УДК 343.98, 343.34, 343:004.9

О. В. ОРЛОВ, Ю. М. ОНИЩЕНКО

АКТУАЛЬНІ НАПРЯМИ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

***Р**озглянуто ключові проблеми вітчизняного законодавства у сфері забезпечення кібернетичної безпеки держави. Розглянуто основні напрями діяльності органів державної влади в системі забезпечення кібернетичної безпеки України, їх використання у відповідних зонах та процедур взаємодії відповідно до нормативної бази.*

Ключові слова: кібернетична безпека, кіберпростір, кібернапад, кіберзагроза, кіберзлочин.

***T**he paper considers key problems of home legislation in the field of ensuring cybernetic safety of the state. Basic areas of activity of public authorities in the system of securing the cybernetic safety of Ukraine are discussed along with their application in the appropriate zones and cooperation procedures according to the legal framework.*

Key words: cybernetic security, cyberspace, cyber attack, cyber threat, cyber crime.

Широке використання сучасних інформаційних технологій у суспільстві та державних структурах висуває вирішення проблем інформаційної злочинності якості однієї з основних у рамках державного регулювання системи національної безпеки. Окрім безпосередньої шкоди від можливих випадків несанкціонованого доступу до приватної інформації або інформації з обмеженим доступом її знищення або модифікації, інформатизація суспільства може перетворитися на джерело серйозної загрози безпеці держави і правам людини. На сьогодні боротьба зі злочинами у сфері інформаційних технологій є однією з найбільш актуальних проблем у всьому світі. Зростаюча кількість кіберзлочинів, постійне вдосконалення інформаційних технологій і, як наслідок, нові можливості "вдосконалення" інструментів їх скоєння створюють погрози для глобальних інформаційних мереж і суспільства в цілому. Уже нікого не дивують щоденні публікації засобів масової інформації про нові факти судових розглядів у справах про кіберзлочини, зокрема у справах про шахрайства в галузі інформаційних технологій.

За останні 10 років не раз ставало питання про вдосконалення законодавства, яке регулює сферу використання сучасних комп'ютерних технологій. Багато фахівців, зокрема Ю. Батурін, В. Вехов, В. Голубев, М. Діхтяренко, Б. Романюк, О. Снегірьов, що займаються даною проблематикою, періодично пропонували різні поправки і доповнення до існуючих норм, але на даний час вони не реалізовані.

В останній час депутати пропонують доповнити КК статтями про злочини в комп'ютерній сфері. За кіберзлочини українців хочуть позбавляти волі строком від трьох до шести років. Відповідні санкції прописані в законопроекті про внесення змін у Кримінальний Кодекс України (щодо доповнення статтями, за якими настає кримінальна відповідальність у комп'ютерній сфері).

Під категорію комп'ютерних злочинів підпадають: спроба впливу або вплив на обробку даних шляхом навмисного проектування програми, використання неправильних або незавершених даних, несанкціонованого використання даних.

Крім того, каратиметься спроба підробки даних, використання підроблених даних або заміщення даних підробленими; спроба незаконного вилучення, блокування, стирання, зміни даних; спроба затримки обробки даних, спрямована проти підприємства, державної влади; викрадення даних, захищених від несанкціонованого доступу, не призначених для правопорушника.

Згідно з пропозиціями депутатів, відповідальність за кіберзлочини передбачає позбавлення волі строком до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до двох років.

За вчинення тих самих дій повторно або за попередньою змовою групою осіб пропонують карати позбавленням волі на строк від трьох до шести років [3].

Мета статті – розглянути ознаки кіберзлочинності в Україні, дати поняття кіберзлочинності, проаналізувати роботу служб і відомств для протидії кіберзлочинності та надати пропозиції щодо створення нових органів і організацій для координації боротьби з кіберзлочинністю.

