поведінки, проведення роз'яснювальної роботи у двох напрямах: тлумачення чинного законодавства з приводу можливих наслідків для винного (винних) в частині відповідальності, а також для потерпілого (потерпілих) – розлади психіки, аж до можливого самогубства дитини.

Фінальним, найбільшим за обсягом, напрямом запобігання на державному рівні – вбачається створення єдиного, консолідованого документу – концепції протидії або навіть законодавчого акту, яким було б узагальнено заходи та механізми взаємодії у напрямі протидії як кібербулінгу, так і булінгу в цілому.

Список бібліографічних посилань

1. Бандурка І. О. Захист дитинства в Україні: кримінально-правові та кримінологічні засади : монографія. Х., 2017. 432 с.

2. Дівочі розбірки: в Одесі група дівчат-підлітків жорстоко побила ровесницю та зняла все на відео // УНІАН: інформаційне агенство. 04 серпня 2018 12:53. URL: https://www.unian.ua/incidents/10213073-divochi-rozbirki-v-odesi-grupa-divchat-pidlitkiv-zhorstoko-pobila-rovesnicyu-ta-znyala-vse-na-video.html (дата звернення: 28.10.2018).

3. Лубенець І. Кібернасильство (кібербулінг) серед учнів загальноосвітніх навчальних закладів. *Jurnalul juridic national: teorie şi practică. Национальный юридический журнал: теория и практика*. 2016. № 3 (19). С. 178–182.

4. «Солодкий» конфлікт в школі Харкова: батьки обділеної тортом учениці хочуть справедливості. URL: https://ukr.segodnya.ua/ukraine/sladkiy-konflikt-v-shkole-harkova-roditeli-uchenicy-kotoruyu-obdelili-tortom-hotyat-spravedlivosti-1182186.html (дата звернення: 28.10.2018).

Одержано 02.11.2018

УДК 351.741 В 68

Олексій Гнатович ВОЛОШИН,
старший викладач кафедри криміналістичного забезпечення та судових експертиз
Навчально-наукового інституту № 2
Національної академії внутрішніх справ;
Віталій Вячеславович ПОЛІЩУК,
курсант 403 навчальної групи
навчально-наукового інституту № 2
Національної академії внутрішніх справ

КІБЕРАТАКИ – СУЧАСНИЙ ЗАСІБ ГІБРИДНОЇ ВІЙНИ

З огляду на те, що проблема кіберзлочинності на сучасному етапі розвитку України набуває глобального виміру та становить загрозу інформаційному суспільству отримала відображення у нормативно – правових актах національного та міжнародного рівнів. Кібератаки значно почастішали, тому було вирішено посилити механізми захисту державних комп'ютерних систем. 15 березня 2016 року Президент України видав Указ «Про введення в дію рішення Ради національної

безпеки та оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». В складі Ради національної безпеки створено робочий орган – Національний координаційний центр кібербезпеки. Поява цього органу цілком обґрунтована, адже поруч з перевагами інформаційних технологій, їх активно використовують для «здійснення терористичних актів, в тому числі шляхом порушення штатних режимів автоматизованих систем управління технологічним процесами на об'єктах інфраструктури [1].

У науковій літературі боротьба зі злочинністю розглядається як першочергове загальнодержавне завдання, яке є складовою частиною діяльності органів державної влади. Особливе місце в боротьбі зі злочинами, пов'язаними з протиправним використанням комп'ютерної інформації та комп'ютерних технологій, необхідно надати правоохоронним органам України. Наказом МВС України від 07.07.2017 № 575 «Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні» і розділі XV зазначенні особливості організації взаємодії при досудовому розслідуванні кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку (кіберзлочинів) [2].

В умовах сьогодення, що характеризується агресивними діями Російської Федерації проти України, шляхом застосування методів гібридної війни, використання кібератак в інформаційному просторі є однією із форм її.

Інформаційна війна – це узгоджена діяльність з використання інформації як зброї для ведення бойових дій. Головним стратегічним національним ресурсом стає інформаційний простір, тобто інформація, мережева інфраструктура та інформаційні технології. зростання яких має місце [3].

Одним з ключових компонентів гібридної агресії проти України стала пропаганда, яка створила сприятливий ґрунт для ініціювання внутрішніх заворушень, економічного тиску а також кібератак. При цьому Інтернет використовується для поширення радикальної ідеології, вербування прихильників і фінансування незаконної діяльності, пов'язаної з тероризмом.

Одним із наслідків пропаганди Російська Федерація постійно збільшує кількість операцій по кібершпіонажу, та все більше намагається вплинути на громадську думку, не гребуючи використанням фейкових новин. які спрямована, перш за все, проти слабких місць України.

