ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ ОРГАНАМИ ВНУТРІШНІХ СПРАВ

КРАВЦОВА Марина Олександрівна - Ад'юнкт ад'юнктури та докторантури Харківського національного університету внутрішніх справ

УДК ***343.2:343.4(477)***

В статье изложен анализ нормативно-правовых актов Украины относительно деятельности органов внутренних дел, направленных на выявление и предупреждение киберпреступности. Установлено, что в настоящее время не существует единого основного законодательного акта, который бы четко регулировал деятельность органов внутренних дел в сфере предупреждения киберпреступности. На основании проведенного анализа определено, что в результате одновременного действия нескольких нормативных актов в указанной сфере существуют несогласованности относительно заданий, функций и порядка взаимодействия подразделений органов внутренних дел; отсутствие законодательно разработанных понятий относительно предупреждения киберпреступности. Также исследованием установлено несогласованность некоторых правовых актов Украины с международными актами.

Ключові слова: кіберзлочинність, запобігання, нормативно-правове регулювання.

Інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки [1].

Проблематика правового регулювання кіберзлочинності досліджувалася такими науковцями, як В. Б. Клаверов, В. Номоконов, М.В. Салтевський, М.Г. Чернец та ін. У цій статті ми спробуємо максимально чітко відобразити основні засади правового регулювання кіберзлочинності та виявити його недоліки для розробки подальшої стратегії щодо запобігання кіберзлочинності органами внутрішніх справ України.

Збільшення об'ємів інформації, комп'ютерних мереж та кількості користувачів, спрощення доступу до інформації, що циркулює у мережах, суттєво збільшує ймовірність викрадення або знищення цієї інформації.

На сучасному етапі значимість проблеми захисту інформаційних ресурсів визначається наступними факторами:

- розвитком світових та національних комп'ютерних мереж та нових технологій, що забезпечують доступ до інформаційних ресурсів;
- переводом інформаційних ресурсів на електронні носії та концентрацією їх в інформаційних системах;
- збільшення вартості інформації, що створюється та накопичується;
- розробка та удосконалення інформаційних технологій, що можуть ефективно використовуватися кримінальними структурами [2].

Фахівці виокремлюють наступні напрямки правового регулювання Інтернет-відносин: захист особистих даних та приватного життя у мережі; регулювання електронної комерції та інших операцій

і забезпечення їх безпеки; захист інтелектуальної власності; боротьба проти протиправного змісту інформації та протиправної поведінки у мережі; правове регулювання електронних повідомлень [3].

У ряді міждержавних нормативно-правових актів визнано, що кіберзлочинність сьогодні становить загрозу не тільки національній безпеці окремих держав, а загрожує людству та міжнародному порядку.

За оцінками Інтерполу, прибутки комп'ютерних злочинців у світі посідають третє місце після доходів наркоділків та нелегальних постачальників зброї.

У той самий час в Україні відсутня концепція стратегії реалізації державної політики щодо боротьби з кіберзлочинністю, у зв'язку з чим наявність цієї проблематики та її розуміння в контексті державної та міжнародної безпеки на загальнодержавному рівні обумовлює необхідність вчинення дійових заходів, з боку вищих органів державної влади, спрямованих на протидію злочинним проявам у цій сфері.

Зазначене вище обумовлює необхідність розроблення відповідних нормативно-правових актів, удосконалення чинного законодавства і, в першу чергу, законодавчого закріплення діяльності правоохоронних органів у сфері державної політики щодо боротьби з кіберзлочинністю.

Проблеми кіберзлочинності, у контексті інформаційної безпеки як складової національної безпеки, розглядалися неодноразово Радою національної безпеки і оборони України. Про це, зокрема, свідчать укази Президента України: Про рішення Ради національної безпеки і оборони України від 17 червня 1997 року «Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин» від 21 липня 1997 р. № 663/97 [4]; Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року «Про заходи щодо вдосконалення державної політики та забезпечення інформаційної безпеки України» від 6 грудня 2001 р. № 1193/2001 [5]; «Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень» від 14 липня 2000 р. № 891[6]; «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31 липня 2000 р. № 928/2000 [7]; «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних» від 24 вересня 2001 р. № 891/2001[8] та інші.

