УДК 65.012.8

І. М. РЯЗАНЦЕВА,
кандидат юридичних наук,
доцент кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ;

В. В. ТУЛУПОВ,
кандидат технічних наук, доцент,
начальник кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ПРОБЛЕМНІ ПИТАННЯ РОЗБУДОВИ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

Проаналізовано концептуальну нормативно-правову базу у сфері розбудови національної системи кібербезпеки. Розкрито суб'єкти систем кібербезпеки. Запропоновано основні напрями розбудови системи кібербезпеки із прив'язкою до конкретних суб'єктів реалізації. Підкреслено потребу врахування терористичних загроз під час створення системи кібербезпеки. Досліджено особливості підготовки фахівців у сфері кібербезпеки, проаналізовано міжнародний досвід. На підставі проведеного аналізу запропоновано впроваджувати у систему забезпечення кібербезпеки програмне забезпечення аналітичної обробки накопиченої інформації з подальшим прийняттям рішень.

Ключові слова: *нормативно-правова база, напрямки розбудови системи кібербезпеки, суб'єкти системи кібербезпеки, підготовка фахівців, кібертероризм.*

За останні десятиліття інформація стала настільки потужним фактором розвитку суспільства, що привела до утворення нового інформаційного укладу, який сприяє внутрішньодержавній і світовій інтеграції та реінтеграції. Україна на теперішній час міцно стала на шлях впровадження нових технологій. Це, у свою чергу, зумовлює потребу у розбудові якісної системи кібербезпеки.

Вивченням цього питання в Україні займалися О. Бандурка, Д. Дубов, В. Захаров, М. Літівінов, О. Манжай, М. Ожеван, Ю. Орлов та багато інших науковців.

З точки зору розбудови ефективної системи кібербезпеки основоположною є нормативно-правова база для її запровадження. У цьому сенсі можна виділити низку концептуальних нормативно-правових актів:

– Конституція України [1], у ст. 17 якої відзначається, що забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього Українського народу;

– Конвенція про кіберзлочинність [2], відповідно до норм якої країни-учасниці повинні здійснити низку заходів на національному рівні, спрямованих на боротьбу з кіберзлочинами;

– Закон України «Про основи національної безпеки України» [3], в якому на законодавчому рівні було закріплено основні принципи забезпечення національної безпеки взагалі та інформаційної безпеки зокрема;

– Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [4], у якому на законодавчому рівні закріплено визначення терміна «інформаційна безпека»;

– Стратегія національної безпеки України «Україна у світі, що змінюється» [5], яка відповідно до законодавства визначає загальні принципи, пріоритетні цілі, завдання і механізми захисту життєво важливих інтересів особистості, суспільства та держави від зовнішніх і внутрішніх загроз, у тому числі у сфері забезпечення інформаційної безпеки, зокрема, створення національної системи кібербезпеки.

Названими нормативними актами база для розбудови системи кібербезпеки не вичерпується, однак за допомогою їх аналізу можна уявити кістяк, на основі якого потрібно формувати суб'єктно-об'єктну модель такої системи.

На теперішній час організаційна структура забезпечення кібербезпеки України представлена трьома основними суб'єктами: Службою безпеки України (Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки), Державною службою спеціального зв'язку та захисту інформації України (Державний центр захисту інформаційно-телекомунікаційних систем), МВС України

(Управління боротьби з кіберзлочинністю у складі блоку кримінальної міліції).

Також наприкінці червня 2014 року у складі Національної гвардії України планується створити Управління інформаційної безпеки, функціями якого мають стати взаємодія та оперативне управління інформаційними потоками в режимі бойової обстановки.

Координація дій між цими відомствами, на жаль, перебуває не на найкращому рівні через розбалансованість системи влади. У зв'язку з цим вважаємо виправданим зосередити координаційну функцію у сфері забезпечення системи кібербезпеки у Державній службі спеціального зв'язку та захисту інформації України, яка на сьогодні має найбільший досвід щодо убезпечення державних електронних інформаційних ресурсів.

