Катерина Рудой,
кандидат юридичних наук, доцент,
професор кафедри адміністративного права
та адміністративного процесу
Одеського державного університету
внутрішніх справ

УДК 351.74

Протидія кіберзлочинності як напрям забезпечення міжнародної безпеки ОВС України

Протягом останнього десятиліття у світовій політиці відбулися значні зміни, що призвели до концептуального перегляду способів та засобів забезпечення міжнародної безпеки. Саме тому, прогресивний розвиток України як суверенної, демократичної, правової держави можливий тільки за умови як найповнішого забезпечення належного рівня економічної та інформаційної безпеки. Важливу роль в цьому процесі відіграють правоохоронні органи з огляду на їх компетенцію щодо запобігання злочинам та іншим правопорушенням, в тому числі у сфері інформаційної та економічної безпеки. Органи внутрішніх справ є найчисельнішою ланкою в системі правоохоронних органів, вони не тільки в організаційному, але й у функціональному плані посідають найважливіше місце в системі правоохоронних органів. В свою чергу для забезпечення економічної та інформаційної безпеки в системі Міністерства внутрішніх справ створено Управління боротьби з кіберзлочинністю МВС України, основним завданням якої є попередження та боротьба з кіберзлочинністю. Крім того, Міністерство внутрішніх справ України бере участь у формуванні та реалізації державної політики з питань боротьби з кіберзлочинами, у т.ч. такими, що вчиняються з терористичною метою; забезпечує у межах своєї компетенції безпеку громадян у національному сегменті кіберпростору; вживає необхідних заходів щодо попередження, своєчасного виявлення, припинення і розкриття кіберзлочинів; забезпечує належне функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні кіберзлочинів; забезпечує взаємодію з операторами та провайдерами телекомунікацій з питань попередження кіберінцидентів кримінального характеру; взаємодіє з компетентними органами інших країн в рамках надання міжнародно-правової допомоги у протидії кіберзлочинам [2].

Таким чином, питання забезпечення економічної та інформаційної безпеки України розглядаються як один із найважливіших національних

пріоритетів, що вимагає посиленої уваги представників владних структур, політичних партій, науковців, широкої громадськості, а тому дослідження протидії кіберзлочинності як напрямку забезпечення міжнародної безпеки ОВС України є актуальним та своєчасним.

Серед науковців, які займаються даною проблематикою, необхідно відзначити роботи О. Бандурки, Ю. Батуріна, В. Вехова, В. Голубева, М. Діхтяренко, Ю. Онищенко, О. Орлова, Б. Романюка, О. Снегірьова та інших, які періодично пропонували різні поправки і доповнення щодо удосконалення організаційно-правових засад протидії кіберзлочинності в Україні [4].

На сьогоднішній день в Україні діє низка Законів України та нормативних документів різних рівнів, що охоплюють проблеми забезпечення кібербезпеки держави. Це, зокрема, Закони України «Про Державну службу спеціального зв'язку та захисту інформації України», «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України». Крім того в межах даної проблеми діє два стратегічних документа: Стратегія національної безпеки України та Доктрина інформаційної безпеки України, а також ратифікована Верховною Радою України «Конвенція про кіберзлочинність». Чинний Кримінальний кодекс України встановлює (відповідно до Розділу (XVI) відповідальність за «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (статті 361-363) [1; 5; 6; 7; 10].

Забезпечення кібернетичної безпеки являє собою сукупність політичних, соціальних, економічних та інформаційних відносин разом із організаційно-адміністративними та техніко-технологічними заходами шляхом комплексного підходу у тісній взаємодії державного і приватного секторів та громадянського суспільства. Основним нормативно-правовим актом, що врегулює відносини у сфері протидії кіберзлочинності в Україні, повинен стати Закон України «Про кібернетичну безпеку», що сприятиме визначенню основних засад державної політики, спрямованої на захист життєво важливих інтересів особи, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем. Тому 27 березня 2015 року питання законодавчого забезпечення кібербезпеки України та протидії кіберзлочинності обговорювались під час засідання Робочої групи при Комітеті з питань законодавчого забезпечення правоохоронної діяльності Верховної Ради України, на якому робоча група з підготовки реформування законодавства у сфері інформаційної безпеки та боротьби з кіберзлочинністю розглянула проект спеціального (базового) Закону "Про основні засади забезпечення кібербезпеки України", розробленого Державною службою спеціального зв'язку та захисту інформації України, та законопроект з захисту інформаційної безпеки та протидії кіберзлочинності, розробленого Службою безпеки України. Відповідно до статті 7 проекту Закону України «Про кібернетичну безпеку» та проекту Закону України «Про основні засади забезпечення кібербезпеки України» Міністерство внутрішніх справ віднесено до основних суб'єктів забезпечення кібернетичної безпеки [5; 6].