Загальновідомо, що наша країна є одним з лідерів за кількістю кібератак у всьому світі. Україна опинилася на четвертому місці після Росії, Тайваню і Німеччини [7]. Це відбувається тому, що українські закони, які регулюють питання кіберпростору і злочинних посягань у ньому, недостатньо розроблені та реалізовані. У зв'язку з цим зазначимо, що в Україні в якості кіберзлочинів кримінальним законом передбачено і закріплено в окремому Розділі XVI Кримінального кодексу України суспільно небезпечні діяння "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" [6]. Кіберзлочини можна класифікувати на два види: традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та інтернету (шахрайство з використанням ЕОМ, незаконне збирання відомостей, що становлять комерційну таємницю, шляхом несанкціонованого доступу до комп'ютерної інформації тощо), та нові злочини, що стали можливі завдяки новітнім комп'ютерним технологіям.

У Кримінальному кодексі України станом на 10 липня 2011 р. правовий розділ XVI КК містить шість статей. Найчастіше з використанням комп'ютера та інтернету вчиняються такі традиційні злочини: порушення авторського права і суміжних прав (ст. 176); шахрайство (ст. 190); незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення (ст. 200); ухилення від сплати податків,

зборів (обов'язкових платежів) (ст. 212); ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301); незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231) [6].

Розвиток комп'ютерних технологій надав можливість здійснення кіберзлочинів практично безкарно, оскільки в даний час кримінальне законодавство не адаптоване до нового вигляду злочинів у сфері інформаційних технологій.

Для порівняння можна навести кримінальне законодавство, що регламентує відповідальність у сфері кіберзлочинності Японії, яке постійно удосконалюється і модифікується. Так, наприклад, неодноразово мінялася частина кримінально-правових норм, які регулюють кіберзлочини. Останні зміни мали місце в 2011 р. Верхня палата парламенту Японії ухвалила доповнення до Кримінального кодексу, згідно з яким відповідальність за вчинення кіберзлочинів стала більш суворою. За створення і розповсюдження комп'ютерних вірусів покарання може скласти до трьох років тюрми. За скоєння аналогічних злочинів доповнення передбачають також штраф у розмірі до 500 тис. ієн (більше 6200 дол. США). Запроваджено покарання і за новий склад злочину – розповсюдження порнографії по електронній пошті [8].

У зв'язку з ратифікацією Україною Конвенції про кіберзлочинність 7 вересня 2005 р. вважається за доцільне вживати термін кіберзлочини [1].

Конвенція містить норми, здатні доповнити і поліпшити законодавчу базу нашої держави в цій сфері.

Конвенція про кіберзлочинність направлена на регулювання трьох основних питань:

– кримінально-правової характеристики злочинів у сфері комп'ютерної інформації;

– кримінально-процесуальних аспектів боротьби зі злочинністю, направлених на забезпечення збирання доказів при розслідуванні комп'ютерних злочинів;

– міжнародної співпраці в кримінально-процесуальній діяльності, яка направлена на збирання доказів скоєння таких злочинів за кордоном.

Конвенція про кіберзлочинність називає п'ять видів комп'ютерних злочинів: незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему, незаконне використання пристроїв комп'ютерних паролів, кодів доступу або інших подібних даних.

Конвенція про кіберзлочинність включає норми права, які держави-учасники зобов'язалися включити в національне законодавство, а також норми, що встановлюють порядок міждержавної співпраці у справі боротьби зі злочинністю у сфері високих технологій.

Виникнення даного виду злочинів вимагає використання спеціальної термінології, яка буде єдиною як для правоохоронних органів, так і для спеціалістів з інформаційних технологій (ІТ). Багато понять, що входять в ІТ-лексикон, давно використовуються в сучасному світі, наприклад такі, як кіберпростір,

кібертероризм, але підходи представників технічних і юридичних галузей науки до кожного терміну різні.

