ЩОДО КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Смілянець Єгор Ігорович
курсант 3 курсу ФПФПКП
Дніпропетровський державний університет внутрішніх справ, Україна

Білаш Олексій Олександрович
курсант 3 курсу ФПФПКП
Дніпропетровський державний університет внутрішніх справ, Україна

Науковий керівник: Плахотний Артем Павлович
старший викладач кафедри тактико-спеціальної підготовки, підполковник поліції
Дніпропетровський державний університет внутрішніх справ, Україна

Анотація. *Ця тема розглядає актуальні аспекти кібербезпеки під час воєнного конфлікту та ролі кіберзагроз у воєнному контексті. Зростаюча кількість кібератак та їх вплив на військові операції стають серйозною загрозою для національної та міжнародної безпеки. Анотація описує важливі аспекти:*
Розглядаються різновиди кіберзагроз, які можуть виникнути під час військових конфліктів, включаючи кібершпигунство, кіберсаботаж, та кібертероризм. Пояснюється, як ці загрози можуть вплинути на військові операції та національну інфраструктуру.
Аналізується необхідність впровадження заходів кібербезпеки під час воєнного стану. Описуються кроки, які військові та цивільні органи можуть прийняти для захисту критичних інформаційних систем та мереж у таких умовах.
Аналізується міжнародна динаміка в сфері кібербезпеки під час воєнного стану, зокрема міжнародні договори, правила та регулювання, що регулюють кібероперації в контексті війни. Висвітлюється важливість міжнародного співробітництва та превентивних заходів для зменшення кіберзагроз в умовах воєнного стану.

Постановка проблеми. З початку війни Україна стала об'єктом численних кібератак за участю урядових установ, приватних організацій та громадян. Компанії, які є частиною критичної інфраструктури, особливо енергетичні, комунікаційні, медіа та фінансові компанії, також повинні бути пильними, оскільки ці галузі часто розглядаються як пріоритетні цілі під час війни.

Викладення основного матеріалу. У сучасній ситуації інформаційного світу кібербезпека займає особливе місце в наукових дослідженнях і активно розвивається з кожним роком. Останнім часом Кібербезпека та її окремі аспекти стали предметом численних досліджень дослідників. Але проблема визнання цього явища залишається відкритою, що логічно і необхідно, враховуючи надвисокі темпи розвитку зв'язків з громадськістю в електронній сфері. Це пояснюється, перш за все, розширенням можливостей інформаційного впливу на суспільні відносини, що обумовлює появу нових загроз громадській безпеці, необхідність оновлення та вдосконалення системи її забезпечення. Крім того, сама концепція кібербезпеки вимагає якісного переосмислення, викликаного швидкими внутрішніми змінами феномену інформації і домінуючою тенденцією в розвитку світової спільноти, яка в основному набуває "інформаційний" вимір. У цьому сенсі масштаби сучасної трансформації інформаційної сфери є причиною багатьох теоретичних і практичних проблем, що вимагають уточнення концепції кібербезпеки і додання їй більшої сили і системності. Варто почати з концепцій, які важливі для нашого дослідження. Для

того щоб визначити деталі сприйняття поняття "забезпечення кібербезпеки" в рамках даного дослідження, рекомендується зосередитися на визначенні самого поняття "забезпечення безпеки" [3, ст. 17].

По-перше, розгляньте профіль вашої компанії, географію та інші фактори, щоб краще зрозуміти ризики поточних сценаріїв загроз, які можуть виникнути.

Кіберзахист. Має сенс переглянути важливий набір засобів контролю кібербезпеки, які допоможуть знизити ймовірність успішних атак, особливо тих, які допоможуть захиститися від загроз з боку агресорів і організованих груп, які активізували свою діяльність під час війни.

Моніторинг кібербезпеки. На додаток до превентивного захисту, ефективний моніторинг безпеки також важливий для своєчасного виявлення вторгнень і реагування на них. Середній час між початковим зломом і запуском шкідливого ПО деструктивного характеру тепер вимірюється днями, а не тижнями або місяцями, як раніше.

Люди. Підприємство повинно планувати можливість призупинення діяльності в зоні бойових дій, а в деяких випадках організовувати тимчасову кадрову допомогу для забезпечення функціонування життєво важливих служб, поки працівник не зможе повернутися до офісу чи країни. Організації повинні бути обізнані про ризики, пов'язані з організованими злочинними угрупованнями, на додаток до підтримки своїх співробітників і їх сімей. Ці групи намагаються скористатися кризою, створюючи підроблені веб-сайти, які надають допомогу чи корисну інформацію або приймають пожертви. Існує висока ймовірність фішингової кампанії, спрямованої на високопоставлених чиновників, які фокусуються на темі війни в Україні і відкрито висловлюють свою позицію з приводу війни.

