Скиммери можуть накопичувати вкрадену інформацію про пластикові картки або дистанційно передавати її по радіоканалу зловмисникам, які знаходяться поблизу. Після копіювання інформації з карти шахраї виготовляють дублікат карти і, знаючи ПІН, знімають всі гроші в межах ліміту видачі, як в Росії, так і за кордоном. Також шахраї можуть використовувати отриману інформацію про банківську карту для здійснення покупок в торгових точках.

Більшість кібератак проводиться віддалено, дуже часто з території інших країн. Для підвищення ефективності боротьби з такими злочинами доцільною буде міжнародна співпраця у сфері кібербезпеки. Наприклад, Інтерпол відкрив у Сінгапурі центр інновацій з пошуку злочинців в Інтернеті та захисту інформаційного простору. У цьому центрі будуть працювати понад 100 експертів з більш ніж 50 країн. Крім того, для підвищення ефективності протидії кіберзлочинності, Інтерпол планує активно залучати і представників приватного сектору, які працюють у сфері цифрових технологій. Щодо нашої держави то значним проривом у цій області стала заява між Україною і Сінгапуром підписана 29 жовтня 2018 р. міністрами внутрішніх справ цих країн.

Висновок. Для ефективної протидії кіберзлочинності окремих відомчих ініціатив вже недостатньо. Потрібна чітка централізована координація зусиль для забезпечення злагодженої взаємодії усіх зацікавлених суб'єктів. Також потрібно визначити основні пріоритети розвитку державних структур по боротьбі з кіберзлочинністю такі як: реорганізація та удосконалення законодавчої і нормативно-правової бази; створення єдиного інформаційного простору в загальній та організація і удосконалення динамічної взаємодії із зарубіжними законодавчими та державними органами; запровадження сучасних новітніх інформаційних технологій в органи державної влади, технічна підготовка, перепідготовка та підвищення кваліфікації фахівців по боротьбі з кіберзлочинністю.

Одержано 01.11.2018

УДК 343.346.8:004.056.53

Олександр Ігорович ГОНЧАРЕНКО,
слухач магістратури факультету № 1
Донецького юридичного інституту внутрішніх справ;
ORCID: https://orcid.org/0000-0003-1971-4057

ПРАВООХОРОННА ДІЯЛЬНІСТЬ ЩОДО ПОПЕРЕДЖЕННЯ КІБЕРЗЛОЧИНІВ

Останнім часом майже усі політичні та суспільні процеси тісно пов’язані з інформаційним простором та інформаційними технологіями, на ряду з цим, кількість кіберзлочинів та спроб їх вчинення зростає.

Відповідно до п. 3 ч. 1 ст. 2 Закону України «Про Національну поліцію» одним з завдань національної поліції є протидія злочинності, що передбачає виконання комплексу дій з виявлення, попередження та розкриття злочинів [1].

Питання протидії кіберзлочинам, їх виявлення та попередження у наш час набирає все більшої актуальності, через велику кількість атак, як на промислових гігантів, так і на рядових користувачів мережі Інтернет. Чинною Стратегією кібербезпеки України на Національну поліцію України покладено обов'язки з забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі [2].

Попередження кіберзлочинів як вид превентивних заходів потребує розроблення гнучкої моделі комплексу методів та засобів з виявлення, попередження інцидентів та швидкісного інформування об'єктів атак, а також широкого загалу населення.

Одним з найважливіших кроків, на нашу думку, є підвищення обізнаності працівників правоохоронних органів, представників приватного сектору і потенційних жертв про кіберзлочинність та надання відповідних консультацій відносно зменшення їх віктимності.

Всеукраїнське соціологічне дослідження, проведене Інститутом соціології НАН України в 2009 році, виявило тривожні тенденції: понад 28% опитуваних дітей готові надіслати свої фотокартки незнайомцям у соціальних мережах, 17% без коливань діляться персональною інформацією, 22% дітей періодично потрапляють на сайти для дорослих, 28% дітей, побачивши в Інтернеті рекламу алкоголю або куріння, хоча б один раз спробували їх купити, а 11% − спробували купувати наркотики, близько 14% опитуваних час від часу відправляють платні SMS за бонуси в онлайн-іграх і не звертають увагу на вартість послуги.

Лише у 18% випадків дорослі перевіряють, які сайти відвідує дитина, тільки 11% батьків знають про такі онлайн-загрози, як «дорослий» контент, азартні ігри, онлайн-насилля та кіберзлочинність [3].

За результатами дослідження «Майкрософт Україна» про рівень комп'ютерної безпеки в Україні, проведеного у 2012 р. в Києві, 92% українців недостатньо обізнані про кіберзагрози. У більшості українців легко виманити пароль від пошти чи спонукати дати доступ до власної інформації у соціальній мережі та тільки 8% розуміють, як можна захиститися від таких кіберзагроз як фішинг, крадіжки особистих даних, тощо. Саме соціальна інженерія сьогодні стає основним джерелом загроз у мережі. Тільки 30% респондентів опікується своєю репутацією в Інтернеті, третина користувачів, у яких є діти, майже нічого не знають про загрози в мережі.

