of irresistible impulse presence in the subject of crime while infliction of death of other person, as well as fact finding of the suddenness of such state occurrence due to illegal violence, regular abuse or great insult from the side of the victim. Thus, in the course of prejudicial inquiry there arises the need to involve specialists who possess the relevant psychological and psychiatric knowledge and can conduct the necessary forensic studies and provide efficient conclusion. It appears that the competence of expert-psychiatrist includes the evaluation of mental health of a person, diagnostics of mental disorders and diseased states but the competence of expert-psychologist refers to analysis of individual and psychological peculiarities of the person under examination and study of the period of psycho-emotional tension if such period has anteceded the occurrence of affected state. There was formulated the list of common questions of forensic psychologic-psychiatric examination which is assigned in the course of investigation of criminal proceedings on intentional homicide committed in state of strong mental agitation.

Key words: *special knowledge, intentional homicide, state of strong mental agitation, psychologic-psychiatric examination, psychologist, psychiatrist.*

Стаття надійшла 10 грудня 2014 р.

УДК 65.012.8

О. І. Зачек

ПРАВОВІ ПРОБЛЕМИ ПРОТИДІЇ КІБЕРЗЛОЧИНЦЯМ, ЩО ДІЮТЬ З-ЗА МЕЖ УКРАЇНИ

Розглянуто правові проблеми протидії кіберзлочинцям, що діють з-за меж України. Наведено приклади кібератак на українські інформаційні системи та сайти в період проведення антитерористичної операції на сході України. Окреслено правові підстави боротьби з кіберзлочинами. Розглянуто проблеми, які виникають унаслідок неможливості затримання злочинців, які вчиняють кібератаки проти українських інформаційних систем з-за меж України. Надано пропозиції зі змін до законодавства з метою ефективної протидії кіберзлочинцям у таких випадках.

Ключові слова: *кіберзлочини, кібертероризм, кібератаки, хакерські методи, правові проблеми.*

Постановка проблеми. Останнім часом значно зросла кількість атак на інформаційні системи. В одних випадках злочинців цікавить інформація, яка зберігається та обробляється в таких системах.

В інших випадках вони намагаються заблокувати функціонування інформаційних систем. Особливо зросла кількість кібератак на українські інформаційні системи та сайти в період проведення антитерористичної операції на сході України. Зокрема, в повідомленні УНІАН від 08.08.2014 зазначено, що було виявлено зараження десятків комп'ютерів у офісі Прем'єр-міністра України Арсенія Яценюка, а також у посольствах України російською троянською програмою Snake, відомою також під назвами Turla і Uroboros. Ця програма перехоплює мережевий трафік та дає змогу отримати віддалений доступ до зараженого комп'ютера через мережу Інтернет. На думку експерта з кібервійни в Royal United Services Institute Пітера Робертса, ця троянська програма створена російськими оперативниками для доступу до систем безпеки й оборони урядових органів інших країн [1]. Згідно з повідомленням СБУ, під час президентських виборів російські хакери вчиняли атаки на сервер ЦВК. Також, відповідно до повідомлення УНІАН, наприкінці липня сайт президента Петра Порошенка був заблокований у результаті DDoS-атаки [1]. Згідно з повідомленням Новости@mail.ru, відповідальність за блокування роботи сайту взяла на себе група хакерів КіберБеркут, яка з'явилася після розформування спецпідрозділу Беркут. Саме це угруповання атакувало сервер ЦВК під час виборів президента, блокувало роботу сайтів МВС та Генпрокуратури України [2].

«Новое время» з посиланням на Reuters повідомило, що російські хакери використовували помилки в Microsoft Windows для стеження за комп'ютерами НАТО, Євросоюзу та України, зокрема комп'ютерами енергетичних та телекомунікаційних компаній. Це виявила компанія iSight Partners, що спеціалізується на кіберрозвідці. Експерти цієї компанії впевнені, що існує зв'язок між цими хакерами та спецслужбами Росії, оскільки йдеться про шпигунство, а не звичайну крадіжку даних [3].

І такі повідомлення з'являються дедалі частіше. Ці дії кіберзлочинців є елементами кібервійни та спробами і здійснення технічної розвідки, і дезорганізації роботи української влади. Також такі дії злочинців можна кваліфікувати як кібертероризм.

Мета здійснення кібертероризму є такою ж, як і в звичайних терористичних дій: порушення державної та суспільної безпеки, залякування населення, ускладнення міжнародних відносин та вплив на ухвалення рішень органами державної влади атакованої країни [4, с. 145].

