ЛІТЕРАТУРА

1. Єдиний звіт про кримінальні правопорушення. Генеральна прокуратура України: сайт. URL: http://www.gp.gov.ua/ua/stst2011.html?dir_id=110381&libid=100820.
2. Мартинюк А. Дослідження незаконних потоків зброї. URL: http://www.smallarmssurvey.org/fileadmin/docs/T-Briefing-Papers/SAS-BP3-Ukraine-UKR.pdf.
3. Про мисливське господарство та полювання: Закон України від 22 лютого 2000 р. № 1478-III. Відомості Верховної Ради України (ВВР). 2000. № 18. Ст. 132; зі змінами станом на 10 березня 2017 р. URL: http://zakon.rada.gov.ua/laws/show/1478-14.
4. Про поводження з вибуховими матеріалами промислового призначення: Закон України від 23 грудня 2004 р. № 2288-IV. Відомості Верховної Ради (ВВР). 2005. № 6. Ст. 138; зі змінами станом на 18 грудня 2017 р. URL: http://zakon.rada.gov.ua/laws/show/2288-15.
5. Про ліцензування видів господарської діяльності: Закон України від 01 червня 2000 р. № 222-VIII. Відомості Верховної Ради (ВВР). 2015. № 23. Ст. 158; зі змінами станом на 28 вересня 2017 р. URL: http://zakon.rada.gov.ua/laws/show/222-19.
6. Про право власності на окремі види майна: постанова Верховної Ради України від 17 червня 1992 р. № 2471-XII. Відомості Верховної Ради України (ВВР). 1992. № 35. Ст. 517; зі змінами станом на 24 січня 1995 р. URL: http://zakon.rada.gov.ua/laws/show/2471-12.
7. Інструкція про порядок виготовлення, придбання, зберігання, обліку, перевезення та використання вогнепальної, пневматичної, холодної і охолощеної зброї, пристроїв вітчизняного виробництва для відстрілу патронів, споряджених гумовими чи аналогічними за своїми властивостями метальними снарядами несмертельної дії, та патронів до них, а також боєприпасів до зброї, основних частин зброї та вибухових матеріалів: наказ Міністерства внутрішніх справ України від 21 серпня 1998 р. № 622; зі змінами станом на 15 травня 2018 р. URL: http://zakon.rada.gov.ua/laws/ show/z0637-98.
8. Про судову практику в справах про викрадення та інше незаконне поводження зі зброєю, бойовими припасами, вибуховими речовинами, вибуховими пристроями чи радіоактивними матеріалами: постанова Пленуму Верховного Суду України від 26 квітня 2002 р. № 3. URL: http://zakon.rada.gov.ua/laws/show/v0003700-02.
9. Кіріленко Ф., Загорулько А. Незаконний обіг зброї і стан боротьби зі злочинами, вчиненими з її використанням. Национальный юридический журнал: теория и практика. 2017. № 12. С. 119–123. URL:http://www.jurnaluljuridic.in.ua/archive/2017/6/part_2/26.pdf.
10. Задоян А.А., Мацкевич И.М., Чучаев А.И. Проблемы криминологического предупреждения незаконного оборота оружия: монография. М.: МГЮА, 2017. С. 127.
11. Рибачук В.І. Кримінально-правові та кримінологічні аспекти боротьби з незаконними діяннями при поводженні зі зброєю, бойовими припасами та вибуховими речовинами: автореф. дис. … канд. юрид. наук: 12.00.08; Одеська національна юридична академія. О., 2001. С. 21.
12. Кулик Л.М. Правові чинники незаконного обігу зброї в Україні. Право і суспільство. 2011. № 2. С. 180–185. URL: http://nbuv.gov.ua/UJRN/ Pis_2011_2_39.
13. Результати роботи поліції за 12 місяців 2017 р. з протидії незаконному обігу зброї: Міністерство внутрішніх справ України від 12 січня 2018 р. URL: http://mvs.gov.ua/ua/news/11656_U_2017_roci_Nacpoliciya_viluchilaz_nezakonnogo_obigu_ponad_dvi_tisyachi_granat_INFOGRAFIKA_FOTO.htm.

