Кононіченко Ірина Олександрівна
Студентка н.гр. 205_СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

КІБЕРБЕЗПЕКА ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

У сучасних умовах розвитку інформаційного суспільства та цифровізації державного управління питання кібербезпеки набуває особливого значення. Державні інформаційні системи зберігають величезні обсяги важливої інформації — персональні дані громадян, інформацію про національну безпеку, діяльність органів влади, критичну інфраструктуру тощо. Будь-яке порушення безпеки цих систем може мати серйозні наслідки для держави й громадян. Тому кібербезпека державних інформаційних систем є однією з ключових складових національної безпеки України.

Кібербезпека – це стан захищеності кіберпростору, при якому забезпечується стійке функціонування інформаційних систем, запобігається несанкціонований доступ, втручання, пошкодження або знищення інформації. Державна інформаційна система — це система, що створена державним органом для автоматизованої обробки інформації, яка використовується для виконання ним повноважень.

Основні нормативно-правові акти, які регулюють сферу кібербезпеки в Україні:

- Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII;
- Закон України «Про інформацію»;
- Постанова КМУ № 518 «Про затвердження Порядку функціонування державної системи кіберзахисту»;
- Національна стратегія кібербезпеки України (Указ Президента № 47/2021 від 26.03.2021).

Кіберпростір — це середовище, яке виникає в результаті взаємодії людей, програм, даних і цифрових пристроїв через глобальні мережі. Кібербезпека охоплює технічні, організаційні та правові заходи, спрямовані на захист цифрового середовища.

Особливістю законодавства України є врахування міжнародних стандартів у сфері кібербезпеки, зокрема документів Європейського Союзу, стандартів ISO/IEC 27001, 27032

Загрози кібербезпеці державних інформаційних систем

Основні загрози:

- кібератаки з боку хакерських угруповань (у т.ч. державних);
- розповсюдження шкідливого програмного забезпечення (віруси, трояни);
- несанкціонований доступ до інформаційних ресурсів;
- внутрішні порушення (недбалість персоналу, помилки адміністраторів);
- фішингові атаки та соціальна інженерія.

Загрози кібербезпеці

Крім вірусу Petya, прикладом масштабної загрози є атака BlackEnergy (2015 рік), яка спричинила збої в енергетичних системах України.

Серед сучасних загроз — використання бот-мереж (botnets), DDoS-атаки, криптографічні атаки, порушення в системах автентифікації. Фішингові атаки стають дедалі витонченішими, використовують елементи штучного інтелекту для імітації офіційних ресурсів держави.

Система забезпечення кібербезпеки в Україні

Головні суб'єкти забезпечення кібербезпеки:

- Рада національної безпеки і оборони України;
- Державна служба спеціального зв'язку та захисту інформації;
- Служба безпеки України;
- Національний координаційний центр кібербезпеки;
- Кіберполіція.

Також діє державна система кіберзахисту, яка включає систему моніторингу, виявлення, запобігання та реагування на кіберінциденти. Державні органи зобов’язані впроваджувати політики інформаційної безпеки, проводити аудит, навчання персоналу та технічне зміцнення інфраструктури.

Система забезпечення кібербезпеки

Національний координаційний центр кібербезпеки (НКЦК) при РНБО здійснює стратегічне управління. Він координує обмін інформацією між суб’єктами кібербезпеки, розробляє сценарії реагування. Держспецзв’язку виконує функції технічного захисту інформації та сертифікації. СБУ через департамент кібербезпеки виконує контррозвідувальні та захисні функції. Також розвиваються центри реагування на комп’ютерні інциденти (CERT-UA).

Перспективи та виклики

В умовах війни з Російською Федерацією Україна стала однією з головних цілей кібератак. Це вимагає зміцнення національного кіберзахисту, розвитку власного програмного забезпечення, підготовки фахівців з кібербезпеки. Також актуальним є розширення міжнародного співробітництва з ЄС, НАТО, США та іншими партнерами.

Перспективи

У майбутньому необхідно:

- посилити нормативно-правову базу щодо відповідальності за кіберзлочини;
- розширити мережу кіберполіції та забезпечити її ресурсами;
- впровадити обов'язкову сертифікацію критичних інформаційних систем;
- проводити загальнонаціональні навчання з кіберзахисту;
- інтегруватися в європейський кіберпростір та долучатись до колективних систем захисту (як-от платформа ЄС по реагуванню на кіберінциденти).

Висновки:

Кібербезпека державних інформаційних систем є критично важливою складовою національної безпеки. Надійний захист інформації, впровадження новітніх технологій, навчання персоналу та координація дій між державними структурами – запорука безпеки цифрової держави.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 року № 2163-VIII.
2. Про Стратегію кібербезпеки України: Указ Президента від від 14.05.2021 року № 447/2021.
3. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова КМУ від 19.06.2019 № 518.
4. Матеріали Національного координаційного центру кібербезпеки URL: https://ncscc.gov.ua