Основна проблема протидії таким злочинцям полягає в їхньому знаходженні за межами досяжності правоохоронних органів України, а також можливій підтримці спецслужбами ворожої держави. Тобто, навіть у разі виявлення їх місцезнаходження немає можливості їх затримати та вилучити засоби вчинення злочинів. Основні етапи боротьби з кіберзлочинцями: виявлення злочину, відслідкування IP-адрес злочинців, ідентифікація злочинців та виявлення їх місця перебування на основі IP-адрес, затримання злочинців та вилучення знарядь учинення злочину.

Метою статті є подання пропозицій зі змін до законодавства з метою ефективної протидії кіберзлочинцям, які атакують українські інформаційні системи та сайти з-за меж України. Завданням дослідження є розгляд проблеми протидії кіберзлочинцям, якщо немає можливості їх затримання.

Стан дослідження. Проблемам боротьби з кіберзлочинністю в Україні присвячено достатньо публікацій у літературних джерелах, зокрема, таких учених: К. І. Бєляков, В. М. Бутузов, В. Д. Гавловський, В. О. Глушков, В. О. Голубєв, О. О. Йона, Н. Ф. Казакова, Д. Й. Никифорчук, С. О. Орлов, Н. А. Савінова, П. Л. Фріс, В. С. Цимбалюк.

Важливість наукового здобутку та внеску в теорію та практику інформаційної безпеки згаданих учених складно переоцінити. Однак аналіз літературних джерел та існуючих загроз правопорядку та державній безпеці України дає підстави стверджувати, що існують проблеми боротьби з кіберзлочинцями, які досі не розглядалися.

Виклад основних положень. В. М. Бутузов вважає, що глобальні інформаційні мережі дають змогу обирати кіберзлочинцям базами для своєї діяльності такі країни, де є привабливі умови для протиправних дій, за які, згідно з місцевим законодавством, не передбачена відповідальність, або де відсутні спеціалізовані підрозділи боротьби з комп'ютерною злочинністю. Тобто більшість транснаціональних злочинних угруповань перебувають на території держав «третього світу» [4, с. 7–8].

На думку В. О. Голубєва, нині немає реальної можливості звернення до правоохоронних органів інших країн, не беручи до уваги офіційні канали, з метою миттєвого реагування на транснаціональні комп'ютерні злочини [5, с. 139]. А з урахуванням останніх політичних реалій, коли злочинці діють за підтримки спецслужб ворожої держави, тобто існує державний кібертероризм, виникає необхідність застосу-

вання нетрадиційних та адекватних методів для захисту національної безпеки від кібератак.

Часто хакерські технології використовують правоохоронні органи інших держав.

Наприклад, ФБР використовувало шкідливе програмне забезпечення та фішинг для затримання злочинця, який на своїй сторінці в MySpace погрожував замінувати навчальний заклад. Для цього створено сторінку, на якій була опублікована стаття з описом справи, а власнику аккаунта надсилалося посилання на неї. Злочинець, зацікавившись, перейшов за посиланням і на його комп'ютер завантажився вірус, який дав змогу ФБР отримати його IP-адресу та MAC-адресу, внаслідок чого злочинець був заарештований [6].

Упродовж двох років ФБР використовує сучасні хакерські методи для ідентифікації злочинців, котрі використовують анонімну мережу Tor, яка не дає змогу відслідковувати, з якого комп'ютера здійснено вихід в Інтернет, та допомагає приховувати фізичне місцезнаходження сервера. Під час відвідування користувачем веб-сайту, на котрому ФБР розмістило код, на комп'ютері встановлюється програма, яка визначає його IP-адресу та MAC-адресу. Це дає змогу встановлювати злочинців, які розповсюджують дитячу порнографію, продають наркотики, зброю тощо [7]. Також цікавиться зламом мережі Tor МВС Російської Федерації, оголосивши закритий конкурс із значним призовим фондом для особи, котра знайде спосіб зламу цієї мережі та розкриття інформації про її користувачів [7].

Британський Центр урядового зв'язку (GCHQ) використав у 2011 році DDoS-атаки та впровадження шкідливих програм на сервери Anonymous для нейтралізації дій хакерів та їх ідентифікації. Це було здійснено у відповідь на DDoS-атаки Anonymous [8].

Технічний директор компанії CrowdStrike Дмитро Альперович на конференції AusCERT 2013 запропонував діяти проти злочинців їхніми ж методами, використовуючи обман, дезінформацію та шкідливі програми [9].