Також вважаємо за потрібне скоригувати систему загроз у сфері кібербезпеки України відповідно до стандартів НАТО, а також викликів, з якими стикається Україна сьогодні.

У цьому сенсі можна виділити гібридні дії екстремістів на сході України, які поєднують у собі активну терористичну діяльність, здійснення інформаційного впливу на свідомість громадян та кіберзлочини. Причому така діяльність здійснюється щонайменше за інформаційної підтримки іноземних джерел, серед яких можна назвати, наприклад, Е. Лімонова [6], С. Удальцова [7] тощо. На думку російського науковця В. М. Янгола, вказані особи очолюють екстремістські організації [8, с. 98, 99]. Таким чином, очевидним у цьому випадку є не лише підтримка екстремістських проявів в Україні громадянами іншої держави, але і створення передумов до порушення безпеки інформаційного простору України з використанням мережі Інтернет. У свою чергу дії так званої організації «Кіберберкут» [9] свідчать про міцні зв'язки тероризму та кіберзлочинності.

У цьому сенсі в рамках розбудови такого напряму системи кібербезпеки, як протидія терористичним загрозам, слушними видаються пропозиції В. М. Янгола: виробити єдину концепцію інформаційно-пропагандистського забезпечення антитерористичної діяльності; створити інформаційний банк про терористичні організації, конкретних осіб, підозрюваних у терористичній діяльності; скоординовано здійснювати спільний контроль за їх переміщенням та джерелами фінансування; забезпечити гарантований швидкий та зручний доступ до інформації усіх суб'єктів антитерористичної діяльності [8, с. 181].

Протидія інформаційній війні та інформаційному тероризму є одним з напрямів забезпечення інформаційної безпеки як складової частини національної безпеки. Механізми протидії зазначеним загрозам мають бути високотехнологічними та мати системний характер [10, с. 26]. Ось чому, наприклад, у США створюють базу терористів у вигляді соціальної мережі [11]. Вказана новація розрахована на нове покоління правоохоронців, яким таким чином буде значно зручніше виконувати покладені на них обов'язки.

На нашу думку, взагалі украй важливо впроваджувати у систему забезпечення кібербезпеки автоматизацію аналітичної обробки одержаної та накопиченої інформації. З цією метою можуть бути використані системи Кронос, Splunk.

Вельми цікавою видається розробка американських спеціалістів, що має назву RIOT (Rapid Information Overlay Technology), яку розробив американський військовий підрядник Raytheon в 2010 році. Це система, створена для швидкого витягання інформації про підозрюваних громадян із соціальних мереж, в тому числі Facebook, Twitter і Foursquare [12].

Разом із урахуванням наведених факторів під час розбудови національної системи кібербезпеки в обов'язковому порядку потрібно враховувати прогностичну складову. В цьому сенсі в нагоді українським фахівцям можуть стати прогнози експертів Європолу, які вважають, що до 2020 року межа між кібератакою та фізичним нападом на людину у багатьох випадках буде стерта. Найбільш поширеними комп'ютерними атаками стануть:

1. Розвиток ринку скремблерів розпізнавання настрою користувачів, симуляції дистанційної присутності, технології Near Field Communication.
2. Розподілені DoS-атаки через хмарні сервіси.
3. Використання хмарних ботнетів і розподілених обчислювальних ресурсів.
4. Сталий ринок викрадених та підроблених віртуальних елементів.
5. Розподілені захищені кримінальні обчислення.
6. Фізичні атаки на дата-центри і точки обміну трафіком.
7. Електронні атаки на критичну інфраструктуру, включаючи джерела енергії, транспорт й інформаційні служби.
8. Мікрозлочинність, включаючи крадіжку і генерацію фальшивих мікроплатежів.

9. Біозломи елементів багатофакторної автентифікації.

10. Насильство проти людей із використанням комп'ютерів, поява шкідливих програм для людей.

11. Війни киберугруповань.

12. Кваліфікована кримінальна розвідка, включаючи дата-майнінг великих об'ємів даних.