УДК 342.9

ПРАВОВИЙ СТАТУС КІБЕРПОЛІЦІЇ ЯК СУБ'ЄКТА ПРОТИДІЇ ЗЛОЧИННОСТІ: НАЦІОНАЛЬНИЙ І ЗАРУБІЖНИЙ ДОСВІД

THE LEGAL STATUS OF CYBERPOLICE AS A SUBJECT TO COUNTERING CRIME: NATIONAL AND FOREIGN EXPERIENCE

Тимошенко О.О., студентка
Навчально-науковий інститут права
Сумського державного університету

Стаття присвячена одній з актуальних тем кримінального права щодо правового статусу правоохоронного органу, який протидіє кібернетичним загрозам на національному рівні. Автори аналізують зарубіжний досвід функціонування суб'єктів попередження кіберзлочинів провідних країн світу. Кіберполіція у процесі реалізації державної політики у сфері кіберзлочинності за своїми технічними та професійними можливостями забезпечує реагування на кіберзагрози. Проте сучасні виклики і небезпеки інформаційного простору потребують системного реагування у сфері модернізації суб'єкта і системи для ефективного та швидкого запобігання кіберзлочинам.
Ключові слова: кіберполіція, напрями протидії кіберзлочинності, попередження хакерських атак, підготовка спеціалістів.

Статья посвящена одной из актуальных тем уголовного права относительно правового статуса правоохранительного органа, который противодействует кибернетическим угрозам на национальном уровне. Авторы анализируют иностранный опыт функционирования субъектов предотвращения киберпреступлений ведущих стран мира. Киберполиция в процессе реализации государственной политики в сфере киберпреступности по своим техническим и профессиональным возможностям обеспечивает реагирование на киберугрозы. Но, несмотря на это, современные вызовы и опасности информационного пространства требуют системного реагирования в сфере модернизации субъекта и системы для эффективного предотвращения киберпреступлений.
Ключевые слова: киберполиция, направления противодействия киберпреступности, предупреждение хакерских атак, подготовка специалистов.

The article is devoted to the coverage of one of the topical issues of criminal law regarding the legal status of a law enforcement agency that counteracts cyber threats at the national level. In addition, the authors analyze the foreign experience of the functioning of subjects promoting the cybercrime of the leading countries of the world. Foreign experience of law enforcement agencies in countering cybercrime is necessary to improve the national system of cyberpolicy cooperation with auxiliary intelligence services in the direction of countering cyber attacks.

Cyberpolice, in the process of implementing state policy in the field of cybercrime, by its technical and professional capabilities, provides response to cyber threats. However, due to the modern challenges and dangers of the information space, require a systemic response to the modernization of the subject and the system for the effective and rapid prevention of cybercrime. The investigation of cybercrime requires the application of new knowledge and skills and the training of competent personnel. In addition, professionals in this field should be able to act quickly to identify criminals and provide evidence of crimes before they are removed. In addition to the special skills required for the cyberpolice unit,

all police officers must be knowledgeable in the expert field, that is, specialize in the mechanism for conducting a forensic examination of digital evidence.

Countering cybercrime includes three areas of activity, that is, prevention of cyber attacks, the general organization of the fight against cybercrime and law enforcement activities aimed specifically at identifying, suppressing and disclosing cybercrime, applying criminal liability and punishment measures against persons who have committed a wrongful act in this field.

Key words: cyber police, ways to counter cybercrime, prevention of hacker attacks, training of specialists.