Однак, діяльність правоохоронних та інших органів влади щодо протидії кіберзлочинності не регламентується одним нормативно-правовим актом, що зумовлює неузгодженість у правовому регулюванні діяльності не лише окремих їх підрозділів, а й інших суб'єктів протидії.

Міністерство внутрішніх справ України організовує діяльність підрозділів міліції та здійснює низку заходів, спрямованих на запобігання кіберзлочинності відповідно до загальнодержавних програм і планів щодо протидії окремим видам злочинів.

Перелічені завдання і функції виконуються не Міністерством внутрішніх справ України загалом, а відповідними підрозділами його центрального апарату. Отже, вказане міністерство відповідно до свого положення реалізує завдання безпосередньо та через утворені в установленому порядку головні управління, управління в Автономній Республіці Крим, областях, містах Києві та Севастополі, управління на залізницях, районні, районні у містах, міські управління і відділи, а також через внутрішні війська, підприємства, установи і організації, що належать до сфери його управління.

Діяльність цих структурних підрозділів щодо попередження злочинності має суттєві відмінності. Якщо для одних управлінь, служб та підрозділів (які виконують контрольно-дозвільні функції) попередження є супутнім завданням у межах правоохоронної діяльності чи супутнім результатом функціональної діяльності, то для інших – однією із функцій у межах правоохоронної роботи (управління, служби і підрозділи, які безпосередньо проводять боротьбу з загальнокримінальною і організованою злочинністю і для яких її попередження є однією

із функцій у межах правоохоронної діяльності міліції), а для третіх – функціональна діяльність включає в себе й попередження (органи, для яких попередження злочинів є процесуально-правовим обов'язком у межах досудового розслідування) [9].

В Україні окремого нормативно-правового акта, який би визначав діяльність органів і підрозділів внутрішніх справ щодо запобігання кіберзлочинності немає. На нашу думку, розроблення і затвердження окремого нормативно-правового акту МВС, який би регламентував в Україні діяльність органів і підрозділів внутрішніх справ щодо запобігання злочинам, позитивно вплинуло б на організацію та ефективність такої діяльності.

Стосовно нормативного регулювання діяльності органів у сфері протидії кіберзлочинності, на наш погляд, доцільно проаналізувати наступні нормативно-правові акти.

Правову основу діяльності правоохоронних органів у сфері протидії кіберзлочинності складає Конвенція Ради Європи «Про кіберзлочинність», прийнята 23 листопада 2001 р. та ратифікована Верховною Радою України 7 вересня 2005 р.

Відповідно до положень зазначеного нормативно-правового акту держави учасники впевнені, що ця Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва [10].

У зазначеному нормативно-правовому акті міститься перелік та тлумачення понять, що стосуються кіберзлочинності, перелік діянь, за вчинення яких необхідно передбачати відповідальність, у тому числі відповідальність юридичних осіб, співробітники яких вчиняють зазначені діяння, положення відносно діяльності та повноважень уповноважених державних органів у цій сфері, положення відносно міжнародного співробітництва.

Аналіз положень вказаного нормативного акту та положень національного законодавства дозволяє зробити висновок, що між ними є певні розбіжності. Так, наприклад, розбіжності відносно діянь, за вчинення яких необхідно передбачити відповідальність, відносно законодавчого закріплення повноважень відповідних державних органів у цій сфері тощо.

Необхідно зазначити, що у структурі Міністерства внутрішніх справ України, відповідно до вимог Закону України «Про центральні органи виконавчої влади» від 17 березня 2011 р. та Положення про Міністерство внутрішніх справ України, затвердженого Указом Президента України від 6 квітня 2011 року № 383/2011 створене Управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України. Метою діяльності зазначеного управління є забезпечення, відповідно до законодавства України, реалізації державної політики у сфері боротьби з кіберзлочинністю, у тому числі організація та здійснення оперативно-розшукової діяльності [11]. Управління у своїй діяльності керується Конституцією України, законами України, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, актами Президента України та Кабінету Міністрів України, нормативно-правовими актами МВС, а також Положенням про Управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України.

