УДК 343.346.8:004.056.53

В.М. Струков, В.В. Торяник

Харківський національний університет внутрішніх справ, Харків

ПРОФІЛАКТИКА КІБЕРЗЛОЧИНІВ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

У роботі розглянуті соціальні підґрунтя кіберзлочинів в Україні, проаналізовані місце та роль кіберзлочинності у контексті інформаційної безпеки держави. За результатами статистичних досліджень виявлені та структуровані уразливі щодо кіберзлочинів категорії населення. Розроблені програми освітніх, організаційних та законодавчих напрямів діяльності для профілактики кіберзлочинів як вагомого чинника забезпечення інформаційної безпеки України. Запропоновані форми практичної реалізації цих програм у рамках діяльності Юридичної клініки Харківського національного університету внутрішніх справ.

Ключові слова: *інформаційна безпека держави, Інтернет, категорії населення, інформаційна обізнаність, насильство, кіберзлочин, освіта, профілактика.*

Кіберзлочинність та інформаційна безпека держави

Низка сучасних та надсучасних противоправних тенденцій у сфері інформаційних відносин та новітній прояв кіберзлочинності – кібертероризм становлять загрозу як окремим громадянам, так і інформаційній безпеці держави. Інформаційна безпека є невід'ємною складовою національної безпеки і важливою самостійною сферою забезпечення національної безпеки [1]. У доктрині інформаційної безпеки України [2] окремою загрозою визначено лише прояви комп'ютерної злочинності та тероризму, що загрожують функціонуванню національних інформаційно-телекомунікаційних систем. Але в сучасних реаліях глибокого латентного проникнення кіберзлочинності у суспільне та державне життя комп'ютерні злочини є складовою всіх загроз негативного інформаційного впливу.

Фундаментальною умовою ефективної протидії кібезлочинності є достатній рівень інформаційно-правової культури суспільства та професійної підготовки фахівців із забезпечення інформаційної безпеки.

Інформаційна безпека згідно законодавства України визначена як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через [3, 4]:

- неповноту, невчасність та невірогідність інформації, що використовується;
- негативний інформаційний вплив;
- негативні наслідки застосування інформаційних технологій;
- несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

Загроза інформаційній безпеці України - це сукупність умов та чинників, які становлять небезпеку інтересам держави, суспільства і особи через негативний інформаційний вплив на свідомість та поведінку громадян, інформаційні ресурси та інформаційно-технічну інфраструктуру. Згідно Закону України «Про основи національної безпеки України» основними інформаційними загрозами національній безпеці є [5]:

- обмеження доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу, передбачену законом таємницю;
- поширення недостовірної, неповної або упередженої інформації

Існує багато технологій здійснення негативного впливу на інформаційну сферу життєдіяльності суспільства. Вони можуть застосовуватись спецслужбами, терористичними та екстремістськими організаціями та угрупованнями, кримінальними структурами, тощо. І можливість такого використання видається досить реальною [6].

Соціальне підґрунтя кіберзлочинів в Україні

Аудиторія користувачів всесвітньої мережі Інтернет в Україні динамічно розширюється, переважно за рахунок молоді. Діти та підлітки повністю не усвідомлюють реальні загрози віртуального простору. Відомі факти залучення підлітків через Інтернет до сексуального насильництва, до екстремістських формувань [7]. Всеукраїнське соціологічне дослідження, проведене Інститутом соціології НАН України в 2009 році, виявило тривожні тенденції: понад 28% опитуваних дітей готові надіслати свої фотокартки незнайомцям у Мережі, 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 відві-

дує дитина, тільки 11% батьків знають про такі онлайн-загрози, як "дорослий" контент, азартні ігри, онлайн-насилля та кіберзлочинність [8].

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 і 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 [9]. За даними системи моніторингу та швидкого реагування на комп'ютерні загрози Kaspersky Security Network у березні цього року на території Росії у середньому за день було зафіксовано понад 800 тис. спрацювань системи захисту дітей від небажаного контенту в Інтернеті [10].

Напрями та форми профілактики кіберзлочинності

В сучасних умовах нагальною стає проблема координації діяльності правоохоронних структур та правового унормування зон відповідальності відомств, процедур взаємодії та засобів комплексного реагування на загрози кібербезпеці держави, а також значної роботи із попередження таких злочинів [11].

В Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України" [12].

Враховуючи наведене доцільна розробка наступних напрямів [13, 14]:

- поширення інформації щодо правил безпечного користування мережею Інтернет;
- внесення теми онлайн-безпеки у шкільну програму для дітей віком від 7 до 14 років, а також у програму навчання та підвищення кваліфікації вчителів;
- вивчення та використовування міжнародного досвіду боротьбі з кіберзлочинністю;
- визначення поняття "дитяча порнографія" у законодавстві України;
- передбачити законодавством України покарання за виробництво і володіння матеріалами, що характеризуються як дитяча порнографія;
- вдосконаленя ресурсної бази підрозділів МВС щодо боротьби та запобігання кіберзлочинів;
- на законодавчому рівні затвердити процедуру блокування Інтернет-ресурсів, що містять інформацію в порушення українського законодавства;
- створення зони довіри в українському сегменті Інтернету.

Організація дослідження та протидії кіберзлочинності у соціальній сфері у ХНУВС

У 2012 р. при Юридичній клініці ХНУВС за ініціативою авторів на науково-методичній базі кафедри інформаційних комунікацій, захисту інформації та документознавства ННІПМК ХНУВС було запропоновано створити Відділ дослідження та протидії кіберзлочинності у соціальній сфері. Передбачаються такі форми роботи відділу.

Місія Відділу:

- навчання та навчальна практика у галузі інформаційної безпеки студентів старших курсів ХНУВС;
- попередження кіберзлочинності через безкоштовну фахову допомогу підліткам та їх батькам;
- цільова реклама освітянської, наукової та правоохоронної діяльності ХНУВС;
- забезпечення конкурентоспроможності ХНУВС у вступних кампаніях.

Завдання Відділу:

- наукові дослідження у галузі кіберзлочинності;
- співробітництво з Юридичною клінікою, Гендерним центром та Зеленою кімнатою ХНУВС;
- впровадження в навчальний процес елементів практичної підготовки правоохоронця;
- надання допомоги населенню у галузі інформаційної безпеки;
- формування інформаційної культури громадян через профільну освіту;
- співробітництво ХНУВС з іншими навчальними закладами, правоохоронними органами, органами юстиції, державної влади та самоврядування, з громадськими організаціями щодо запобігання кіберзлочинності;
- проведення заходів з освіти населення у галузі безпеки інформаційних технологій;
- забезпечення можливості спілкування студентів під час навчального процесу з фахівцями-практиками судових та правоохоронних органів, інших державних органів та органів місцевого самоврядування з питань їх діяльності;
- створення ефективного механізму обміну інформацією між населенням, засобами масової інформації та Відділом;
- проведення правоосвітніх, праворозяснювальних та інших навчально-практичних заходів;
- надання безоплатної технічної та правової допомоги з питань захисту прав і свобод людини у кіберпросторі відповідно до чинного законодавства України.

Принципи діяльності відділу:

- поваги до права, справедливості, людської гідності;
- спрямованості на захист прав і свобод людини;

- гуманізму;
- законності та верховенства права;
- об'єктивності;
- безоплатності надання правової допомоги;
- конфіденційності;
- компетентності.

Зараз накопичується первинний досвід роботи та заплановані власні соціальні дослідження щодо обізнаності категорій населення у галузі інформаційної безпеки.

Висновки

В сучасних реаліях комп'ютерні злочини є складовою всіх загроз негативного інформаційного впливу.

Умовою ефективної протидії кібезлочинності є достатній рівень інформаційно-правової культури суспільства та професійної підготовки фахівців із інформаційної безпеки.

Інтернет в Україні динамічно розвивається, більшість користувачів Мережі не усвідомлюють реальні загрози віртуального простору.

Нагальною стає проблема координації діяльності правоохоронних структур та процедур взаємодії і засобів комплексного реагування на кіберзагрози, а також значної роботи із попередження таких злочинів.

В Україні органом, на який покладаються повноваження щодо протидії кіберзлочинності є МВС.

