КРИМІНАЛЬНЕ ПРАВО, КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО, КРИМІНОЛОГІЯ

Аль-Мзіраві Назар-Абдул-Карімович
студент,
Київський політехнічний інститут імені Ігоря Сікорського

КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА КІБЕРНЕТИЧНОГО ПРОСТОРУ В УКРАЇНІ

Інформаційне суспільство набирає обертів, несучи із собою не тільки позитивні, але й свої негативні явища та тенденції. Українці все більше користуються благами інформаційної цивілізації та намагаються використовувати всі можливості електронної взаємодії. Не зважаючи на суттєві блага, швидкість і зручність сучасних засобів зв'язку, використання інформаційних технологій обумовило виникнення нового виду протиправних деліктів, які отримали назву кіберзлочинів.

При цьому на сучасному етапі законодавство України у сфері боротьби з кіберзлочинністю є недосконалим. Наразі у вітчизняному кримінальному законодавстві не міститься навіть поняття «кібернетичного злочину», а є лише визначення окремих посягань, які вчиняються з використанням комп'ютерних систем та мереж електрозв'язку.

Що стосується нормативної бази з цього питання, то слід звернутися до Закону України «Про основи національної безпеки» від 19.06.2003 року, в якому, зокрема, визначено, що під комп'ютерною злочинністю та комп'ютерним тероризмом розуміється розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб і національних інтересів суспільства й держави, а також намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації.

У 2005 році Україна ратифікувала «Конвенцію про кіберзлочинність» і таким чином імплементувала положення міжнародного акту у вітчизняне законодавство. Що стосується підзаконних нормативних актів, то слід зауважити, що актуальність цієї проблеми було відзначена в Указах Президента: «Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень» від 14.07.2000 р. № 891, «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31.07.2000 р. № 928/2000, «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних» від 24.09.2001 р. № 891/2001. Проте вітчизняний сучасний стан нормативної бази щодо регулювання відносин у сфері кібернетичної злочинності в цілому

можна охарактеризувати як недосконалий через наявну безсистемність і відсутність термінологічної визначеності в базових поняттях [1].

В Україні діє низка Законів і 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».

Разом з цим діє два стратегічних документа: Стратегія національної безпеки України та Доктрина інформаційної безпеки України. 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]).

Водночас спостерігається вільне використання значної кількості термінів (та їх синонімів), що часто не узгоджені між собою. Так у Законі України «Про основи національної безпеки України» згадуються «комп'ютерна злочинність» та «комп'ютерний тероризм», при чому жоден з цих термінів не має свого визначення а ні в цьому, а ні в інших нормативних документах. У Законі України «Про боротьбу з тероризмом» поняття «комп'ютерний тероризм» не згадується взагалі, а елементи, що можуть до нього відноситись, прописані як складова частина поняття «технологічний тероризм». У «Стратегії національної безпеки України» (в редакції від 12 лютого 2007 року № 105/2007) комп'ютерні загрози не згадуються, а «кібербезпека» – лише в контексті необхідності «розробки та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність», у «Стратегії національної безпеки України» (в редакції від 6 травня 2015 року № 287/2015) вже йдеться про актуальні загрози національній безпеці України, зазначається уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак. В основних напрямках державної політики національної безпеки України прописано, що пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів є: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав – членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки,

інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки [2].

Слід зазначити, що в Україні Департамент по боротьбі з кіберзлочинністю МВС України було створено у грудні 2011 року, а відповідні територіальні підрозділи почали створюватися на початку 2012 року. Специфіка діяльності зазначеного підрозділу полягає не тільки у застосуванні норм кримінального законодавства, які є підставами для притягнення до відповідальності за кіберзлочини, а й глибоке знання технічної та технологічної сторони цих діянь, адже працівник правоохоронного органу має добре володіти інформаційними технологіями, бути обізнаним у принципах роботи мереж і пристроїв, що використовуються для вчинення правопорушень, а також обізнаним в останніх розробках у сфері ІТ-індустрії.