На даний момент, на етапі зростання кіберзлочинів не виведено єдиного загальновизнаного поняття кіберзлочинності. Згідно рекомендаціям експертів ООН, термін "кіберзлочинність" охоплює будь-який злочин, який може здійснюватися за допомогою комп'ютерної системи або мережі, в рамках комп'ютерної системи або мережі, проти комп'ютерної системи або мережі. Інакше кажучи, до кіберзлочинів відносяться такі суспільно небезпечні діяння, які здійснюються в кіберпросторі за допомогою або з використанням комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

Зважаючи на те, що в законодавстві відсутнє визначення запропонованих понять, як і відсутнє безпосередньо поняття "кіберзлочину", слід зазначити, що загалом об'єктом дослідження кібернетики як науки, є загальні закономірності процесів управління і передачі інформації в машинах, живих організмах і суспільстві. Тому поняття кіберпростору та кібернетичної безпеки є значно ширшими від запропонованих та не можуть обмежуватися виключно середовищем, що пов'язане з інформаційними, телекомунікаційними та інформаційно-телекомунікаційними системами [2].

Структурний аналіз злочинності у сфері комп'ютерної інформації доводить, що найбільш поширеними діяннями є: неправомірний доступ до комп'ютерної інформації, створення і поширення шкідливих програм і неліцензійного програмного забезпечення, посягання на електронно-платіжні системи, а також поширення порнографічних матеріалів за участю неповнолітніх в інтернеті.

Із-за високої латентності кіберзлочинності для встановлення дійсних масштабів її поширення потрібне використання нових методів і джерел отримання інформації. За останніми даними щороку кіберзлочинці спричиняють шкоду на суму близько 400 млрд дол. США. Ця сума включає збитки, що спричиняються в кількох сферах: від крадіжки об'єктів інтелектуальної власності до махінацій з кредитними картками [5].

Отримання і аналіз доказів у справах про злочини у сфері комп'ютерної інформації – одне з найосновніших і важко вирішуваних на практиці завдань для всіх держав. Вирішення цієї задачі вимагає не лише розробки тактики виробництва слідчих і організаційних заходів, але і наявності спеціальних знань у сфері комп'ютерної техніки і програмного забезпечення, а також внесення поправок до чинного законодавства.

Особи, що займаються розслідуванням даного роду злочинів, і працівники судової системи в більшості своїй не володіють спеціальними пізнаннями у сфері нових комп'ютерних технологій, що обумовлює помилки в кваліфікації і розслідуванні злочинів. Також причинами помилок є відсутність достатньої кількості рекомендацій і роз'яснень по розслідуванню злочинів у сфері інформаційних технологій, відсутність узагальненої судової практики по

кіберзлочинності і відсутності в правоохоронних органах необхідного числа фахівців, що знаються на сучасній техніці і здатних оперативно виявляти і розслідувати комп'ютерні злочини. У зв'язку з цим виникає завдання введення нових спеціалізацій і внесення змін до навчального плану підготовки студентів юридичних вузів, курсантів і слухачів спеціальних навчальних закладів.

Недостатня кількість комплексних досліджень і висока латентність приводять до неефективності існуючих заходів запобігання даного виду злочинів.

На відміну від всесвітньої павутини, яка не визнає національних кордонів і є за своєю природою трансграничною, національні законодавства і правоохоронні органи різних країн у своїй діяльності вимушені брати до уваги особливості кордонів, мовні, політичні, релігійні особливості, що впливають на ефективність боротьби зі злочинністю даного виду. Специфічність характеристик вимагає міждержавного підходу до протидії кіберзлочинам, ефективність якого недосяжна без міжнародної співпраці.

Необхідно також звернути увагу на те, що зарубіжні країни з кожним роком збільшують кількість служб і відомств для протидії кіберзлочинності, тому варто вивчити і перейняти їх досвід.