13. Збільшення атак імперсонації.

14. Складні маніпуляції з репутацією.

15. Підміна реальних даних та шахрайства з використанням соціального інженірінгу.

16. Використання безпілотних апаратів і роботів у злочинних цілях.

17. Хакреські атаки проти сполучних пристроїв із безпосереднім доступом (міжмашинні комунікації, індикатори відображення важливої інформації – Heads-Up Display тощо) [13].

Узагальнюючи наведене, доходимо висновку, що розбудову національної системи кібербезпеки слід здійснювати за трьома основними напрямами:

1) протидія кіберзлочинності;

2) захист вітчизняного інформаційного простору в комп'ютерних мережах;

3) забезпечення інформаційної безпеки критичної інфраструктури.

У рамках розбудови підсистеми протидії кіберзлочинності слід враховувати її «всеосяжний» характер. З огляду на вітчизняне кримінальне законодавство до категорії кіберзлочинів у першу чергу віднесені суспільно небезпечні винні діяння, передбачені статтями розділу XVI Кримінального кодексу України. З урахуванням правоохоронної практики до цієї групи можна віднести й інші діяння, які в більшості випадків здійснюються з використанням Інтернету або електронно-обчислювальної техніки, зокрема такі, що передбачені ст. 176, 177, 185, 190, 200, 203-2, 209, 229, 231, 301 Кримінального кодексу тощо.

Серед кіберзлочинів все більше стає «міжнародних», таких, які як засоби/жертви використовують інформаційні системи різних держав. Через відкриті інформаційні мережі можливий доступ до національних, в тому числі і спеціально захищених інформаційних ресурсів різних держав. Відповіддю міжнародної спільноти глобальному кримінальному світу стала Конвенція ООН проти транснаціональної організованої злочинності [14], що мала допомогти державам у вирішенні спільної проблеми, і відповідно до якої, ці документи не застосовуються стосовно правопорушень, які не відносяться до організованої злочинності, розглядаючи як виняток тільки окремі сфери – особливо корупцію і комп'ютерні правопорушення, що вчиняються окремими особами. Конвенція застосовується у тих випадках, коли «відповідний злочин має «транснаціональний характер». Функції щодо забезпечення протидії кіберзлочинності, очевидно, потрібно зосередити в системі МВС України.

У рамках другого напряму розбудови системи кібербезпеки *(захист вітчизняного інформаційного простору)* слід упровадити підсистему активних операцій з інформаційного впливу. Його здійснення слід організовувати у рамках політики інформаційного протиборства з використанням можливостей Служби безпеки України. Класичними прийомами інформаційного впливу під час доведення інформації є використання певного набору характеристик: видовищність, порушення звичної моделі миру, примушуюча пропаганда, «наклеювання ярликів», «тролінг» (активна участь у багатьох дискусіях під вигаданими іменами), копіпастинг [15].

Обов'язок щодо *забезпечення інформаційної безпеки критичної інфраструктури* має бути покладений на Державну службу спеціального зв'язку та захисту інформації України, яка на теперішній час має досить багато напрацювань як у сфері створення систем захисту об'єктів інформаційної діяльності, так і щодо побудови комплексних систем захисту інформації в автоматизованих системах.

Для забезпечення ефективної роботи спеціалістів у системі національної кібербезпеки слід ретельно підійти до набору кадрів, а також до організації їх підготовки. Прикладом навчального закладу, який здатен надавати таку підготовку в системі МВС України, є Харківський національний університет внутрішніх справ.

Особливу увагу при цьому потрібно приділяти практичній складовій навчання. Для цього необхідно не лише проводити класичну підготовку силами кафедр, але і створити навчальну лабораторію, яка б дозволяла вирішувати завдання:

– навчання прикладним навичкам забезпечення кібербезпеки з використанням правових, організаційних та програмно-технічних рішень;

– розробки науково-методичного забезпечення тактико-технічних особливостей забезпечення кібербезпеки;

– супроводження технічного обладнання;

– залучення до виконання консультативних та експертних завдань.