Тому кібербезпека – одна з основних проблем, що викликає занепокоєння. Гібридна війна має виміри кібер та інформаційний і на

сьогодні вони набувають особливого значення. Особливістю соціальних мереж є те, що через них негативний інформаційний вплив часто здійснюється приховано і має тривалий характер до моменту свого виявлення та «включення» важелів протидії. Очевидно, що соціальні мережі все більше стають ареною протиборства. Наслідки такого протиборства для України залежать в першу чергу від захисту особистих даних інтернет-ресурсів від кіберзагроз.

Кіберпростір, поряд із землею, повітрям, морем і космосом, визнано новим оперативним простором, а кібероперації – невід'ємною частиною гібридної війни. інфраструктури від кібератак. Тож Росією постійно проводяться кібернетичні операції проти об'єктів критичної інфраструктури, приватного сектору, а також інформаційно-телекомунікаційних систем Збройних Сил України які можуть призвести до наслідків кожна з кібератак, що використовуються під час проведення кібероперацій:

– вандалізм – атака, яка, звісно, не вбиває людей, але завдає удару по авторитету держави як у світі, так і серед населення, простими словами, завдає репутаційних втрат;

– пропаганда – розсилка спаму, що містить інформацію пропагандистського характеру, фейкові новини для просування вигідної точки зору та дезорієнтації населення;

– збір інформації – злом приватних сторінок або серверів баз даних для збору цінної інформації та її заміни на інформацію, корисну іншій стороні. Інша назва – кібершпигунство;

– відмова сервісу – атаки з великої кількості комп'ютерів, основна мета яких – порушення функціонування сайтів або комп'ютерних систем;

– втручання в роботу обладнання – атаки на комп'ютери або сервери, які, наприклад, забезпечують роботу комунікаційних цивільних або військових систем, що, у свою чергу, призведе до відключення або виникнення помилок при обміні даними, а ще гірше – буде втрачено зв'язок, а відтак можливість управління діями підрозділів;

– атаки на об'єкти критичної інфраструктури – атаки на комп'ютери та системи, що забезпечують життєдіяльність міст, а саме: системи водопостачання, електроенергії, транспорту.

Використовуючи кіберпростір, хакери можуть зламати захищені мережі та отримати необхідну інформацію, тому ми мусимо спрямувати зусилля на захист своїх мереж і забезпечити їх безпеку, використовуючи такі рівні захисту інформації:

– запобігання – доступ до інформації та технології надається тільки для персоналу, який отримав допуск та має відповідні фахові навички;

– виявлення – забезпечується раннє виявлення злочинів і зловживань, навіть якщо механізми захисту були обійдені;обмеження – зменшується розмір втрат, якщо злочин все-таки відбувся, незважаючи на заходи щодо його запобігання та виявлення; відновлення – забезпечується ефективне відновлення інформації за наявності документованих і перевірених планів з відновлення.

Свої особливості має робота правоохоронних органів що протидії кібератаки в умовах проведення Операції об'єднаних сил. Відтак найактуальніші напрямки роботи кіберполіцейських Донеччини та Луганщини – це боротьба з інтернет-шахрайствами, (як правило, знаходяться на непідконтрольній території) протидія загрозам в сфері кібербезпеки, а також «розвідка» в кіберпросторі щодо дій незаконних збройних формувань.

Що стосується інформаційно-гібридної війни, то щодня, починаючи з 2014 року і по сьогоднішній день, здійснюється щоденний моніторинг мережі Інтернет з метою виявлення осіб, причетних до незаконних збройних формувань і повалення влади, а також щодо виявлення несанкціонованих мітингів, порушення громадського порядку, сепаратизму.

Висновок, який ми повинні зробити для себе, – це збільшення інвестування в кібербезпеку, щоб запобігати атакам на великі державні й приватні компанії і протистояти намірам дестабілізувати суспільство.

Крім того, кожне суспільство потребує правил, стандартів, норм, положень, інструкцій та інших документів, щоб почувати себе захищеним у кіберпросторі хоча б у правовому відношенні. поліпшення стану кібербезпеки в Україні.

Список бібліографічних посилань

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : указ Президента від 15.03.2016 № 96/2016 // БД «Законодавство України» / ВР України. URL: http:// zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 30.10.2018).

2. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС України від 07.07.2017 № 575 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/z0937-17 (дата звернення: 30.10.2018).

3. СБУ: Хакери вкрали 10 млн гривень у Києві // Корреспондент.net. 20 листопада 2017 16:14. URl: https://ua.korrespondent.net/ukraine/3908582-sbu-khakery -vkraly-10-mln-hryven-u-kyievi (дата звернення: 30.10.2018).

Одержано 31.10.2018