В епоху інформаційних технологій виникає проблема кіберзлочинності. Один із її ключових аспектів – анонімність глобальних інформаційних мереж, швидкість передачі інформації та легкість її використання, що дає змогу застосовувати всі ці переваги для здійснення незаконних дій. Глобальний і транскордонний характер цих злочинів сягає значних масштабів. Тому боротьба з кіберзлочинністю є першочерговим завданням забезпечення суверенітету України. Такий орган із захисту прав людини, як кіберполіція, за своїми технічними та професійними можливостями забезпечує реагування на кіберзагрози. Проте сучасні виклики та загрози інформаційному простору вимагають систематичної відповіді у сфері модернізації суб'єкта та системи для ефективного запобігання злочинам в інформаційній сфері.

О.М. Бандурка й О.М. Литвинов зазначають, що протидія злочинності є особливим інтегрованим і багаторівневим об'єктом соціального управління, який включає різноманітну за формами діяльність відповідних суб'єктів, що взаємодіють у вигляді системи різнорідних заходів, спрямованих на пошук способів та інших можливостей ефективного впливу на злочинність із метою зниження інтенсивності процесів детермінації злочинності на всіх рівнях дії, її причин та умов для обмеження кількості злочинних проявів [1, с. 44].

Особливе місце на національну рівні в боротьбі зі злочинами, пов'язаними з протиправним використанням комп'ютерної інформації та комп'ютерних технологій, посідають Департамент кіберполіції Національної поліції України. Він є міжрегіональним територіальним органом Національної поліції України та здійснює оперативно-розшукову діяльність. Цей орган регламентується наказом Кабінету Міністрів України № 831 від 13 жовтня 2015 р. «Про утворення територіального органу Національної поліції» та Положенням про Департамент кіберполіції Національної поліції України № 85 від 10 листопада 2015 р. [2; 3].

Структурні та системні зміни модернізації кіберзлочинності передбачають забезпечення висококваліфікованих працівників у цій галузі. Такі перспективи зумовлюють атестацію працівників підрозділів Національної поліції, які безпосередньо протидіють злочинності. Факультет Харківського національного університету внутрішніх справ – єдиний факультет в Україні, який готує фахівців для підрозділів із боротьби з кіберзлочинністю. Для курсантів діє навчально-тренувальний центр протидії кіберзлочинності та моніторингу кіберпростору.

У США, у штаті Вірджинія, знаходиться академія ФБР, яка пропонує всебічний курс для правоохоронних органів. Мета полягає у підвищенні стандартів правоохоронної діяльності та співпраці в поліцейських департаментах та агенціях в усьому світі. Акцент робиться на підготовці до протидії сучасним викликам за допомогою інноваційних методів, вищої освіти / досліджень і мережі партнерських відносин. Освіта в підрозділі кіберзлочинності вважається досить кваліфікованою, однак її нелегко отримати. Фахівці, які випускаються, є компетентними у сфері кіберзлочинності. Після успішного навчання особи направляються працювати до кіберпідрозділу ФБР. Кіберкоманда передбачає діяльність щодо розгортання тактичних і розвідувальних дій по всій країні і світу. Ці підрозділи включають висококваліфіковані тактичні кадри, навчені контролювати, переслідувати і затримувати злочинців і терористів навіть у найскладніших і найекстремальніших умовах. Також у команді працюють аналітики розвідки, які можуть розслідувати комп'ютери злочинців для отримання критичної інформації та передачі їх відповідному персоналу. Над вивченням нових явищ і прогнозуванням працюють вчені, котрі володіють великим досвідом у різних аспектах інформатики. Вони можуть мати знання в галузі судової експертизи, безпеки, міжмережевої взаємодії, програмування, мережевої архітектури або системного адміністрування [4].

Спираючись на зарубіжний досвід, пропонуємо створити спеціальну академію при МВС, яка б готувала фахівців із протидії кіберзлочинам. Необхідно внести ряд змін до українського законодавства. Також державна політика повинна бути спрямована на обмін досвідом між суб'єктами правоохоронних органів, що дало б змогу кіберполіції перейняти досвід фахівців у цій сфері й організувати висококваліфіковану підготовку з урахуванням особливостей кіберзлочинності в усьому світі.