Міграція в хмару. Воєнний стан в Україні також викликав занепокоєння компаній через нові завдання щодо забезпечення безперебійної роботи життєво важливих служб і систем, які можуть бути пошкоджені або виведені з ладу в результаті бойових дій. Перенесіть свою IT-інфраструктуру в хмару або створіть сайт аварійного відновлення у вашому глобальному хмарному центрі обробки даних, щоб забезпечити необхідний рівень доступності.

Поточна ситуація залишається непередбачуваною, і компаніям і організаціям важливо постійно аналізувати, як ситуація розвивається далі і які сценарії виникають для кожного сценарію, компаніям необхідно аналізувати, як конкретний сценарій впливає на організацію, беручи до уваги людей, бізнес, ланцюжок поставок і технології. У той же час деякі з розглянутих рекомендацій тепер можуть бути реалізовані для підготовки до таких випадків, підвищення стійкості, пом'якшення наслідків і скорочення періоду часу, коли відбуваються інциденти.

Всі сучасні соціально активні люди в Україні користуються Інтернетом за допомогою мобільних пристроїв, Державні установи переходять на стабільну діяльність електронного документообігу, банківський сектор, Залізничний і повітряний транспорт, великі компанії покладаються на стабільність кіберпростору, в якому вони працюють, і засновані на спілкуванні з використанням електронних засобів зв'язку.

Там, де розвиваються нові соціальні відносини, там же з'являється і злочинність. Згідно з офіційною статистикою прокуратури України, кількість виявлених кіберзлочинів за останні 8 років збільшилася майже в 7,5 разів (це не враховує класичні злочини з використанням комп'ютерних технологій і рівень затримок по таких злочинах).

На початку XXI століття злодій - це не завжди холоднокровна озброєна людина. Інформаційна революція призвела до того, що звичайний студент з ноутбуком і доступом до мережі може стати злодієм.

У ситуації війни такий злодій стає бойовою одиницею, його основними інструментами є кібератаки і зломи. Крім того, під час воєнного стану можливі атаки не тільки з боку ворогів, які використовують інформаційний простір для нанесення шкоди обороноздатності України, а й з боку тих, хто вирішив скористатися ситуацією, в якій правоохоронні органи перевантажені. Вона отримує вигоду з коштів громадян. Протягом півтора місяців війни кіберзлочинність в Україні неухильно зростала.

Сьогодні війни в інформаційному просторі можуть завдати меншої шкоди, ніж війни на полі бою. Для досягнення цієї мети в перший місяць війни Конгрес оперативно оптимізував Кримінально-процесуальний кодекс і Кримінально-процесуальний регламент, а також удосконалив підстави і процесуальні механізми притягнення кіберзлочинців до кримінальної відповідальності. Зміни стосуються 2 законів:

- «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації" щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137-IX від 15.03.2022 [5];
- «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24.03.2022.Якщо перший був прийнятий майже 1 місяць тому, то Закон № 2149-IX набув чинності зовсім недавно - тільки в 2022-3-04 роках. Ми пропонуємо розібратися, що саме це змінить [1].

Що таке кіберзлочинність і які її небезпеки під час війни?

Перш ніж аналізувати закон, варто визначитися з термінами. Законодавець дає власне визначення кіберзлочинності, але це не нове. Кіберзлочинність (комп'ютерний злочин) - відповідальність за суспільно небезпечні дії з необережності та/або їх використання у кіберпросторі передбачена Законом України Про кримінальну відповідальність (КК) та/або визнається злочином міжнародними договорами України. («Про основні засади забезпечення кібербезпеки України» Документ 2163-VIII, від 17.08.2022) [2, ст. 4].

Метою таких дій є крадіжка або знищення інформації в інформаційних системах і мережах. В умовах війни кіберзлочинність спрямована на дестабілізацію ситуації в країні, крадіжку необхідних (конфіденційних) даних, виведення з ладу державних установ, обладнання та нанесення іншого серйозного збитку.

З початку війни стало відомо про численні кібератаки на Україну:

- Варто згадати невдалу спробу атаки хакерського угруповання Strontium, які намагалися отримати доступ до комп'ютерних мереж в Україні, США та ЄС, щоб забезпечити тактичну підтримку фізичного вторгнення рОсії в Україну та викрасти конфіденційну інформацію.
- Нещодавно Держспецзв’язку повідомило про отримання українськими користувачами нових небезпечних електронних листів з темою «№ 1275 від 07.04.2022», відкриття яких призводить до отримання хакерами повного контролю над вашим комп'ютером та загрожує крадіжкою та пошкодженням комп'ютерних даних.
- Раніше, 4 квітня, Держспецзв'язку попереджувало про розповсюдження електронних листів з назвою «Військові злочинці РФ.htm», відкриття яких призводить до того, що зловмисники отримують віддалений доступ до комп'ютера жертви.

