Домашенко Аліна Олександрівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Козачина А. М., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор філософії

ФОРМУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННИХ ЗАГРОЗ: ВИКЛИКИ, МІЖНАРОДНИЙ ДОСВІД ТА ШЛЯХИ ВДОСКОНАЛЕННЯ

Сучасний світ дедалі більше залежить від цифрових технологій, інтернету та інформаційних систем. Майже кожна сфера життя – від спілкування до банківських операцій – пов'язана з використанням мережевих сервісів. Однак разом із розвитком технологій зростає і рівень кіберзагроз. Сьогодні кіберзлочини охоплюють не лише приватних користувачів, а й великі компанії та державні установи [1, с. 12].

В умовах війни проти України питання кібербезпеки набуло особливого значення. Кібератаки стали складовою гібридної війни – вони спрямовані на порушення роботи державних установ, об'єктів критичної інфраструктури, інформаційних систем та фінансових установ [2]. Ефективна кібербезпека має бути побудована не лише на рівні держави, а й на рівні кожного громадянина та організації.

У літературі зазначається, що сучасні кіберзагрози, з якими стикається Україна, умовно можна розділити на чотири основні категорії:

1. Деструктивні атаки, зміст яких передбачає використання програм-руйнівників (wiper), як-от HermeticWiper, WhisperGate, які були зафіксовані в перші дні повномасштабного вторгнення. Метою цих атак є виведення з ладу систем управління, баз даних та пошкодження об'єктів критичної інфраструктури.

2. Фішингові атаки, значна частина яких реалізується через соціальну інженерію – від імені державних органів розповсюджуються фішингові листи, підроблені застосунки (наприклад, фейкові «Дія») з метою збору персональних даних або проникнення в інформаційні системи.

3. Кібершпигунство (тривале проникнення у комп'ютерні мережі з метою збору розвідданих, ураження комунікаційних систем або підготовки до фізичних атак) під час якого, зокрема, використовуються RAT-інструменти, модулі screen-capture, кейлогери.

4. Інформаційно-психологічні операції: дезінформація, поширення фейкових повідомлень, deepfake-відео, маніпуляція громадською думкою через Telegram-канали, Інтернет та соціальні мережі. Ці операції спрямовані, у першу чергу, на посилення напруги у суспільстві, дискредитацію державної влади України [3, с. 133].

Отже, ключові загрози інформаційній безпеці України мають комплексний характер і стосуються як технічної сфери, так і соціально-політичних процесів. Кіберзлочинність, поширення дезінформації, інформаційне шпигунство, а також прогалини в правовому регулюванні інформаційного простору зумовлюють потребу в цілісній державній політиці захисту національної інформаційної безпеки.

Європейські країни приділяють увагу навчанню населення основам цифрової безпеки. Наприклад, у багатьох країнах ЄС проводяться загальнонаціональні інформаційні кампанії та тренінги, які навчають громадян розпізнавати загрози в інтернеті [4]. Це формує культуру безпечної поведінки в цифровому середовищі, що є першою лінією оборони від кіберзлочинців.

У сучасній практиці все більше компаній переходять до концепції Zero Trust – «нульової довіри». Це означає, що кожна дія користувача або пристрою в мережі проходить перевірку, а доступ надається лише за принципом «необхідного мінімуму». Такий підхід зменшує можливість зламу навіть у випадку, якщо обліковий запис зловмисник отримає [4].

Досвід показує, що кібербезпека ефективна лише тоді, коли охоплює як технічні, так і організаційні заходи. Це підтверджується й дослідженнями українських фахівців, які вказують на важливість підготовки персоналу та внутрішніх інструкцій із кіберзахисту [1, с. 35].

Національний рівень кібербезпеки визначає здатність держави протидіяти масштабним атакам, захищати критичну інфраструктуру та забезпечувати стабільність інформаційного простору. Європейський Союз активно розвиває спільну політику у сфері кібербезпеки. У 2022 році була ухвалена NIS2 Directive, яка встановлює обов'язкові вимоги до кіберзахисту для енергетичного, транспортного, медичного, фінансового та інших важливих секторів [6].

Важливу роль у розробці стандартів і рекомендацій відіграє European Union Agency for Cybersecurity (ENISA). Це агентство аналізує кіберзагрози, публікує аналітичні звіти та допомагає державам координувати свої дії [4].

Хорошим прикладом ефективної кіберполітики є Естонія. Після масованої кібератаки у 2007 році країна створила розвинену систему кіберзахисту, у тому числі національний кіберцентр, систему резервного копіювання та проведення регулярних тренувань. Завдяки цьому Естонія вважається однією з найбільш захищених у цифровому просторі держав [6].