У зв'язку з багатогранністю кіберзлочинів необхідно визначитися з ефективними напрямами протидії.

Перший напрям передбачає запобігання кіберзлочинам, тобто створення, сертифікацію, ліцензування і впровадження необхідних засобів технічного і програмного захисту інформації, прогнозування розвитку технологій кібербезпеки щодо засобів мобільного зв'язку, інфраструктури електронних комунікацій, розробку і вдосконалення системи державного контролю інформаційної безпеки, а також системи незалежного аудиту інформаційної безпеки, мережевих відповідних груп для комп'ютерних надзвичайних ситуацій, захисту особистих даних [5, с. 6].

Другий напрям протидії кіберзлочинності включає виявлення та призупинення кіберзлочинів. Одним із ключових аспектів є вирішення проблеми організації ефективної взаємодії всіх суб'єктів протидії кіберзлочинності. Таким чином, функціонування допоміжних спеціалізованих організаційних структур адміністрацій і служб комп'ютерної безпеки, завданням яких є забезпечення надійного функціонування засобів захисту, є необхідним елементом цих структур для організації та ведення державного реєстру об'єктів критичної інфраструктури. Багатогранність суб'єктів боротьби з кіберзлочинністю включає багаторівневу координацію їхньої діяльності [6, с. 219].

Третій напрям боротьби з кіберзлочинністю передбачає застосування заходів кримінальної відповідальності та покарання до осіб, які вчинили кіберзлочин. У зв'язку з цим зазначимо, що в національному законодавстві кіберзлочини передбачено і закріплено в окремому Розділі XVI Кримінального кодексу України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [7].

Потреба реалізації ефективних заходів із протидії сучасним кібернетичним загрозам на національному рівні залишається актуальною для багатьох країн. Діяльність кіберпідрозділу ФБР США передбачає роботу щодо припинення дій викрадачів даних і саботажників, які атакують мережі підприємств. Втрати, спричинені корпоративним шпигунством і корупцією даних, щорічно сягають мільярдів доларів і становлять серйозну загрозу для економіки США. Інтенсивний контроль за кримінальною діяльністю в мережі Інтернет здійснює ФБР США. У складі ФБР США у 1996 р. створено Кіберпідрозділ, який функціонує на правах окремого управління в структурі ФБР.

На нього покладено функцію надання допомоги іншим підрозділам ФБР у розслідуванні злочинів, вчинених із використанням комп'ютерних і телекомунікаційних технологій. Кіберпідрозділ ФБР має чотири відділи: протидії незаконним втручанням у роботу комп'ютерних мереж, протидії дитячій порнографії, протидії шахрайствам, протидії порушенням у сфері інтелектуальної власності. Працює також Цілодобовий командний центр кіберспостереження (CyWatch), який у разі значних кібератак об'єднає ресурси ФБР і NCIJTF. Це забезпечує зв'язок юридичних аташе на місцях і приватного сектору з федеральними кіберцентрами, урядовими установами й офісами ФБР. Ці Cyber Action команди (CAT) складаються зі спеціальних агентів, комп'ютерних судових експертів та аналітиків розвідки [8].

Національне бюро з боротьби з шахрайством (NFIB) у Великій Британії є національним поліцейським лідером у сфері боротьби з кіберзлочинністю. Діяльність NFIB спрямована на боротьбу з шахрайством і кіберзлочинністю, виявлення послідовних злочинців, організованих злочинних угруповань, а також нових видів злочинів. NFIB отримує дані за трьома основними напрямами: координації приватних осіб і малого бізнесу (що надходять або безпосередньо, або через поліцейські сили), шахрайства у промисловості і державному секторі, включаючи банківські, страхові, телекомунікаційні й урядові відомства, різних джерел розвідки, включаючи, але не обмежуючись, національні та міжнародні поліцейські системи злочинності / розвідки. NFIB використовує систему під назвою «Know Fraud». Це надзвичайно досконала поліцейська розвідувальна система, здатна обробляти величезні обсяги даних, щоб виявити кібератаки. Аналітики й аналітики криз NFIB проводять аналіз вияву кібератак і звітують про це правоохоронним органам або партнерським агентствам для вжиття заходів.

