.ua/ua/news/17173_Tetyana_Kovalchuk_Princip_nulovoi_tolerantnosti_do_domashnogo_nasilstva__indikator_rozvinenogo_suspilstva_FOTO.htm

Анастасія Москвичова. Як працює «Поліна» – поліція проти домашнього насильства. Радіо Свобода. 2019 р. URL: https://www.radiosvoboda.org/a/28602166.html

DOI https://doi.org/10.36059/978-966-397-358-6-3

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ В УМОВАХ ВІЙНИ В УКРАЇНІ

Білецький Богдан Михайлович
здобувач освітньо-наукового рівня (доктор філософії),
Науково-дослідний інститут публічного права
м. Київ, Україна

Клюйко Сергій Валерійович
здобувач освітньо-наукового рівня (доктор філософії),
Науково-дослідний інститут публічного права
м. Київ, Україна

Кожна сучасна соціально активна людина в Україні використовує мобільні пристрої та користується інтернетом, державні органи переходять на електронний документообіг, стабільна діяльність банківського сектору, залізниці й авіатранспорту, великих підприємств залежить від стабільності кіберпростору, з яким вони працюють, та базується на комунікації за допомогою електронних засобів зв'язку.

В умовах війни такий злодій стає бойовою одиницею, а його основний інструмент – кібератаки і злами. Крім того, під час воєнного стану атаки можливі не лише з боку ворога, який використовує інфопростір для завдання шкоди обороноздатності України, а й з боку тих, хто вирішив скористатися ситуацією, коли правоохоронні органи перевантажені, та поживитися коштами наших громадян. Протягом півтора місяця війни кіберзлочинність в Україні стабільно зростає.

В наш час війна в інформаційному просторі може завдати не меншої шкоди, аніж війна на полі бою. Розуміючи це, у перший місяць війни парламент оперативно оптимізував кримінальне та кримінально-процесуальне законодавство, удосконаливши підстави та процесуальні

механізми притягнення до кримінальної відповідальності кіберзлочинців. Зміни зосереджено у двох законах:

– «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;

– «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24.03.2022.

Перш ніж аналізувати закон, варто визначитися із термінологією. Законодавець надає власне визначення кіберзлочину, яке не є новим. Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність (ККУ) та/або яке визнано злочином міжнародними договорами України (п. 8 ч. 1 ст. 1 Закону України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 N 2163-VIII).

Мета таких дій – розкрадання або руйнування інформації в інформаційних системах і мережах. В умовах війни кіберзлочини можуть здійснюватися з метою дестабілізації ситуації в країні, крадіжки необхідних (конфіденційних) даних, виведення з ладу державних інституцій, техніки, завдання іншої матеріальної шкоди.

Від початку війни стало відомо про велику кількість кібератак на Україну:

1. 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 IT-інфраструктура, вивести з ладу обладнання та сервіси, а також отримати контроль над мережею та обладнанням компанії.

2. 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 приклади лише масованих атак. Ймовірно, про атаки менших масштабів та окремі випадки персональних зламів просто не повідомляється.

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

Також Закон 2149-IX передбачає, що втручання в роботу інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж не вважатиметься несанкціонованим, якщо таке втручання вчинено відповідно до Порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж, текст якого Держспецзв'язку зараз активно напрацьовує.

Ще до початку війни, після кібератак 14 січня на сайти державних органів влади, відчувалася необхідність запровадження невідкладних змін в українському законодавстві для узаконення процедури Bug Bounty (залучення зовнішніх фахівців до пошуку помилок і вразливостей програмних продуктів, інформаційно-комунікаційних систем тощо). Тож на сьогодні ІТ-спільнота зможе легально тестувати державні інформаційні системи на наявність вразливостей, а держава отримає інструмент для значного підвищення ступеня захисту таких систем.

З іншого боку, запровадження ч. 6 ст. 361 ККУ є логічним продовженням змін у конструкції ч. 1 ст. 361 ККУ. Адже те, про що вказано у частині 6, раніше не визнавалося злочином відповідно до частини 1.

Електронна система публічних закупівель Prozorro заявила, що тимчасово призупиняє програму Bug Bounty у зв'язку з введенням воєнного стану в Україні до завершення воєнних подій. Незважаючи на припинення програми, дії багхантерів не будуть вважатися правопорушеннями, а нові звіти про знайдені вразливості будуть прийняті до розгляду після завершення воєнного стану та відновлення програми пошуку вразливостей Bug Bounty.

Варто визнати й певну неповноту закону в цій частині. Від початку війни в Україні активізувався неофіційний громадський рух кіберопору ворогові, так звана «КіберАрмія». Звичайні люди, поряд із професіоналами сфери ІТ, атакують ворога у кіберпросторі, завдаючи йому збитків та зриваючи плани. Формально такі дії можуть підпадати під ознаки складів злочинів, що передбачені ст. ст. 361, 361-1 ККУ.

Ймовірно, що навіть при ініціюванні відповідного кримінального провадження проти таких осіб, правоохоронні органи та суди використовуватимуть загальні механізми їх звільнення від відповідальності, адже дії таких осіб відповідають інтересам України та українського народу та не є суспільно небезпечними. Незважаючи на це, формалізація подібного звільнення від відповідальності на рівні приміток чи окремих частин відповідних спеціальних статей ККУ є бажаною у майбутньому, аби правоохоронні органи не витрачали власних зусиль на «дружній вогонь» чи пошук юридичних шляхів його уникнення.

Отже підвищення ефективності боротьби з кіберзлочинністю під час війни та посилення відповідальності за відповідні злочини є давно назрілим кроком. Новий закон розширює межі діяльності правоохоронних органів щодо розслідування кіберзлочинів, передбачених статями 361, 361-1 ККУ. Посилення санкцій та додаткова криміналізація окремих діянь здатні частково стримати потенційних злочинців від вчинення нових злочинів.

Виправданим є й запровадження відповідальності за злочини, що скоєні у воєнний час. Настільки суворі санкції за їх вчинення продиктовані поточною ситуацією в країні, адже особа, яка завдає шкоди національним інтересам України чи українцям у кіберпросторі, тим самим допомагаючи агресору у цій війні, не може нести відповідальності меншої, ніж військові злочинці.

Сфера кіберпростору і раніше потребувала посиленого захисту та змін. Відкрите вторгнення росії стимулювало вдосконалення чинного законодавства та гарантій безпеки у сучасному інформаційному середовищі.

На підставі викладеного можемо констатувати, що під час війни в зоні ризику перебувають державні органи, великі підприємства, підприємства оборонної та критичної інфраструктури, а також підприємства, які забезпечують населення та оборону усім необхідним в умовах війни. Є ризики й для місцевих жителів, які перебувають в зоні бойових дій.

Література:

1. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. – LigaZakon: сайт. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix

2. Кримінальний кодекс України. Законодавство України: сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text