УДК 004.946.5.056

Вікторія Русланівна Лисак,
студентка 2 курсу юридичного факультету
Тернопільського національного економічного університету

Кіберзлочинність: як захистити себе в мережі

За останні кілька років комп'ютерні технології глибоко проникли в повсякденне життя людини. Заперечувати їх важливість практично неможливо, адже кожен день людина використовує різні комп'ютерні блага, вони стали невід'ємною частиною її звичного способу життя.

Проте, разом з розвитком інформаційних технологій зростає і кількість злочинів у цій сфері. Кіберзлочини, або іншими словами комп'ютерні злочини, – це суспільно небезпечні винні діяння, вчинені у кіберпросторі за допомогою комп'ютера та Інтернету. Кіберзлочинці зазвичай полюють на персональні дані, банківські рахунки, конфіденційну та комерційну інформацію, паролі тощо. Потерпілими від цих атак можуть бути як фізичні, так і юридичні особи, а також держава [1].

Для ефективної боротьби з кіберзлочинністю та регулювання відносин у цій сфері держава на законодавчому рівні впроваджує різноманітні нормативно-правові акти. До таких актів, зокрема, належать Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» та інші закони [4].

Крім того, важливу роль у протидії кіберзлочинності відіграє Конвенція про кіберзлочинність, яка належить до українського законодавства, адже належним чином ратифікована ВРУ. Відповідно до цієї Конвенції, кіберзлочини поділяються на чотири види, а саме: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ; нелегальне перехоплення; втручання у дані; втручання у систему; зловживання пристроями), правопорушення, пов'язані з комп'ютерами (шахрайство), правопорушення, пов'язані зі змістом (дитяча порнографія), а також правопорушення, пов'язані з порушенням авторських та суміжних прав [3].

Кількість кіберзлочинів в Україні щороку зростає. Найпоширенішим видом злочинів є шахрайство. Зокрема, впродовж 2019 року було зареєстровано 45836 злочинів у сфері шахрайства, 21153 проваджень з яких було закрито. Найчастіше шахраї створюють сайти і продають неіснуючий товар, дуже багато злочинів, які стосуються виманювання інформації з карток та онлайн-кредитування [5].

Друге місце посідають кіберзлочини у сфері незаконного втручання в роботу комп'ютерів – у 2019 році зареєстровано 1079 правопорушень, серед яких 74 було закрито. Розповсюдження порнографії займає третє місце серед найбільш популярних кіберзлочинів. Згідно з даними Генеральної прокуратори України, у 2019 році було зареєстровано 774 проваджень і лише 47 вирішено [5].

Варто зазначити, що повністю захистити себе від кібератак неможливо. Проте виконання хоча б мінімальних правил техніки безпеки поводження в мережі значно підвищить шанси, що вас не зламають. До основних правил належать: уважно читайте сайти, де залишаєте персональні дані; створюйте складні паролі, не варто використовувати один і той самий пароль і для банківської картки, і для входу в соціальні мережі; не використовуйте громадський Wi-Fi для важливих цілей, не здійснюйте платіжних операцій, адже через них хакери можуть перехопити ваші дані, тому краще користуватись мобільним Інтернетом.

Не давайте нікому персональні дані, паролі і коди-підтвердження з СМС для операцій з картками; перевіряйте інформацію за офіційним номером банку; не скачуйте в Інтернеті сумнівні файли; користуйтесь ліцензійним програмним забезпеченням; не переходьте на підозрілі посилання та за спливаючими вікнами; періодично здійснюйте резервне копіювання важливої інформації; тримайте свої гаджети в полі зору, коли знаходитеся у місцях, де до них може бути доступ сторонніх осіб [2].

До того ж, варто встановити двофакторну автентифікацію для email та акаунтів у соцмережах. Для входу в акаунт, окрім паролю, налаштуйте відправлення СМС на ваш мобільний із одноразовим кодом або ж встановіть додаток – генератор кодів. Мало хто знає про те, що сумнівний номер телефону чи картки можна перевірити на сайті кіберполіції, а також звернутися до спеціалістів із запитом [5].

Можна зробити висновок, що сучасний світ живе в епоху інформаційних технологій. Можливості мережі є не лише джерелом інформації, знань та спілкування, але й джерелом підвищеної небезпеки. Саме тому

потрібно бути готовим до того, що в будь-який момент у кого-небудь може виникнути бажання отримати доступ до ваших персональних даних, банківських рахунків чи паролів. Саме тому дотримання певних правил зменшить ризик цих кібератак. Це унеможливить доступ зловмисників до ваших аккаунтів та вбереже вас від потрапляння в пастки кіберзлочинців [2].

Список бібліографічних посилань

1. За п'ять років кіберзлочинність в Україні виросла вдвічі / Економічна правда : сайт. 21.10.2019. URL: https://www.epravda.com.ua/news/2019/10/21/652782/ (дата звернення: 21.10.2019).
2. Нікулеско Д. Кібербезпека: вразливі моменти // Юридична газета online : сайт. URL: http://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html (дата звернення: 21.10.2019).
3. Конвенція про кіберзлочинність : від 07.09.2005 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 21.10.2019).
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 21.10.2019).
5. Що варто знати про кіберзлочинців в Україні? // Радіо Свобода : сайт. URL: https://www.radiosvoboda.org/a/details/29031166.html (дата звернення: 21.10.2019).

Одержано 01.11.2019