Матвійчук Оксана Миколаївна
курсант 204 навчальної групи ННІ № 3 НАВС, рядовий поліції

Науковий керівник:
Яровий Кирило Васильович
кандидат юридичних наук, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції

СУЧАСНИЙ СТАН КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

Кожна соціально активна особа в Україні користується мобільними пристроями та інтернетом. Державні органи переходять на електронний документообіг. Стабільна діяльність банківського сектору, залізниць та авіатранспорту, а також великих підприємств залежить від стабільності кіберпростору. Україна переживає переломний етап, де війна перетворюється на битву не лише на полі бою, а й в інформаційному просторі. Внаслідок цього зростає кіберзлочинність, яка викликана як зовнішніми, так і внутрішніми загрозами, використовуючи перевантаженість правоохоронних органів та загальний хаос в суспільстві.

Хоча проблеми кіберзахисту в Україні вже досліджувалися у працях вчених, таких як Алпеєв А.С., Архіпов О.Є., Бакалинський О.О., Богданов О.М., Грибунін В.Г., Горбатько О.В., Мохор В.В., та Чепуренко Я.О., на сьогодні це питання стало найбільш поширеним та актуальним для суспільства, оскільки воно стосується всіх, хто працює з інформаційними технологіями.

У юридичній літературі кіберзлочин – це небезпечне діяння у кіберпросторі чи з використанням комп'ютерних технологій, передбачене законом, яке полягає в розкраданні або руйнуванні інформації в мережах і системах. У воєнний час це може спрямовуватися на дестабілізацію країни, крадіжку конфіденційних даних, а також на пошкодження державних інституцій і техніки [1].

Передумовами та чинниками, які формують загрози у сфері кібербезпеки України, є:

– недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського права у вітчизняне законодавство, недостатня врегульованість цифрової складової частини розслідування злочинів, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері;

– відсутність у значної частини міністерств і відомств відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом. Фінансування робіт із кіберзахисту здійснюється за залишковим принципом з технологічними помилками;

– відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності країни, що вимагає суворого дотримання відповідних стандартів;

– невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі; – відсутність законодавчого акта про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури;

– незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки;

– відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту [2, с. 11].

Отже, в умовах воєнного стану в Україні, окрім існуючих правоохоронних органів, які борються з кіберзлочинністю, необхідно створити спеціальні підрозділи для захисту від кібервоєнних операцій супротивника та надавати адекватну відповідь на його інформаційну інфраструктуру.

Так, наприклад, правоохоронними органами України, США, Великої Британії, Японії, Філіппін, Індонезії, Малайзії було проведено такі операції: – «секс Торшн», внаслідок якої затримано 56 осіб, ліквідовано 4 транснаціональні кримінальні угрупування; – «Зевс», завданням якої було знешкодження міжнародної організованої злочинної групи, котра з метою викрадення фінансових реквізитів і доступу до банківських рахунків розповсюджувала шкідливе програмне забезпечення «Зевс». Під час операції знешкоджено інфраструктуру в мережі, що включала понад 40 тис. інфікованих комп’ютерів і серверів, левова частка яких знаходилась на території України. Спричинені збитки понад 300 млн доларів. Члени організованого злочинного угруповання – хакери з Одеси та Харкова на чолі з громадянином рф [3, с. 68].

Кібервійська, або служба кібероборони, повинна входити до складу Збройних сил України та містити структурні підрозділи, що здійснюють кіберрозвідку та спеціальні кібероперації, включаючи психологічні впливи на ресурси супротивника. Діяльність таких підрозділів повинна бути законодавчо регульована. Діяльність цих підрозділів повинна бути законодавчо регульована.

Це завдання складне через відсутність чітких норм щодо ведення військових дій у кіберпросторі, зокрема відносно їх початку, масштабів та розрізнення від традиційних кіберзлочинів. Проте поточна ситуація вимагає вирішення цього питання негайно.

Тому, у зв'язку з високим рівнем інформатизації суспільства, Україна повинна забезпечити ефективний механізм протидії кіберзлочинам, які є серйозною загрозою для національної безпеки. Оскільки ці злочини мають транснаціональний характер, правоохоронним органам України потрібне вдосконалене технічне забезпечення та компетентність для співпраці на міжнародному рівні у кримінальних розслідуваннях із цієї сфери, а також загалом у боротьбі з кіберзлочинністю. Україна має необхідні ресурси для розвитку своїх кібербезпекових здібностей для відповіді на сучасні виклики та загрози.

Список використаної літератури:

1. Закон України "Про основні засади забезпечення кібербезпеки України" № 2163-VIII (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403).

2. Проєкт «Стратегія кібербезпеки України на 2021–2025 роки». Рада національної безпеки і оборони України: веб-сайт. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 15 квітня 2024 р.)

3. Демедюк С. В., Демедюк Т. С. Міжнародний досвід протидії кіберзлочинності. Вісник ХНУВС. 2014. № 4 (67). С. 65–75. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/6023/Mizhnarodnyi%20dosvid%20protydii%20kiberzlochynnosti_%20 Demediuk%20SV_Demediuk_2014.pdf (дата звернення: 14 квітня 2024 р.).