Зростаюча актуальність кіберсфери в міжнародних відносинах спонукала дедалі більше урядів інтегрувати оборонну стратегію в кібербезпеці та напад. Італія зробила значний крок, наслідуючи тенденцію НАТО. Завдяки італійському законодавству, Збройні сили зможуть наймати приватних хакерів та спеціалістів для проведення наступальних та оборонних цифрових операцій. Цей крок визнає, що сучасна війна — це не лише ракети чи дрони, а й контроль над критичною інфраструктурою та громадською думкою. До недавніх часів італійська кібербезпека переважно контролювалася Національним агентством кібербезпеки, але наразі Міністерство оборони має можливість діяти автономно навіть у мирний час, зосереджуючись на основній меті – захисті установ та громадян, зміцнення національного щита від атак на межі війни та проведення наступальних дій проти ворожих суб'єктів, якщо це необхідно. Адже кібервійна зараз є опорою сучасної геополітики.

В Україні також активно розвивається система національної кібербезпеки. Важливу роль відіграє Державна служба спеціального зв'язку та захисту інформації України, яка координує заходи з кіберзахисту, проводить спільні навчання з партнерами та забезпечує кібероборону державних інформаційних систем [7].

Центри (підрозділи) забезпечення кібербезпеки або кіберзахисту створено також у Службі безпеки України (СБУ), Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України та Збройних Силах України.

Активно розвивається співпраця у сфері кібербезпеки із зарубіжними партнерами (Сполучені Штати Америки, Сполучене Королівство Великої Британії та Північної Ірландії, Федеративна Республіка Німеччина, Королівство Нідерландів, Японія тощо), поглиблюється співпраця з ЄС та НАТО, проводиться кіберпідготовка за участю інших держав та міжнародних організацій.

Тож, розвиток системи кібербезпеки України здійснюється на основі досвіду побудови національної системи кібербезпеки; аналізу сильних та слабких сторін моделей кібербезпеки інших країн; практики організації роботи в цій сфері та взаємодії з іншими суб'єктами кібербезпеки. Заходи та засоби кіберзахисту спрямовані на оперативне реагування на кібератаки та інші кіберінциденти, та впровадження контрзаходів, спрямованих на мінімізацію вразливості систем зв'язку. У цьому контексті, на нашу думку, важливо не обмежуватися впровадженням лише сучасних технічних рішень, а й удосконалювати правові інструменти, зміцнювати міжнародну взаємодію та формувати належний рівень медіаграмотності громадян.

Кібербезпека – складна система, яка включає індивідуальні дії, організаційні заходи та державну політику. Це спільна відповідальність урядів, компаній та громадян. Без належної уваги до кожного з цих рівнів неможливо забезпечити надійний захист від сучасних кіберзагроз. Посилення безпеки інформації та мереж є основоположним для забезпечення захисту даних та стійкості до кіберзагроз. Досвід країн Європи свідчить, що лише спільна відповідальність громадян, бізнесу та держави дає реальні результати у боротьбі з кібератаками [5; 6]. Україна вже робить важливі кроки у цьому напрямку, але подальший розвиток кіберзахисту потребує інвестицій у освіту, кадри та міжнародну співпрацю.

З метою вирішення проблемних питань, пропозиціями щодо покращення може стати:

1. Розробка національної програми з кіберосвіти, яка охоплюватиме школярів, студентів та працівників державного сектору.
2. Посилення вимог до організацій щодо впровадження політик кібербезпеки та навчання персоналу.
3. Розвиток міжнародної співпраці з ЄС у сфері обміну досвідом та інформацією про кіберзагрози.
4. Кадровий та технологічний розвиток: збільшення кількості фахівців шляхом створення державних освітніх програм і стипендій у сфері кібербезпеки.
5. Проведення національних тренувань з кіберзахисту, які об'єднуватимуть державні органи, бізнес і громадські організації, підвищення обізнаності про важливість кібербезпеки.

Список використаних джерел

1. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко та ін.; за заг. ред. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.
2. Матеріали з офіційного сайту Служба безпеки України. URL: https://ssu.gov.ua
3. Горун О. Ю. Кіберзагрози України в умовах агресії РФ. *Інформація і право*. 2025. № 3 (54). С. 131–138. URL: http://il.ippi.org.ua/article/view/340520
4. ENISA. Cybersecurity Education and Awareness. URL: https://www.enisa.europa.eu
5. Directive (EU) 2022/2555 (NIS2 Directive). URL: https://eur-lex.europa.eu
6. National Cybersecurity Strategy of Estonia. URL: https://www.mkm.ee
7. Матеріали з офіційного сайту Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua