївна
Студентка н.гр. 105_СПД ННІ права та психології НАВС

Науковий керівник:
Хахановський Валерій Георгійович
доктор юридичних наук, професор, професор кафедри інформаційних технологій ННІ права та психології НАВС

КІБЕРБЕЗПЕКА БІЗНЕСУ: ВІД МАЛОГО ДО ВЕЛИКОГО

Сьогодні кібербезпека стала однією з ключових умов стабільності бізнесу незалежно від його масштабу. Малі, середні та великі підприємства дедалі частіше стають мішенню кіберзлочинців, адже дані, ресурси та фінансові активи є об'єктом особливої цінності.

Мета даної роботи – розглянути виклики та підходи до забезпечення кібербезпеки бізнесу на різних рівнях його розвитку.