• Під прицілом знаходяться також об'єкти критичної інфраструктури. Український провайдер Укртелеком зазнав потужної атаки 28 березня 2022 року, під час якої хакери намагались · проаналізувати, як влаштована ІТ-інфраструктура, вивести з ладу обладнання та сервіси, а також отримати контроль над мережею та обладнанням компанії.

• 23 березня ворог намагався здійснити кібератаку на державні установи України з використанням шкідливої програми Cobalt Strike Beacon, яка уражає комп'ютер у випадку її відкриття.

Це лише приклади масштабних атак. Можливо, про окремі випадки незначних нападів або особистих переломів просто не повідомляється.

Відповідальність за кіберзлочини передбачена розділом XVI КК України, саме 2 норми із цього розділу і зазнали змін відповідно до нового Закону 2149-IX [6].

Було оновлено основну правову структуру злочину, передбаченого статтею 361 Кримінального кодексу

Крім термінів, частина 361 статті 1 Кримінального кодексу [6] отримала конструктивні зміни - формальний склад замінив матеріальний. Надалі, щоб кваліфікувати діяння як злочинне за такими нормами, людині досить вчинити дії (несанкціоноване втручання), а наслідки необов'язкові (наприклад, поворот, втрата, підробка, блокування інформації і т.д.). Це спрощення полягає в криміналізації діянь, за які раніше не встановлювалася кримінальна відповідальність, і в той же час в криміналізації діянь, за які не встановлювалася кримінальна відповідальність. З іншого боку, санкції проти "спрощеного складу" також стали помітно м'якше. [1, ст. 1]

З початку війни в Україні кібербезпека країни опинилася під серйозною загрозою. Російські кіберзлочинці здійснюють численні атаки на державні установи, приватні компанії та громадян України. Мета цих атак - дестабілізувати ситуацію в країні, завдати шкоди критичній інфраструктурі та нанести економічний збиток.

Уряд України ухвалив ряд заходів для посилення кібербезпеки країни, зокрема:

Закон № 2149-IX, який передбачає посилення кримінальної відповідальності за кіберзлочини [1].

Закон № 2137-IX, який спрощує процедуру розслідування кіберзлочинів [6].

Ці заходи спрямовані на те, щоб зробити кіберпростір України більш безпечним і покарати кіберзлочинців, які намагаються завдати шкоди Україні.

Висновок. В умовах воєнного стану кіберзлочинність є серйозною загрозою для України. Російські кіберзлочинці здійснюють численні атаки на об'єкти критичної інфраструктури, державні установи та приватні компанії. Для підвищення рівня кібербезпеки в Україні необхідно забезпечити належний захист державних установ та критичної інфраструктури, а також підвищувати обізнаність громадян про кіберзагрози та способи їх захисту.

Список використаних джерел:

1. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 р. № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 10.11.2023).
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.11.2023).
3. Про внесення змін до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації : Закон України від 04.06.2020 р. № 681-IX. URL: https://zakon.rada.gov.ua/laws/show/681-20#Text (дата звернення: 10.11.2023).

4. Лісовська ЮП. Кібербезпека: ризики та заходи: навч. посібник. К.: Видавничий дім «Кондор. 2019.
5. Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам: Закон 2137-IX | ЮРЛІГА. ЮРЛІГА. URL: https://ips.ligazakon.net/document/T222137?an=1 (дата звернення: 10.11.2023)
6. Савенко АБ, Плахотний АП. ВОЄННІ ЗЛОЧИНИ ПРОТИ МИРНОГО НАСЕЛЕННЯ. Адаптація правової системи України до права Європейського Союзу.:261.
7. Сизов ВК, Плахотний АП. ЕФЕКТИВНА ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ В УМОВАХ ВІЙСЬКОВОГО СТАНУ Є ЕЛЕМЕНТОМ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА УСПІШНОГО ВЕДЕННЯ ВІЙСЬКОВИХ ОПЕРАЦІЙ. InThe 6 th International scientific and practical conference “Modern problems of science, education and society”(August 14-16, 2023) SPC “Sci-conf. com. ua”, Kyiv, Ukraine. 2023. 671 p. 2023 Aug 14 (p. 651).