Шумська В. Р.,
студентка 5 курсу,
8 групи, факультету адвокатури
Національного юридичного університету
імені Ярослава Мудрого

СУЧАСНИЙ СТАН ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ: ОКРЕМІ ПИТАННЯ ЗАКОНОДАВЧОГО РЕГУЛЮВАННЯ

Ключові слова: кіберзлочинність, кібербезпека, кіберпростір, Інтернет.
Keywords: cybercrime, cyber security, cyber space, Internet.

Анотація: у тезах в загальному вигляді проаналізовано світові збитки від кіберзлочинності, висвітлено актуальність кібербезпеки в світовому контексті, окреслено законодавче підґрунтя у сфері кібербезпеки України, наведено деякі недоліки українського законодавства з цих питань, проаналізовано систему органів в Україні, на яких покладено обов'язки здійснення кіберполітики.

Abstract: the thesis presents the generally analyzed global losses resulting from cybercrime, importance of the questions concerning cyber security in the world, the state of Ukrainian law regulation in the sphere of cyber security and problem areas of it, the range of the Ukrainian authorities in the field of cyber-policy.

21 століття — це вік нестримної інформаційної еволюції. Важко навіть на мить уявити, щоб сталося з життям на планеті, якщо б перестали функціонувати всі комп'ютери, інші електронні пристрої та Інтернет... Адже весь світ, життєдіяльність та благополуччя людей

сьогодні повністю залежать від технічних винаходів людства. Широке включення комп'ютерних технологій до зростаючої з кожним днем кількості сфер діяльності суспільства та держави наближає Україну не лише до світових стандартів та тенденцій, а й до ряду негативних наслідків. Зокрема, мова йде про те, що розвиток технологій створив сприятливе середовище для існування такого явища, як кіберзлочинність. Розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації – це далеко не повний перелік кіберзлочинів.

Деякі науковці відзначають, що висока соціальна небезпека кіберзлочинності випливає, насамперед, із суспільних відносин, яким вона загрожує, а також з її транснаціонального та організованого характеру [1, с. 4] Як влучно зазначає Горянінов К. К. ця особливість багатьох кіберзлочинів зумовлює постійне ускладнення в міжнародному масштабі норм та правил, пов'язаних з виявленням та ідентифікацією злочинців, проведенням розслідувань та судових переслідувань за фактами транскордонних комп'ютерних злочинів [2, с. 245].

Міжнародне співтовариство вважає за потрібне приділяти питанням кібербезпеки значну увагу. Це підтверджується, наприклад, існуванням міжнародної конференції з кібербезпеки (International conference on cyber security), яка проводиться кожні 18 місяців. Найближча конференція відбудеться в січні 2018 року в Нью-Йорку, США. Така конференція слугує платформою для обміну досвідом у сфері кіберборотьби та кібербезпеки між світовими лідерами та експертами у даній сфері.

Кіберпростір як глобальне явище вимагатиме глобальних запобіжних заходів. Врахування ціни кіберзлочинів при побудові інформаційної моделі злочинності сприятиме визначенню найбільш криміналізованих сфер, і як наслідок ефективному запобіганню злочинним проявам кіберзлочинності у сучасному суспільстві [3, с. 60].

За даними Федерального бюро розслідувань (США) збитки від одного злочину, який вчиняється у кіберпросторі за допомогою комп'ютера, становлять у середньому 500 тис. дол., тобто в 20 разів більше, ніж при використанні інших злочинних методів. Загальна сума збитків від «електронного грабежу» щорічно становить близько 600 млн. дол [4, с. 9].

Варто зазначити, що європейську спільноту питання кіберзлочинності почали переймати ще в кінці 20 ст. Зокрема, у 1986 р. у Парижі групою експертів Організації економічного співробітництва і розвитку було вперше дано кримінологічне визначення комп'ютерного злочину, під яким розумілася будь-яка незаконна, неетична або недозволена поведінка, що стосується автоматизованої обробки або передачі даних. Після чого почалася всесвітня боротьба з кібертероризмом [4, с. 17].

Сучасний кіберпростір і ті процеси, які нині відбуваються в ньому, значно нагадують проблеми часів холодної війни, для якої були характерні високі рівні латентних загострень на міжнародній арені, непрямі методи боротьби (передусім активізація розвідувальної діяльності всіх сторін глобального протистояння), перенесення конфліктів на територію третіх країн (наприклад у формі протистоянь за сфери впливу) та гонка озброєнь (у даному випадку – «кіберозброєнь») [5].

В Україні механізми забезпечення кібербезпеки держави перебувають на етапі становленні. Останній час в засобах масової інформації досить часто можна почути про одиничні кіберзлочини, а, також, випадки масових хакерських атак на території українського кіберпростору. Починаючи з червня цього року в Україні сталося декілька хвиль масштабник кібератак, від яких найбільше постраждали комп'ютерні мережі центральних органів влади. На сайті Департаменту кіберполіції Національної поліції в Україні зазначається: «Департамент кіберполіції попереджує про новий виток протистояння в кібернетичному просторі. Злочинці продовжують вчиняти дії, направлені на дестабілізацію комп'ютерних систем і доступу громадян до Інтернет-мережі, державних установ, фінансових та ділових центрів, з метою створення безладу та хаосу в житті країн, які покладаються на сучасні технології у повсякденному житті. Хакери поступово відходять від схеми зараження кожного окремого комп'ютера, та здійснюють атаки на серверне обладнання компаній розробників, з метою використання їх в якості «служби доставки» шкідливого коду, який вбудовують в чергове оновлення популярних програмних продуктів (Supply chain attacks(ланцюжок поставок)).