Звичайно, такі методи можуть викликати цілком заслужену критику, але, на нашу думку, у виняткових випадках, коли йдеться про національну безпеку України, за рішенням суду, використання їх є доцільним. Але для цього повинно бути створене правове підґрунтя застосування таких методів.

Правовим підґрунтям боротьби з кіберзлочинністю в Україні є такі законодавчі акти. Вперше комп'ютерна злочинність та комп'ю-

терний тероризм згадуються в Законі України від 19.06.2003 «Про основи національної безпеки України» [10]. Базовим нормативним документом є Європейська конвенція про кіберзлочинність, яку Україна ратифікувала в 2005 році [11]. Також є підзаконні нормативні акти: Указ Президента України від 31. 07. 2000 р. «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» [12], Указ Президента України від 24. 09. 2001 р. «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» [13]. Діяльність Управління боротьби з кіберзлочинністю МВС України регламентується Положенням про Управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України, яке було затверджене Наказом МВС України від 30.10.2012 № 988 «Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС» [14]. П. 5.3.13 цього положення передбачає: «Уживати інших передбачених законодавством заходів, спрямованих на ефективну організацію попередження та протидії кримінальним правопорушенням, які віднесено до компетенції Управління», тобто, за умови внесення змін у законодавство є можливість застосування Управлінням вказаних методів.

Кримінальна відповідальність за злочини в цій галузі передбачена розділом XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України від 05.04.2001 р. [15].

Але жоден із цих документів не передбачає використання хакерських методів правоохоронними органами.

В Кримінальному процесуальному кодексі України 2012 року є статті, які дозволяють зняття інформації з транспортних телекомунікаційних мереж (стаття 263) та зняття інформації з електронних інформаційних систем (стаття 264).

Стаття 263 регламентує зняття інформації з транспортних телекомунікаційних мереж, під якими розуміють «мережі, що забезпечують передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого виду між підключеними до неї телекомунікаційними мережами доступу» [16].

Стаття 264 регламентує зняття інформації з електронних інформаційних систем.

Зняття інформації і з транспортних телекомунікаційних мереж, і з електронних інформаційних систем здійснюється на підставі ухвали слідчого судді. Ухвала не потрібна лише у тому разі, коли доступ до електронної інформаційної системи не обмежений власником та не потребує подолання системи логічного захисту. Також у КПК зазначено, що провайдери повинні сприяти правоохоронним органам у їх діяльності із зняття інформації [9].

Але тут не передбачена протидія злочинцям з використанням методів, які використовують іноземні спецслужби, та які описані вище.

Оскільки кіберзлочини у випадку їх спрямування проти національної безпеки України підпадають під визначення «технологічний тероризм», яке дається в Законі України «Про боротьбу з тероризмом» [17], цей закон може бути правовим підґрунтям для боротьби з такими злочинами.

Висновки. Розглянувши наявні загрози в галузі кібербезпеки України та існуюче правове забезпечення боротьби з кіберзлочинністю в Україні, ми вважаємо необхідним термінове внесення пропозицій до Закону України «Про боротьбу з тероризмом», а саме до статті 5 «Повноваження суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом». Пункт 2 цієї статті доцільно доповнити таким текстом: «Управління боротьби з кіберзлочинністю МВС України з метою припинення терористичних дій у випадку кібератак на українські інформаційні системи та сайти з-за меж України, коли відсутня можливість затримання злочинців, може здійснювати блокування IP-адрес, з яких вчиняються кібератаки, зокрема з використанням шкідливих програм».

---

1. Російська програма-шпигун знайдена на комп'ютерах в офісі Яценюка. Новини УНІАН від 08.08.2014 [Електронний ресурс]. – Режим доступу: http://www.unian.ua/science/948970-rosiyska-programa-shpigun-znaydena-na-kompyuterah-v-ofisi-yatsenyuka.html.

2. Хакеры утверждают, что «положили» сайт Президента Украины. Новости@mail.ru от 29.07.2014 [Електронний ресурс]. – Режим доступу: http://news.mail.ru/inworld/ukraina/incident/19030136/?frommail=1.

3. Российские хакеры с помощью ОС Windows нанесли удар по компьютерам НАТО, ЕС и Украины. «Новое время» від 02.11.2014 [Електронний ресурс]. – Режим доступу: http://nvua.net/world/Rossiyskie-hakery-atakovali-kompyutery-NATO-ES-i-Ukrainy-s-celyu-shpionazha-Reuters-16022.html.

4. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія / В. М. Бутузов. – К.: КИТ, 2010. – 408 с.