Наприклад, у США створені такі відомства, як Electronic Crimes Task Forces ECTF підрозділ Секретна служба США (United States Secret Service USSS), федеральне агентство США підпорядковане міністерству внутрішньої безпеки США (уведено в підпорядкування в 2003 р. до цього було підпорядковано міністерству фінансів США). Ці підрозділи створюють взаємодію між службами, правоохоронними органами (федерального рівня, рівня штату, локальними), приватним сектором, академічним співтовариством і виявляють і запобігають кіберзлочинам US Cyber Command (військовий підрозділ, який здійснює свою діяльність у кіберпросторі), United States Computer Emergency Readiness Team (Національний відділ кіберзахисту Департаменту внутрішньої безпеки США), Computer Crime and Intellectual Property Section (Відділ комп'ютерної злочинності і інтелектуальної власності), Internet police (Інтернет-поліція, мережева поліція). У Великій Британії боротьбою з кіберзлочинністю займається відділ по боротьбі з кіберзлочинами, що входить до складу Агентства по боротьбі з організованою злочинністю. У ФРН основну діяльність щодо боротьби з кіберзлочинністю здійснює Федеральна кримінальна поліція. У Франції 1 липня 2008 р. шляхом об'єднання двох спецслужб Центрального директорату загальної розвідки (RG) і Директорату стеження за територіями (DST) створено Головне управління внутрішньої розвідки Direction centrale du Renseignement interieur, DCRI. Однією з функцій даного управління є боротьба з кіберзлочинністю. В Естонії в 2006 р. створено комп'ютерну групу реагування на надзвичайні ситуації (CERT-EE). У Республіці Білорусь Управління по розкриттю злочинів у сфері високих технологій Міністерства внутрішніх справ є самостійним оперативно-розшуковим підрозділом Міністерства, безпосередньо підпорядкованим першому заступникові Міністра внутрішніх справ – начальникові головного управління кримінальної міліції.

Сьогодні в Україні на порядку денному стоїть питання про створення нових органів і організацій, що координують і здійснюють боротьбу з кіберзлочинністю, що, у свою чергу, вимагає підготовки національних кадрів, представників яких можна було б залучати и на службу в транснаціональні органи і організації, направлені на боротьбу з кіберзлочинністю.

Наказом МВС від 30 жовтня 2012 р. № 988 затверджено положення про Управління боротьби з кіберзлочинністю МВС України. Управління є самостійним структурним підрозділом у складі кримінальної міліції МВС, яке відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, у тому числі організовує і здійснює в межах компетенції і відповідно до законодавства оперативно-розшукову діяльність [8].

У Харківському університеті внутрішніх справ у 2013 р. створено факультет підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми, який здійснює таку підготовку: слідчі, що спеціалізуються на розслідуванні кіберзлочинів; оперативні працівники для підрозділів боротьби з кіберзлочинністю. Випускники факультету відповідно до напрямів підготовки та спеціалізацій отримують знання та навички, засвоюють методи та засоби, які забезпечують розкриття та протидію кіберзлочинам.

Література:

1. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 р. № 2824-IV // ВВР України. – 2006. – № 5-6. – Ст. 71.

2. Про внесення змін до Закону України "Про основи національної безпеки України" щодо кібернетичної безпеки : лист № 75 від 29.04.2013 р. Голові Комітету ВРУ з питань інформатизації та інформаційних технологій щодо проекту закону // Інтернет Асоціація України [Електронний ресурс]. – Режим доступу : http://www.inau.org.ua/52.4839.0.0.1.0.phtml.

3. За кіберзлочини українцям даватимуть шість років [Електронний ресурс]. – Режим доступу : http://tsn.ua/ukrayina/za-pidrobku-komp-yuternih-danih-ukrayincyam-svitit-6-rokiv.html.

4. Как бороться с киберпреступностью – будет решать управление МВД [Електронний ресурс]. – Режим доступа : http://jurliga.ligazakon.ua/print_news/type_news/82911.htm.

5. Кіберзлочинці щороку крадуть інформації на 400 млрд дол. [Електронний ресурс]. – Режим доступу : http://zik.ua/ua/news/2013/07/30/421804.

6. Кримінальний кодекс України від 05.01.2001 р. // ВВР України. – 2001. – № 25-26. – Ст. 131.

7. Украина – один из лидеров по количеству кибератак в мире [Електронний ресурс]. – Режим доступа : http://www.pravda.com.ua/rus/news/2013/03/8/6985180.

8. Япония ужесточает наказание за киберпреступления / Судебно-юридическая газета [Електронний ресурс]. – Режим доступа : http://sud.ua/newspaper/2011/06/29/37957-yaponiya-yzhestochaet-nakazanie-za-kiberprestypleniya.

Надійшла до редколегії 17.09.2013 р.