Користувачі, довіряючи таким програмам, навіть не помічають, що їх персональні дані та керування комп'ютером належать невідомим, одразу після встановлення чергового «патчу». Вірус NotPetya (Diskoder.C) який уразив Україну 27 червня 2017 року, показав, наскільки сильними можуть бути ці типи нападів.»

Концептуально проблема розбудови ефективних механізмів кібербезпеки Української держави походить від відсутності законодавчо визначених термінів, що описують цю сферу [5]. Зокрема, в нормативно-правових документах України терміни з префіксом «кібер-» практично не зустрічаються. Навпаки, у багатьох нормативно-правових актах у цьому контексті застосовуються словосполучення «злочини у сфері використання ЕОМ…».

Правове забезпечення цієї проблеми потребує вдосконалення. Позитивним зрушенням у цьому контексті є підписання Президентом України Закону України «Про основні засади забезпечення кібербезпеки України», яким визначаються основні завдання кіберполітики. Набрання чинності цим законом відбудеться 09.05.2018.

Важливим для національного кіберпростіру є Указ Президента України яким приведено в дію рішення РНБО від 27.01.2016 «Про стратегію кібербезпеки України». А ще у 2005 році Україна ратифікувала Конвенцію про кіберзлочинність.

Щодо механізмів практичного забезпечення кібербезпеки в державі, то в Україні такі функції покладено на декілька відомств. Перш за все, у складі Служби безпеки України діє Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки.

Важливу роль в реалізації заходів боротьби та запобігання кіберзлочинності відіграє Департамент кіберполіції Національної поліції в Україні, до завдань якого належать реалізація державної політики в сфері протидії злочинності, завчасне інформування населення про появу нових кіберзлочинців, впровадження програмних засобів для систематизації кіберінцидентів, реагування на запити зарубіжних партнерів.

Державна служба спеціального зв'язку та захисту інформації відповідно до своїх завдань безпосередньо включена до забезпечення кібербезпеки держави.

У структурі Міністерства оборони України принаймні два основних управління відповідають за питання, що пов'язані з кібербезпекою держави. Так, в Апараті МОУ цією діяльністю опікується Управління інформаційних технологій, що підпорядковане заступнику Міністра оборони України – керівнику апарату. В Генеральному штабі Збройних сил України функціонує Головне управління зв'язку та інформаційних систем.

Незважаючи на подібну розгалуженість відомств, що задіяні в системі забезпечення кібербезпеки держави, вітчизняній кібербезпековій сфері притаманні певні стратегічні проблеми, які все ще потребують вирішення [5].

Отже, національна безпека України, її економічне процвітання та соціальне благополуччя населення в цілому та кожної людини все більше залежать від урегульованості питань інформаційної безпеки та захищенності на державному рівні. За останні роки в Україні спостерігається позитивне пожвавлення роботи із розроблення та впровадження стратегій боротьби з кіберзлочинністю.

Список використаних джерел:

1. Дремлюга Р. И. Интернет-преступность : автореф. дис. на соискание ученой степени канд. юрид. наук : спец. 12.00.08 "Уголовное право и криминология; Уголовно-исполнительное право" / Р. И. Дремлюга. – Владивосток, 2007. – 26 с.
2. Горяинов К. К. Транснациональная преступность: проблемы и пути решения / К. К. Горяинов , А. П. Исеченко, Л. В. Кондратюк. – М. : ИНФРА–М, 1997. – 386 с.
3. Сметаніна Н. В. Національний і міжнародний досвід визначення та розрахунку ціни кіберзлочинності / Н. В. Сметаніна // Міжнародні стандарти з кібербезпеки та їх застосування в Україні : матеріали «круглого столу» (м. Харків, 19 квіт. 2016 р.). – Харків, 2016. – С. 59–61. – Режим доступу : http://dspace.nlu.edu.ua/handle/123456789/10682 .
4. Ищенко Е. П. Виртуальный криминал / Е. П. Ищенко. – М. : Проспект, 2011. – 232 с.
5. Дубов Д. В. Стратегічні аспекти кібербезпеки України / Д. В. Дубов // [Електронний ресурс]. – Режим доступу: http://sp.niss.gov.ua/content/articles/files/16-1446038514.pdf .

Міністерство освіти і науки України

Національний юридичний університет
імені Ярослава Мудрого

ЗЛОЧИННІСТЬ У ГЛОБАЛІЗОВАНОМУ СВІТІ

Матеріали XVI Всеукраїнської кримінологічної конференції для студентів, аспірантів та молодих вчених

(м. Харків, 12 грудня 2017 р.)

За загальною редакцією
професора *А. П. Гетьмана* і професора *Б. М. Головкіна*

Харків
«Право»
2017

УДК 343.9.01:005.44
ББК 67.61я431
З-68

З-68 **Злочинність** у глобалізованому світі : матеріали XVI Всеукр. кримінол. конф. для студентів, аспірантів та молодих вчених (м. Харків, 12 груд. 2017 р.) / за заг. ред. А. П. Гетьмана і Б. М. Головкіна. – Харків : Право, 2017. – 420 с.

ISBN 978-966-937-307-6

ISBN 978-966-937-307-6