Досвід функціонування подібних лабораторій у частині протидії кіберзлочинності існує у провідних вищих навчальних закладах світу. Так, в університеті Пердью (США) функціонує «The Purdue University Cyber Forensics Lab», яка окрім суто наукових та навчальних функцій залучається до проведення комп'ютерно-технічних експертиз. Подібний підрозділ (UCD Centre for Cybersecurity & Cybercrime Investigation) існує й у провідному європейському виші з надання освіти у сфері протидії кіберзлочинності Дублінському університетському коледжі (University College Dublin). Вказані лабораторії надають також платні послуги з дистанційного навчання. Повний курс дистанційного навчання у Дублінському університетському коледжі з питань протидії кіберзлочинності коштує близько 7 тис. євро.

Підсумовуючи, слід наголосити, що проблема створення ефективної системи кібербезпеки є не лише національною, але й міжнародною.

Запорукою ефективної розбудови такої системи є високий рівень культури та професійної підготовки фахівців із забезпечення інформаційної безпеки. Гарантувати ефективну протидію кібернетичним загрозам в Україні може лише застосування комплексних підходів до забезпечення інформаційної безпеки. Сьогодні наша держава повинна здійснювати активні кроки:

– у розбудові власної системи кібербезпеки;

– активно розвивати співробітництво між державами і приватним безпековим сектором, безпековими установами та приватними компаніями, задіяними у сфері інформаційно-комунікаційних технологій;

– завершити роботу із визначення структури і завдань єдиної загальнодержавної системи протидії кіберзлочинності.

Список використаних джерел

1. Конституція України : від 28.06.1996 // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

2. Конвенція [Ради Європи] про кіберзлочинність : від 07.09.2005 ; ратиф. Верховною Радою України 07.09.2005 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575.

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

4. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : закон України від 09.01.2007 № 537-V [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/537-16.

5. Стратегія національної безпеки України «Україна у світі, що змінюється» : затв. указом Президента України від 12.06.2007 № 105 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/105/2007. – В редакції від 08.06.2012.

6. Лимонов Э. Блог / Эдуард Лимонов [Електронний ресурс]. – Режим доступу: http://echo.msk.ru/blog/limonov/.

7. Удальцов С. Блог / Сергей Удальцов [Електронний ресурс]. – Режим доступу: http://echo.msk.ru/blog/udaltsov/.

8. Янгол В. Н Оперативно-розыскное противодействие политическому терроризму : дис. … канд. юрид. наук : 12.00.09 / Янгол Владимир Николаевич. – СПб., 2006. – 201 с.

9. Киберберкут [Електронний ресурс]. – Режим доступу: http://vk.com/cyberberkut1.

10. Манжай О. В. Правові засади захисту інформації : навч. посіб. / О. В. Манжай. – Харків : НікаНова, 2014. – 104 с. : іл.

11. Reilly R. B. Modus Operandi is building a 'Facebook' for tracking terrorists / Richard Byrne Reilly // Venturebeat [Електронний ресурс]. – Режим доступу: http://venturebeat.com/2014/06/21/modus-operandi-is-building-a-facebook-for-tracking-terrorists/. – June, 2014.

12. Gallagher R. Software that tracks people on social media created by defence firm [Електронний ресурс] / Ryan Gallagher // The Guardian. – 10 Feb. 2013. – Режим доступу: http://www.guardian.co.uk/world/2013/feb/10/software-tracks-social-media-defence.

13. Project 2020 : Scenarios for the Future of Cybercrime – White Paper for Decision Makers [Електронний ресурс] / International Cyber Security Protection Alliance ; European Cybercrime Centre. – 25 p. – Режим доступу: https://www.europol.europa.eu/sites/default/files/publications/2020_white_paper.pdf.

14. Конвенция Организации Объединенных Наций против транснациональной организованной преступности : прин. резолюцией 55/25 Ген. Ассамблеи от 15 нояб. 2000 г. [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml.