5. Голубєв В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В. О. Голубєв, В. Д. Гавловський, В. В. Цимбалюк; за заг. ред. доктора юридичних наук, проф. Р. А. Калюжного. – Запоріжжя: Просвіта, 2001. – 252 с.

6. ФБР использовало фишинг и malware для раскрытия личности преступника. «Geektimes« від 30.10.2014 [Електронний ресурс]. – Режим доступу: http://geektimes.ru/post/240825.

7. Для борьбы с пользователями Tor ФБР заражает их компьютеры. «CNews» від 07.08.2014 [Електронний ресурс]. – Режим доступу: http://www.cnews.ru/ news/top/index.shtml?2014/08/07/581945.

8. Британские спецслужбы использовали DDoS-атаки против Anonymous. «Хабрахабр» від 06.02.2014. [Електронний ресурс]. – Режим доступу: http://habrahabr.ru/post/211564.

9. Лучшая защита предприятия от хакеров – нападение. «PCWEEK» від 27.05.2013 [Електронний ресурс]. – Режим доступу: http://www.pcweek.ru/ security/article/detail.php?ID=151005.

10. Про основи національної безпеки України: Закон України від 19.06.2003 № 964-IV [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/964-15.

11. Про кіберзлочинність: Конвенція Ради Європи // Офіційний вісник України. – 2007. – № 65. – С. 107. – Ст. 2535. – Код акта 40846/2007. – 10 вересня.

12. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: Указ Президента України від 31.07.2000 № 928/2000 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/ laws/show/928/2000.

13. Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних: Указ Президента України від 24.09.2001 № 891/2001 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/891/2001

14. Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС: Положення про Управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України, затверджене наказом МВС України від 30.10.2012 № 988 [Електронний ресурс]. – Режим доступу: http://document.ua/pro-organizaciyu-dijalnosti-upravlinnja-borotbi-z-kiberzloch-doc130740.html.

15. Кримінальний кодекс України від 05.04.2001 № 2341-III, Редакція від 17.05.2014, підстава 1194-18 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/2341-14.

16. Кримінально-процесуальний кодекс України від 28.12.1960 № 1001-05 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/1001-05.

17. Про боротьбу з тероризмом від 20.03.2003 № 638-IV: Закон України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/ laws/show/638-15/print1409665648697960.

Зачек О. И. Правовые проблемы противодействия киберпреступникам, действующим из-за границ Украины

Рассмотрены правовые проблемы противодействия киберпреступникам, действующим из-за границ Украины. Приводятся примеры кибератак на украинские информационные системы и сайты в период проведения антитеррористической операции на востоке Украины. Определены правовые основания борьбы с киберпреступлениями. Рассмотрены проблемы, возникающие вследствие невозможности задержания преступников, которые осуществляют кибератаки против украинских информационных систем из-за границ Украины. Сформулированы предложения по внесению изменений в законодательство с целью эффективного противодействия киберпреступникам в описанных случаях.

Ключевые слова: *киберпреступления, кибертерроризм, кибератаки, хакерские методы, правовые проблемы.*

Zachek O. I. Legal problems of combating cybercriminals acting from abroad of Ukraine

The article deals with the legal problems of combating cybercriminals acting from abroad of Ukraine. The number of attacks on information systems significantly increased in the last time. The number of cyber attacks on information systems and Ukrainian sites especially increased during the antiterrorist operation in eastern Ukraine. The article gives examples of cyber attacks. Such actions of cybercriminals are elements of cyberwar and are trying to implement technical intelligence and disorganization of Ukrainian authorities. Also, these steps of criminals can be described as cyberterrorism. The main problem of counteraction to such criminals is their location outside of the reach of the law enforcement agencies of Ukraine and possible support them by special services of hostile state. As a result there is no possibility to detain them and exclude the tools of crime. It is necessary to use alternative and adequate methods to protect national security from cyber attacks, where criminals operate with the support by intelligence services of the hostile state, that there is a state cyberterrorism. Numerous cases of use hacking technologies by law enforcement agencies of other countries are now. Of course, these methods can cause a well-deserved criticism, but in our opinion, in exceptional cases, when it comes to national security of Ukraine, their use is appropriate according to court decision. The legal basis of application of such methods must be created. The article describes the legal basis of fight against cybercrime. Are given suggestions on changes to the legislation in order to effectively counteraction cybercriminals in case they can not be detained due to actions from outside Ukraine, including the amendments to the Law of Ukraine «On Combating Terrorism».

Key words: *cybercrime, cyberterrorism, cyber attacks, hacking techniques, legal problems.*

Стаття надійшла 8 грудня 2014 р.