Сьогодні в Україні на порядку денному стоїть питання підготовки національних кадрів, що координують і здійснюють 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 підготовку слідчих, що спеціалізуються на розслідуванні кіберзлочинів, та оперативних працівників для підрозділів боротьби з кіберзлочинністю.

Необхідно зазначити, що забезпечення кібернетичної безпеки ґрунтується на принципах: верховенства права, пріоритетності захисту прав і свобод людини і громадянина від кіберзагроз; своєчасного та адекватного реагування на кіберінциденти, запобігання виникненню надзвичайних ситуацій на об'єктах критичної інформаційної інфраструктури; вільного доступу населення до інформації щодо стану кібернетичної безпеки; чіткого розмежування повноважень і взаємодії органів державної влади та приватного сектору сфері кібернетичної безпеки; особистої відповідальності громадян про власну безпеку, неухильного дотримання ними правил безпечної поведінки у кіберпросторі; відповідальності у межах своїх повноважень посадових осіб за дотримання вимог щодо кіберзахисту об'єктів критичної інформаційної інфраструктури [7]. Тому класифікацію принципів протидії кіберзлочинності в Україні можна розподілити на три групи: на загальні, спеціальні та принципи забезпечення інформаційної та економічної безпеки.

До основних заходів профілактики правопорушень у сфері електронної комерції, що здійснюються підрозділами боротьби з кіберзлочинністю МВС України, відносяться: аналітична розвідка, тобто перехід до збагачених інформаційно-наукових та прогностичних форм діяльності підрозділів УБК МВС України, вивчення матеріалів прихованого спостереження, повідомлень негласних працівників, даних перехоплення з різних каналів зв'язку, а також аналіз повідомлень, публікацій і виступів у засобах масової інформації, статистичних даних, зведень, що містяться в державному і недержавному автоматизованих банках даних і інформаційних системах та ін.

До системи заходів запобігання та протидії правопорушенням у сфері шахрайства та легалізації (відмиванню) доходів, одержаних злочинним шляхом, які застосовує Управління боротьби з кіберзлочинністю МВС України, входять заходи інформаційної взаємодії між суб'єктами фінансового моніторингу: 1) збір, накопичення, систематизація, аналіз та узагальнення інформації про фінансові операції, які є об'єктом фінансового моніторингу; 2) виявлення фактів приховування незаконного походження доходів; 3) виявлення джерел одержання таких доходів та маршрути переміщення; 4) виявлення напрямів використання. Здійснення інформаційної взаємодії УБК МВС України з суб'єктами фінансового моніторингу дозволяє: 1) сформувати багатосторонні інформаційно-телекомунікаційні зв'язки між державними органами, задіяними у боротьбі з легалізацією незаконно отриманих доходів; 2) забезпечити оперативний обмін інформацією; 3) здійснити аналіз фінансових операцій і отримати конкретні результати, які є підставою застосування заходів, спрямованих на боротьбу з легалізацією тіньових доходів; 4) здійснити контроль виконання рішень, прийнятих у процесі здійснення фінансового моніторингу.

Крім того, з метою реалізації ефективних заходів протидії кіберзлочинності підрозділами боротьби з кіберзлочинністю МВС України важливо враховувати досвід правоохоронних органів зарубіжних країн. Так, наприклад, національні законодавства і правоохоронні органи різних країн у своїй діяльності вимушені брати до уваги особливості кордонів, мовні, політичні, релігійні особ-

ливості, 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 [3].

Перераховані вище обставини обумовлюють прийняття спеціального законодавства та розробки загальнодержавної комплексної стратегії протидії з кіберзлочинністю в Україні із урахуванням європейського досвіду, а також визначення основних напрямків діяльності державних органів та органів місцевого самоврядування, інститутів громадянського суспільства, юридичних і фізичних осіб щодо захисту основ конституційного устрою, прав і свобод людини та громадянина, забезпечення цілісності й національної безпеки держави, виявлення і ліквідації причин та умов, що сприяють проявам кіберзлочинності, а також попередження, виявлення та зупинення кіберзлочинності й ліквідації її наслідків. З урахуванням зазначених пропозицій та рекомендацій протидія кіберзлочинності в України підрозділами боротьби з кіберзлочинністю МВС України буде відповідати міжнародним стандартам, що сприятиме покращенню правоохоронної діяльності у сфері інформаційної та економічної безпеки України в цілому.