Також критично вразливі для кіберзлочинів користувачі, старші за 49 років – вони нічого не роблять для того, аби захиститися від кіберзагроз [4].

Соціологічне дослідження проведене, навесні 2017 року 63% дорослого населення України є постійними користувачами мережі Інтернет. Найбільш популярним є вихід у Інтернет через домашній стаціонарний комп'ютер або ноутбук 54%, хоча сьогодні вже 42% дорослого населення в Україні хоч раз на місяць користуються Інтернетом на мобільних пристроях (перш за все на смартфонах).

Як свідчить практика, в чинному законодавстві України існують прогалини щодо регулювання питань відносно протидії кіберзлочинності. Виходячи з цього, для забезпечення ефективної правоохоронної діяльності щодо попередження кіберзлочинів необхідно:

Створити умови для забезпечення постійного розвитку внутрішньодержавної правової бази у сфері обігу комп'ютерної інформації, яка повинна відповідати вимогам сьогодення та бути адаптованою до норм міжнародного права. Особливої уваги потрібно приділяти удосконаленню та узгодженню кримінального та кримінально-процесуального законодавства, пов'язаного з кваліфікацією, виявленням та розслідуванням кіберзлочинів. Слід також вирішити правові питання з приводу розголошення провайдерами інформації про користувачів на запит правоохоронних органів та можливості використання такої інформації як доказу тощо.

В свою чергу, суб'єкти інформаційного обороту повинні забезпечувати відповідну систему фізичного і технічного захисту комп'ютерної інформації.

На державному рівні доцільно розробити спеціальні системи захисту комп'ютерної інформації загальнонаціонального значення та створити правове підґрунтя для їх функціонування. При цьому необхідно передбачити належне державно-правове регулювання систем захисту, з метою недопущення обмеження прав і законних інтересів фізичних та юридичних осіб.

Висновок: Для попередження кіберзлочинів необхідно постійно проводити моніторинг інформаційних загроз, ґрунтовні дослідження функціонування та розвитку кіберзлочинності. Не останнє місце також повинно займати спеціалізоване правове виховання суб'єктів інформаційного обороту та користувачів комп'ютерної техніки.

Список бібліографічних посилань

1. Про Національну поліцію : закон України від 02.07.2015 № 580-VIII // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/580-19 (дата звернення: 20.10.2018).

2. Стратегія кібербезпеки України : указ Президента України від 15 березня 2016 року № 96/2016 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 23.10.2018).

3. Безпека дітей в Інтернеті // Міністерство освіти і науки України. URL: https://mon.gov.ua/ua/osvita/pozashkilna-osvita/vihovna-robota-ta-zahist-prav-ditini/bezpeka-ditej-v-interneti (дата звернення: 23.10.2018).

4. 92% українців не знають як захистись в Інтернеті. А діти вже знають. Вони дивляться мультфільм // Mama_ua. 07 лютого 2012 р. URL: http://mamaua.blogspot.com/2012/02/92.html (дата звернення: 23.10.2018).

Одержано 02.11.2018

УДК 343.431

Денис Олександрович ГРИЩЕНКО,
старший викладач кафедри кібербезпеки факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ;
Ярослав Віталійович ОСІПОВ,
курсант 3 курсу групи Ф4-302 факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ

ТОРГІВЛЯ ЛЮДЬМИ, ЯК КІБЕРЗЛОЧИН

Торгівля людьми є тяжким злочином проти людства, що спустошує життя приблизно 45,8 мільйона людей у світі сьогодні. Багато хто розуміє, що сучасне рабство було знято з нашого світу минулого століття з запереченням У. Вілберфорса, Авраама Лінкольна та багатьох, хто стояв за їхніми боками. Однак торгівля людьми все ще мешкає серед нас і зростає з тривогою. Справді, сьогодні в рабстві більше людей, ніж у той час, коли ми вважали, що торгівля людьми залишила нас. У системах нашого сучасного суспільства існують різні фактори еволюції, які сприяли зростанню цієї біди проти людства. Зростання Інтернету та, особливо, «Dark Web» дають можливість торговцям людьми скористатися своїм злочином з більшою легкістю у сучасному світі.

Торгівлю людьми, Організація Об'єднаних Націй визначає «торгівлю людьми як вербування, перевезення, передачу, приховування чи отримання людей шляхом загрози або застосування сили або інших форм примусу, викрадення, шахрайства, обману, зловживання владою або положенням вразливості або надання або отримання платежів або вигод для досягнення згоди особи, яка контролює іншу особу, з метою експлуатації. Експлуатація повинна включати, як мінімум, експлуатацію проституції інших осіб або інших форм сексуальної експлуатації, примусової праці або служб, рабства або практики, подібних до рабства, служби або вилученні органу». Торгівля людьми є злочинною діяльністю, яка часто має високоорганізований характер, часто перетинає національні кордони та законодавчу сферу. Торговці людьми керують цим прибутковим бізнесом, використовуючи найсучасніші технології, щоб приховати свою злочинну діяльність, з невеликим побоюванням попастися.