У Французькій Республіці в 1994 р. було створено «Службу протидії зловживанням у сфері інформаційних технологій». Цей підрозділ підпорядковується Управлінню паризької кримінальної поліції, основним завданням якого є боротьба з «інтелектуальним» піратством і «хакінгом». У лютому 2008 р. Міністр внутрішніх справ Франції Мішель Алліот-Марі оприлюднив французьку Стратегію з питань боротьби з кіберзлочинністю. Мета Стратегії – співпраця між приватним бізнесом (постачальником інформаційно-телекомунікаційних послуг) і правоохоронними органами з метою обміну інформацією й об'єднання зусиль у боротьбі з кіберзлочинністю [9, с. 245].

Невелика прибалтійська держава Естонія славиться високим рівнем кібератак. У цій державі не існує структурного підрозділу кіберполіції, проте в 2006 р. створено комп'ютерну групу реагування на надзвичайні ситуації CERT Estonia (Computer Emergency Response Team of Estonia). Ця команда відповідає за контроль інцидентів із кібербезпеки, працює над попередженням кібершахрайства щодо естонських користувачів, консультує їх щодо кіберзагроз і засобів захисту. Також команда CERT Estonia відпрацьовує інциденти з ІБ в мережах естонських комерційних компаній.

Таким чином, можемо зробити **висновок**, що кіберполіція є важливим суб'єктом протидії кіберзлочинності. Її діяльність ґрунтується на попередженні, виявленні та розкритті злочинів у сфері інформаційних технологій у кіберпросторі. Підготовка спеціалістів до протидії з кіберзлочинністю передбачає удосконалення вмінь і навичок у цій сфері. Крім того, для удосконалення захисту в інтернет-просторі необхідно врахувати зарубіжний досвід держав, які розвиваються у цьому напрямі. Ці країни організовують свою діяльність із залученням спецслужб до створення модернізованих систем і підготовки конкурентоспроможних фахівців.

ЛІТЕРАТУРА

1. Бандурка О.М. Протидія злочинності та профілактика злочинів: монографія. Х.: ХНУВС, 2011. 308 с.

2. Про утворення територіального органу Національної поліції від 13 вересня 2015 р. № 730: постанова Кабінету Міністрів України. Офіційний вісник України. 2015. № 76. Ст. 349.

3. Про затвердження Положення про Департамент кіберполіції Національної поліції України: наказ Національної поліції України від 10 листопада 2015 № 85. Офіційний вісник України. 2015.

4. Careers for FBI Special Agents in the Cyber Division. URL: https://translate.google.com.ua/translate?hl=ru&sl=en&tl=ru&u=https%3A%2F%2Fwww.fbiagentedu.org%2Fcareers%2Ffbi-special-agent%2Fspecial-agent-cyber-crimes%2F&anno=2.

5. Катеринчук І.П. Правоохоронні органи в боротьбі з кіберзлочинністю. URL: http://oduvs.edu.ua/wpcontent/uploads/2017/01/Katerinchuk_I.P._Pravookhranitelniye_organy_v_borbe_s_kiberprestupnostyu.-5-7.pdf

6. Джужа О.М. Курс кримінології: загальна частина: підручник. К.: Юрінком Інтер, 2001. 352 с.

7. Кримінальний кодекс України від 05 квітня 2001 р. № 2341-III. Відомості Верховної Ради України. 2001. № 25–26. Ст. 131.

8. Anderson R.J. Statement Before the Senate Committee on Homeland Security and Governmental Affairs. URL: http://www.fbi.go/news/testimony/ cyber-security-terrorism-and-beyond-addressing-evolving-threats-to-the-homeland.

9. Бутузов В.М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2008. Вип. 19. С. 240.