Основними завданнями зазначеного управління є:

- участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії злочинам і правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також ін-

шим злочинам та правопорушенням, учиненим з їх використанням;

- попередження та протидія злочинам і правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

- попередження та протидія злочинам і правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (у сферах платіжних систем; обігу інформації протиправного характеру із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (далі – протиправного контенту); економіки, яка включає в себе фінансові та торгові транзакції, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж, а також протидія забороненим видам господарської діяльності у цій сфері (далі – електронної комерції); надання телекомунікаційних послуг; а також шахрайствам і легалізації (відмиванню) доходів, одержаних від зазначених вище злочинів);

- сприяння іншим підрозділам МВС України у проведенні заходів, спрямованих на запобігання, протидію, розкриття та розслідування злочинів, які відносяться до їх компетенції, у порядку, передбаченому законодавством та іншими нормативно-правовими актами [12].

Крім того, у вказаному нормативно-правовому акті визначаються функції та повноваження зазначеного управління.

Отже, на підставі зазначеного можна дійти до висновку, що зазначене вище управління є головним структурним підрозділом Міністерства внутрішніх справ України, який, відповідно до чинного законодавства, здійснює протидію кіберзлочинності.

Доцільно також зауважити, що на підставі аналізу нормативно закріплених положень про структурні підрозділи кримінальної міліції можна зробити висновок, що до суб'єктів протидії кіберзлочинності слід віднести: Департамент боротьби з незаконним обігом наркотиків МВС України, Департамент кримінальної міліції у справах дітей, Державну службу боротьби з економічною злочинністю, Департамент карного розшуку. У Положенні про Державну службу боротьби з економічною злочинністю відсутні норми щодо запобігання кіберзлочинності. Хоча таку діяльність служба здійснює, а саме протидіє злочинам, що вчиняються в економічній сфері за допомогою електронно-обчислювальних машин (комп'ютерів). У Положенні про кримінальну міліцію у справах дітей окремо не зазначено такий напрям роботи, як запобігання кіберзлочинності. Однак у ньому вказано, що кримінальна міліція у справах дітей виявляє дорослих осіб, які займаються виготовленням та розповсюдженням порнографічної продукції, видань, що пропагують насильство, жорстокість, сексуальну розпусту, тобто діянь, що можуть вчинятися за допомогою технічних засобів, у тому числі комп'ютерів. У нормативно-правових актах, що регламентують діяльність Департаменту карного розшуку, також відсутні посилання на боротьбу з кіберзлочинністю, однак ураховуючи, у багатьох випадках, організований характер кіберзлочинності, на вказаний Департамент та його структурні підрозділи покладаються завдання із запобігання кіберзлочинності.

Крім того, правову основу діяльності правоохоронних органів у сфері боротьби зі кіберзлочинністю складають наступні нормативно-правові акти.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05 квітня 1994 р. Зазначений нормативно-правовий акт містить визначення понять, що використовуються у сфері інформаційно-телекомунікаційних систем. Регламентує об'єкти захисту, суб'єктів відносин, що виникають у вказаній сфері та порядок поводження з інформацією, що міститься у цих системах тощо.

Безпосередньо, що стосується діяльності правоохоронних органів, вказаний документ регламентує повноваження спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації та

його регіональних органів, якими є:

- розробка пропозиції щодо державної політики у сфері захисту інформації та забезпечення її реалізації в межах своєї компетенції;
- визначення вимог та порядоку створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
- організація проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;
- здійснення контролю за забезпеченням захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
- здійснення заходів щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та надання рекомендації з питань запобігання такій загрозі [13].