Найчастіше інтернет-шахраї намагаються заволодіти даними платіжних карт клієнтів, також часто за допомогою спеціальних пристроїв зчитують дані картки. Ще одним поширеним способом шахрайства є створення підробок сайтів відомих інтернет-магазинів. Також зафіксовано такий вид шахрайства, як «фішинг» – створення сайтів для збору реквізитів платіжних карток під виглядом надання послуг (наприклад, поповнення мобільних телефонів через Інтернет). У першому кварталі 2015 року було виявлено 2 «фішингових» сайти, у другому – 12, у третьому – 9, у четвертому – 15 і тільки за один місяць, січень 2016 року, було виявлено 47 таких сайтів.

Нагальною є проблема координації діяльності правоохоронних структур та правового унормування сфер відповідальності центральних органів виконавчої влади, правоохоронних органів, а також досконаліть процедур взаємодії і засобів комплексного реагування на загрози кібербезпеці держави, а також необхідність значної роботи із запобігання таким злочинам.

Законом України «Про Державну службу спеціального зв'язку та захисту інформації України» на неї покладено функцію участі у «формуванні та реалізації державної політики у сфері захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації». Обмеженість суто захистом (технічним) державних інформаційних ресурсів не відповідає сучасним тенденціям у сфері боротьби із кіберзлочинністю, а потребує, насамперед, додаткового розширення зон уваги правоохоронних органів, у тому числі щодо приватних комп'ютерних мереж та окремих користувачів. Крім того, зазначена служба не має повноважень проводити оперативно-розшукову діяльність, чим займаються профільні відділи, управління та департаменти СБУ та МВС України. Водночас діяльність цих трьох структур у сфері боротьби із кіберзлочинністю є ключовою.

Отже, проведений аналіз проблем чинного законодавства та нормативно-правових актів у сфері кібербезпеки дозволяє зробити такі висновки: незважаючи на наявність низки законодавчих та нормативно-правових документів щодо забезпечення безпеки кіберпростору держави, вони не охоплюють усього спектру сучасних загроз кібербезпеці держави.

У чинній нормативно-правовій базі відсутні визначення ключових елементів державної інфраструктури саме від кібератак. Відсутні не просто усталені визначення ключових термінів, але й такі, що можуть ефективно

застосовуватись у практиці правоохоронної діяльності. Державні органи безпекового сектору здійснюють низку заходів з метою подолання зазначених недоліків на рівні робочих груп із розробки концептуальних нормативно-правових документів у даній сфері [3].

Список використаних джерел:

1. Правове регулювання кіберзлочинності [Електронний ресурс]. – Режим доступу : http://ukrjustice.com.ua/pravove-rehulyuvannya-kiberzlochynnosti/

2. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» [Електронний ресурс] : Указ Президента України від 26.05.2015 р. № 287/2015. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/287/2015#Find

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

Войтків Ю.В.
курсант,
Національна академія внутрішніх справ

ТРИМАННЯ В ДИСЦИПЛІНАРНОМУ БАТАЛЬЙОНІ ВІЙСЬКОВОСЛУЖБОВЦІВ ЯК ВИД ПОКАРАННЯ

Тримання в дисциплінарному батальйоні військовослужбовців є одним із специфічних видів покарань, який застосовується до військовослужбовців. У вітчизняній системі покарань, сформованій за ступенем суворості, цей вид покарань займає десяту позицію (ст. 51 КК України). Більш суворими видами покарань визнаються лише позбавлення волі на певний строк та довічне позбавлення волі. Тримання у дисциплінарному батальйоні як вид покарання передбачено у санкціях 11 статей розділу XIX «Злочини проти встановленого порядку несення військової служби (військові злочини)» КК України.

Екскурс в недалеке історичне минуле засвідчує, що у наукових та військово – адміністративних джерелах мали місце висловлювання щодо доцільності виключення тримання в дисциплінарному батальйоні військовослужбовців із системи покарань. Водночас, у науковому дискурсі з цієї проблематики мали місце чіткі однозначні позиції на підтримку цього виду покарання. Зокрема, науковцями О.М. Сарнавським [1, с. 447; 2, с. 459], А.С. Овчаренком [3, с. 84] з використанням належного методологічного інструментарію наводяться наукові висновки щодо ефективності застосування тримання в дисциплінарному батальйоні військовослужбовців як виду покарання та його ролі у реалізації завдань кримінально – правової політики із запобігання та протидії військовій злочинності.

У цьому контексті варто відмітити й позицію законодавця, який розширив категорію військовослужбовців, стосовно яких може бути застосовано судом тримання в дисциплінарному батальйоні. З прийняттям Закону України « Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності військовослужбовців, надання командирам