15. Зеленина Е. В Королевстве кривых зеркал… / Е. Зеленина // Время. – 17 дек. 2013 г. – № 181 (17337). – С. 2.

Надійшла до редколегії 20.06.2014

РЯЗАНЦЕВА И. М., ТУЛУПОВ В. В. ПРОБЛЕМНЫЕ ВОПРОСЫ ПОСТРОЕНИЯ НАЦИОНАЛЬНОЙ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ

Проанализирована концептуальная нормативно-правовая база в сфере построения национальной системы кибербезопасности. Раскрыты субъекты системы кибербезопасности. Предложены основные направления построения системы кибербезопасности с привязкой к конкретным субъектам реализации. Подчеркнута потребность учета террористических угроз во время создания системы кибербезопасности. Исследованы особенности подготовки специалистов в сфере кибербезопасности, проанализирован международный опыт. На основании проведенного анализа предложено внедрять в систему обеспечения кибербезопасности программное обеспечение аналитической обработки накопленной информации с последующим принятием решений.

Ключевые слова: *нормативно-правовая база, направления построения системы кибербезопасности, субъекты системы кибербезопасности, подготовка специалистов, кибертерроризм.*

RIAZANTSEVA I. M., TULUPOV V. V. ISSUES OF NATIONAL CYBERSECURITY SYSTEM CONSTRUCTION

The conceptual regulatory base in the sphere of developing national cybersecurity system is analyzed in the article. Some provisions of every regulatory act are revealed. The vastness of above list of regulatory acts is emphasized. The existing and operating structure of cybersecurity system is disclosed. It is offered to provide the State Service for Special Communication and Information Protection of Ukraine with the coordinating function in the sphere of cybersecurity system's functioning. Based on the analysis the authors insist that there is a strong link between terrorist groups and cybercriminals, who recently has been affecting the cybersecurity system of Ukraine. The importance of prognostic function for developing an effective cybersecurity system is stressed. The basic directions of developing such a system with the reference to specific subjects of realization are offered: 1) cybercrime counteraction; 2) protection of the national information space within computer networks; 3) provision of information security of the critical infrastructure. Examples of realizing information confrontation are presented and cybercrime structure under Ukrainian law is generally revealed. The features of training specialists in the field of cyber security are researched; the international experience is analyzed. The authors noted on the necessity to implement a network of special laboratories within the system of training specialists. They would solve the following problems: teaching applied skills to ensure cybersecurity with the usage of legal, organizational, and software and hardware solutions; development of scientific and methodical provision of tactical and technical characteristics of cybersecurity guaranteeing; technical support of equipment; involvement in realizing advisory and expert missions. Based on the analysis the authors offer to implement software of analytical processing of the accumulated information with the further decisions making into the cybersecurity system. Examples of such software and modern developments in this area are provided.

Keywords: *regulatory base, directions of cybersecurity system construction, subjects of cybersecurity system, specialists training, cyberterrorism.*

УДК 343.55

І. В. СЕМЕНОГОВ,
аспірант
Харківського національного університету внутрішніх справ

ЗАГАЛЬНІ ПИТАННЯ КРИМІНАЛЬНО-ПРАВОВОЇ ХАРАКТЕРИСТИКИ ДІЯННЯ У СКЛАДАХ ЗЛОЧИНІВ, ПЕРЕДБАЧЕНИХ СТАТТЯМИ 164 ТА 165 КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ

Досліджено питання змісту, ознак та форм діяння, яке входить до об'єктивної сторони ухилення від сплати аліментів на утримання дітей або від сплати коштів на утримання непрацездатних батьків (ст. 164, 165 КК України). Метою роботи є уточнення кримінально-правової характеристики ухилення від сплати аліментів на утримання дітей або від сплати коштів на утримання непрацездатних батьків. У дослідженні використано діалектичний метод, формально-логічний (догматичний) метод та системно-структурний аналіз.

Ключові слова: *діяння, об'єктивна сторона злочину, ухилення від сплати, аліменти, злочинна бездіяльність, критерії бездіяльності.*