У разі виявлення уповноваженими особами вказаного органу порушень захисту зазначеної інформації, порядку поводження з цією інформацією звертаються до відповідних органів, у тому числі до органів внутрішніх справ, з метою притягнення винних осіб до відповідальності.

Наступним нормативно-правовим актом, що регламентує діяльність правоохоронних органів у зазначеній сфері, є Закон України «Про захист суспільної моралі» від 20 листопада 2003 р. Зазначений нормативно-правовий акт містить визначення понять, що використовуються у сфері суспільної моралі, основні напрями державного регулювання обігу інформаційної продукції, що негативно впливає на суспільну мораль тощо.

Безпосередньо, що стосується діяльності правоохоронних органів, вказаний документ регламентує завдання Національної експертної комісії України з питань захисту суспільної моралі, якими є:

- координація розробки концепції захисту суспільної моралі, розробка засад державної політики з обігу продукції сексуального характеру та регулювання відповідних відносин;
- аналіз процесів і тенденцій, що відбуваються у сфері захисту суспільної моралі, розробка рекомендацій для органів державної влади та місцевого самоврядування по їх правовому регулюванню;
- контроль за дотриманням чинного законодавства України у сфері захисту суспільної моралі;
- участь у розробці міжнародних договорів України з питань захисту суспільної моралі [14].

У разі виявлення уповноваженими особами вказаного органу порушень обігу інформації, що є предметом у вказаній сфері, в тому числі за допомогою використання комп'ютерних технологій, вони повинні звертатися до зазначених вище підрозділів органів внутрішніх справ з метою припинення останніми даних фактів та притягнення винних осіб до відповідальності.

Безпосередньо, що стосується діяльності правоохоронних органів, у тому числі підрозділів по боротьбі з кіберзлочинністю, вказаний документ визначає їх завдання у зазначеній сфері відносно розвитку міжнародного співробітництва, перейняття зарубіжного досвіду, розроблення пропозицій відносно удосконалення їх діяльності.

Наступним документом, який є правовою основою діяльності правоохоронних органів у сфері боротьби з кіберзлочинністю, є Указ Президента «Про заходи щодо забезпечення захисту прав і законних інтересів дітей» від 05 травня 2008 р. № 411/2008.

На підставі вивчення зазначених нормативних актів, на нашу думку, можна зробити висновок, що правове регулювання діяльності правоохоронних органів у сфері протидії кіберзлочинності має наступні недоліки:

- відсутня чітка регламентація заходів протидії кіберзлочинності, а саме відсутність єдиного нормативно-правового акту Міністерства внутрішніх справ України відносно протидії аналізованому прояву

злочинності;

- відсутність законодавчо розробленого понятійного апарату щодо визначення понять у зазначеній сфері;
- неузгодженість завдань і функцій стосовно протидії кіберзлочинності серед підрозділів органів внутрішніх справ;
- неузгоджений порядок взаємодії підрозділів органів внутрішніх справ у вказаній сфері;
- неузгодженість існуючих держаних нормативно-правових актів з міжнародними, що були ратифіковані Верховною Радою України;
- неузгоджений порядок міжнародного співробітництва уповноважених органів з органами інших держав у цій сфері.

Література

1. Доктрина інформаційної безпеки України. Затверджена указом президента України від 8 липня 2009 р. № 514/2009 [Електронний ресурс] / Верховна Рада України : Законодавство. – 10.06.2013 р. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/514/2009.

2. Клаверов В. Б. Как противодействовать компьютерной преступности? [Електронний ресурс] / Владимир Борисович Клаверов ; Интернет агентство LIVING : статьи. – Режим доступу: http://living.biz.ua/index.php?page=stati&id=%CA&aid=304.

3. Номоконов Виталий. Актуальные проблемы борьбы с киберпреступностью [Електронний ресурс] / Виталий Номоконов ; Владивостокский центр исследования организованной преступности, Центр исследования компьютерной преступности. – Режим доступу: http://www.crime-research.org/library/Nomokon1.html.