Список використаних джерел

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

2. *Орлов О. В.* Актуальні напрями державної політики України у сфері боротьби з кіберзлочинністю/ О. В. Орлов, Ю. М. Онищенко / Теорія та практика державного управління. – Вип. 3 (42). [Электронный ресурс]. – Режим доступа: http://www.kbuapa. kharkov.ua/ e-book/tpdu/2013-3/doc/1/01.pdf

3. *Интерпол:* киберпреступления являются самой опасной криминальной угрозой [Электронный ресурс]. – Режим доступа: http://www.virusovnet.org/main/309.

4. *Зозуля Є. В.* Діяльність органів державної влади та управління України щодо нормативно-правового та організаційного забезпечення міжнародного співробітництва у боротьбі з кіберзлочинністю/ Є. В. Зозуля / Право і суспільство. - № 4. – 2011. [Электронный ресурс]. – Режим доступа: irbis-nbuv.gov.ua/.../cgiirbis_64.exe Pis_2011_4_19.pdf

5. *Проект* Закону України «Про основні засади забезпечення кібербезпеки України» [Электронный ресурс]. – Режим доступа : http://search.ligazakon.ua/l_doc2.nsf/link1/JH1N268A.html

6. *Раді* пропонують ухвалити законопроект про протидію кіберзлочинності [Электронный ресурс]. – Режим доступа : http://imi.org.ua/news/49411-radi-proponuyut-uhvaliti-zakonoproekt-pro-protidiyu-kiberzlochinnosti.html

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

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

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

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

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

Рудой К. М. Протидія кіберзлочинності як напрям забезпечення міжнародної безпеки ОВС України

Статтю присвячено аналізу чинного законодавства у сфері забезпечення кібернетичної безпеки, виокремлено та охарактеризовано заходи протидії кіберзлочинності у різних галузях. Визначено принципи протидії кіберзлочинності, які класифіковано на: загальні, спеціальні та принципи забезпечення інформаційної та економічної безпеки. Визначено специфіку організації діяльності Управління боротьби з кіберзлочинністю МВС України, форм та методів його діяльності, взаємодії з іншими правоохоронними органами з питань профілактики правопорушень у сфері боротьби з кіберзлочинністю. Сформульовано конкретні пропозиції та рекомендації, спрямовані на удосконалення адміністративно-правових засад діяльності УБК МВС України.

Ключові слова: кіберзлочинність, сфера телекомунікацій, Управління боротьби з кіберзлочинністю МВС України, правове регулювання, принципи, інформаційна безпека, економічна безпека.

Рудой Е. Н. Противодействие киберпреступности как направление обеспечения международной безопасности ОВД Украины

Статья посвящена анализу действующего законодательства в сфере обеспечения кибернетической безопасности, выделены и охарактеризованы меры противодействия киберпреступности в различных сферах. Определены принципы противодействия киберпреступности, которые классифицированы на: общие, специальные и принципы обеспечения информационной и экономической безопасности. Определено специфику организации деятельности Управления борьбы с киберпреступностью МВД Украины, форм и методов его деятельности, взаимодействия с другими правоохранительными органами по вопросам профилактики правонарушений в сфере борьбы с киберпреступностью. Сформулированы конкретные предложения и рекомендации, направленные на усовершенствование административно-правовых основ деятельности УБК МВД Украины

Ключевые слова: киберпреступность, сфера телекоммуникации, Управление борьбы с киберпреступностью МВД Украины, правовое регулирование, принципы, информационная безопасность, экономическая безопасность.

Rudoy K. Combating cybercrime as the direction of international security bodies of internal affairs Ukraine

This article is devoted to the analysis of current legislation in the area of cyber security, isolated and characterized the measures combating cybercrime in various fields. It defines the principles of cybercrime, which are classified into: general, special and principles of information and economic security. Identified the specific organization of the activities of the Department on cybercrime of the Ministry of Internal Affairs of Ukraine, forms and methods of its activity, interaction with other law enforcement agencies on issues of crime prevention in the fight against cybercrime. Specific proposals and recommendations aimed at improving the legal and administrative framework for the operation of the Department on cybercrime of the Ministry of Internal Affairs of Ukraine.

Key words: cybercrime, telecommunications sphere, Department on cybercrime of the Ministry of Internal Affairs of Ukraine, legal regulation, principles, information security, economic security.