Для виконання науково-дослідних та профілактичних заходів при Юридичній клініці ХНУВС запропоновано створити Відділ дослідження та протидії кіберзлочинності у соціальній сфері.

Список літератури

1. Тихомиров О.О. Протидія кіберзлочинності як складова державного забезпечення інформаційної безпеки / О.О. Тихомиров // Актуальні проблеми управління інформаційною безпекою держави : зб. матНПК, (Київ, 22 берез. 2011 р.).- Ч. 2. – К.: Вид-во НА СБ України, 2011. – С. 78-82.

2. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 липня 2009 року № 514/2009 [Електронний ресурс]. – Режим доступу : http://zakon1. rada. gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009.

3. Закон України «Про інформацію» // ВВР. – 2003. – № 48.

4. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» // ВВР. – 2007. – № 12.

5. Закон України «Про основи національної безпеки України» // ВВР. – 2006. – № 14.

6. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи / В. Петрик // Юридичний журнал. – 2009. – № 5. – С. 45–46 (www:justinian.com.ua).

7. Дети и Интернет, как защитить ребенка от асоциальных сайтов? [Електронний ресурс]. – Режим доступу: http://www.svobodanews.ru/ content/transcript/462683.html.

8. Безпека дітей в Інтернеті [Електронний ресурс]. – Режим доступу: http://www.mon.gov.ua /index.php/ua/117-pozashkilna-osvita-vikhovna-robota-ta-zakhist-prav-ditini.

9. 92% українців недостатньо обізнані про кіберзагрози [Електронний ресурс]. – Режим доступу: http://www.onlandia. org.ua/SocialAction/Details/7.

10. Kaspersky Security Network [Електронний ресурс]. – Режим доступу: http://www. kaspersky.ru/downloads/pdf/ kaspersky_security_network.pdf.

11. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка [Електронний ресурс]. – Режим доступу: http:// www.niss.gov.ua/articles/454.

12. Литовченко И.В. И др. Дети в интернете: как научить безопасности в виртуальном мире / И.В. Литовченко и др.. – К.: Изд. дом "Аванпост-Прим", 2010. – 234 с.

13. Про внесення зміни до ЗУ "Про ратифікацію Конвенції про кіберзлочинність" (ВВР), 2011, N 5, ст.32) [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov. ua/laws/ show/2532-17

14. Региональный обзор об изображениях сексуального насилия над детьми посредством использования информационных и коммуникационных технологий в Беларуси, Молдавии, России и Украине [Електронний ресурс]. – Режим доступу: www.ecpat.net.

Надійшла до редколегії 31.01.2013

Рецензент: д-р техн. наук, проф. О.А. Серков, Національний технічний університет «ХПІ», Харків.

ПРОФИЛАКТИКА КИБЕРПРЕСТУПЛЕНИЙ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

В.М. Струков, В.В. Торяник

В работе рассмотрены социальные основы киберпреступлений в Украине, проанализированы место и роль киберпреступности в контексте информационной безопасности государства. По результатам статистических исследований выявлены и структурированы уязвимые в отношении киберпреступлений категории населения. Разработаны программы образовательных, организационных и законодательных направлений деятельности для профилактики киберпреступлений как весомого фактора обеспечения информацийной безопасности Украины. Предложены формы практической реализации этих программ в рамках деятельности Юридической клиники Харьковского национального университета внутренних дел.

Ключевые слова: *Информационная безопасность государства, Интернет, категории населения, информационная осведомленность, насилие, киберпреступление, образование, профилактика.*

PREVENTION OF CYBER CRIME IN THE CONTEXT OF THE STATE INFORMATION SECURITY

V.M. Strukov, V.V. Toryanik

In this work the social foundations of cyber crime in Ukraine, analyzed the role and place of cybercrime in the context of information security. According to statistical studies identified and mapped vulnerable to cyber population. The programs of educational, organizational and legislative activities for the prevention of cyber crime as a significant factor in ensuring the security of Ukraine information . Proposed form of the implementation of these programs as part of the Legal Clinic of Kharkiv National University of Internal Affairs.

Keywords*: Information security of the state, the Internet, the categories of the population, information awareness, violence, cyber crime, education, prevention.*