4. Указ Президента «Про рішення Ради національної безпеки і оборони України від 17 червня 1997 р. «Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин»» від 21 липня 1997 р. № 663/97 [Електронний ресурс] / Верховна Рада України : Законодавство. – 10.06.2013 р. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/663/97.

5. Указ Президента «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року «Про заходи щодо вдосконалення державної політики та забезпечення інформаційної безпеки України»» від 6 грудня 2001 р. № 1193/2001 [Електронний ресурс] / Верховна Рада України : Законодавство. – 10.06.2013 р. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1193/2001.

6. Указ Президента «Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень» від 14 липня 2000 р. № 891 [Електронний ресурс] / Верховна Рада України : Законодавство. – 10.06.2013 р. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/891/2000.

7. Указ Президента «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31 липня 2000 р. № 928/2000. [Електронний ресурс] / Верховна Рада України : Законодавство. – 10.06.2013 р. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/928/2000.

8. Указ Президента «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних» від 24 вересня 2001 р. № 891/2001. [Електронний ресурс] / Верховна Рада України : Законодавство. – 10.06.2013 р. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/891/2001.

9. Кримінологія: Загальна та Особлива частини : [Підруч. для юрид.спец.вищ.навч. закл. / І.М. Даньшин, В.В. Голіна, О.Г. Кальман, О.В. Лисодєд] ; За ред. :І.М. Даньшин ; Нац. юрид. акад. України ім. Ярослава Мудрого. – Х. : Право, 2003. – 351 с. -С. 108.

10. Конвенція Ради Європи «Про кіберзлочинність», прийнята 23 листопада 2001 р., ратифікована Верховною Радою України 7 вересня 2005 р. [Електронний ресурс] / Верховна Рада України : Законодавство. – 10.06.2013 р. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_575.

11. Наказ МВС «Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС» від

АНОТАЦІЯ

У статті проведено аналіз нормативно-правових актів України щодо діяльності органів внутрішніх справ, направленої на виявлення та запобігання кіберзлочинності. Встановлено, що на теперішній час не існує єдиного основного законодавчого акту, який би чітко регулював діяльність органів внутрішніх справ у сфері запобігання кіберзлочинності.

На підставі проведеного аналізу визначено, що в результаті одночасної дії декількох нормативних актів у зазначеній сфері існують неузгодженості щодо завдань, функцій та порядку взаємодії підрозділів органів внутрішніх справ; відсутність законодавчо-розроблених понять щодо запобігання кіберзлочинності. Також дослідженням виявлено неузгодженість деяких правових актів України з міжнародними актами.

31 травня 2012 р. № 494. [Електронний ресурс]. – Режим доступу: http://document.ua/pro-organizaciyu-dijalnosti-upravlinnja-borotbi-z-kiberzloch-doc103883.html.

12. Наказ МВС «Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС» від 31 травня 2012 р. № 494. [Електронний ресурс]. – Режим доступу: http://document.ua/pro-organizaciyu-dijalnosti-upravlinnja-borotbi-z-kiberzloch-doc103883.html.

SUMMARY

The article describes the analysis of legal acts of Ukraine concerning the activities of internal affairs aimed at the detection and prevention of cybercrime. It was found that at present there is no single primary legislation that would clearly regulate the activities of law-enforcement bodies in the area of prevention of cybercrime. Based on this analysis, it is determined that the simultaneous action of several regulations in this area, there are inconsistencies regarding the tasks, functions, and procedures of interaction of divisions of internal affairs; the absence of legislation on the prevention of the developed concepts of cybercrime. Also, the study found some inconsistency of legal acts of Ukraine with international acts.

13. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 квітня 1994 р. [Електронний ресурс] / Верховна Рада України : Законодавство. – 10.06.2013 р. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/print1329869296477451

14. Закон України « Про захист суспільної моралі» від 20.11.2003 р. [Електронний ресурс] / Верховна Рада України : Законодавство. – 10.06.2013 р. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1296-15/print1329869296477451