Червинська Ксенія Олегівна
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

СУЧАСНІ ВИКЛИКИ В СФЕРІ КІБЕРБЕЗПЕКИ

Кіберпростір сьогодні – це середовище, де взаємодіють мільярди пристроїв, а обсяги інформації подвоюються щороку. Разом з цим зростає і кількість кіберзагроз. Якщо на початку 2000-х більшість атак мали аматорський характер, то сьогодні вони організовуються цілими хакерськими угрупованнями, фінансуються державами чи кримінальними синдикатами. Це робить кібербезпеку глобальним викликом XXI століття.

Кібербезпека – це система організаційних, технічних і правових заходів, спрямованих на захист інформаційних систем від несанкціонованого доступу, знищення, блокування чи викривлення даних.

Значення кібербезпеки зростає через: 1) цифровізацію державного управління (електронні сервіси, «Дія», електронні документи); 2) онлайн-банкінг і фінансові операції, де витік інформації може призвести до мільйонних збитків; 3) зростання кількості електронних пристроїв (смартфони, «розумні» годинники, IoT-пристрої); 4) кібервійни, що стають елементом міжнародних конфліктів.

Кіберпростір перетворився на арену геополітичної боротьби. Хакерські атаки можуть паралізувати роботу електростанцій, транспортних мереж чи банківських систем. Прикладом є масові атаки на Україну в 2015–2017 роках, що призводили до відключення електроенергії та блокування державних ресурсів.

Кібершпигунство дозволяє державам та корпораціям отримувати конфіденційні дані конкурентів, впливати на політику інших країн та здійснювати маніпуляції в інформаційному просторі.

Кіберзлочини проти приватних осіб. Найбільш поширені форми:

- фішинг – виманювання особистих даних через підроблені сайти та повідомлення;
- віруси та шкідливе програмне забезпечення, які блокують роботу комп’ютерів чи викрадають інформацію;
- шантаж (ransomware) – блокування пристрою з вимогою викупу;
- крадіжка даних банківських карток (завдає мільярдні збитки щороку).

Виклики інтернету речей. Мільярди «розумних» пристроїв (камери, датчики, побутова техніка) часто не мають достатнього захисту. Хакери можуть використати їх як «точку входу» для масштабних атак. Наприклад, заражені «розумні» телевізори чи маршрутизатори об'єднують у «ботнети», які паралізують роботу великих сайтів.

Соціальна інженерія. Сучасні атаки дедалі частіше спрямовані не на комп'ютери, а на людей. Хакери створюють психологічні маніпуляції: дзвінки від «працівників банку», підроблені електронні листи, повідомлення від «знайомих» у соцмережах. Людина сама передає зловмиснику потрібну інформацію.

Штучний інтелект як виклик і можливість. З одного боку, AI дозволяє швидше виявляти аномалії та підозрілі дії. З іншого – зловмисники застосовують його для створення реалістичних фейкових відео, автоматизації атак чи масового фішингу.

Дефіцит кваліфікованих кадрів. За даними міжнародних організацій, у світі не вистачає понад 3 мільйонів фахівців із кіберзахисту. Це означає, що навіть великі компанії залишаються без належного рівня безпеки.

***Шляхи протидії кіберзагрозам*:**

1. *Розвиток національних стратегій кібербезпеки*. Україна вже ухвалила відповідні документи, але їх необхідно постійно оновлювати відповідно до нових викликів.
2. *Використання сучасних технологій*. Багаторівнева аутентифікація, шифрування, системи виявлення вторгнень, аналіз великих даних.
3. *Міжнародне співробітництво*. Кіберзагрози не мають кордонів, тому боротьба з ними вимагає спільних дій. Приклад – Будапештська конвенція про кіберзлочинність.
4. *Освіта та підготовка кадрів*. Важливо створювати програми навчання з кіберзахисту в школах і закладах вищої освіти.
5. *Цифрова грамотність населення*. Користувачі мають знати основи безпеки: не відкривати підозрілі листи, не повідомляти паролі, перевіряти сайти.

Отже, кібербезпека стала однією з найважливіших сфер у житті сучасного суспільства. Від неї залежить стабільність економіки, національна безпека, особиста безпека кожної людини.

Сучасні виклики – кібервійни, кіберзлочинність, розвиток інтернету речей, використання штучного інтелекту – потребують комплексної відповіді. Подолати їх можливо лише за умови поєднання новітніх технологій, ефективного законодавства, міжнародної співпраці та підвищення цифрової культури суспільства.

На мою думку, кібербезпека – це не лише завдання держави чи IT-компаній, а спільна справа кожного громадянина, адже найчастіше саме людський фактор є ключовим у питаннях захисту інформації.