УДК 343.346.8

Коваленко Н. В.,
кандидат юридичних наук, доцент,
доцент кафедри адміністративного та митного права
Університету митної справи та фінансів

ПРО ПРАВОВИЙ РЕЖИМ КІБЕРБЕЗПЕКИ В УКРАЇНІ

ON LEGAL REGIME OF CYBERSECURITY IN UKRAINE

В статті представлений аналіз чинного та перспективного національного законодавства (практики його застосування) в галузі кібернетичної безпеки як однієї зі складових безпеки держави. Актуальність дослідження питання правового режиму кібербезпеки підтверджена необхідністю запуску ефективної системи захисту для запобігання вчиненню правопорушень (злочинів) через віртуальний простір. Досліджені норми кримінального та адміністративного права, що у сукупності становлять правовий режим кібербезпеки в Україні.

Ключові слова: *правовий режим, кібербезпека, державний примус, інформаційний простір.*

В статье представлен анализ действующего и перспективного национального законодательства (практики его применения) в области кибернетической безопасности как одной из составляющих безопасности государства. Актуальность исследования вопроса правового режима кибербезопасности подтверждена необходимостью запуска эффективной системы защиты для предотвращения совершения правонарушений (преступлений) посредством виртуального пространства. Исследованы нормы уголовного и административного права, которые в совокупности составляют правовой режим кибербезопасности в Украине.

Ключевые слова: *правовой режим, кибербезопасность, государственное принуждение, информационное пространство.*

The article is an analysis of existing and future national legislation (its implementation) in the field of cyber security as one of the state's security components. Relevance of the research question of the legal regime of cybersecurity confirmed the need to launch an effective protection system to prevent the commission of offenses (crimes) by the virtual space. Abstract rules of criminal and administrative law, which together make up the legal regime of cybersecurity in Ukraine.

Key words: *legal regime, cybersecurity, state coercion, information space.*

Науково-технічний прогрес докорінно змінив суспільство: на сьогоднішній день інформаційні технології та технології у сфері телекомунікації відіграють чи не найважливішу роль у розвитку країн та визначенні рівня життя населення. Але разом із запровадженням нових технологій й відкриттям величезного інформаційного простору з'являються й невідомі до цього моменту проблеми, серед яких слід назвати, зокрема, кібернетичні злочини, правопорушення, що становлять загрозу не лише для окремих громадян, а й державної безпеки країн (з урахуванням сфери впливу технологій).

Актуальним це питання є не лише для України, а й для всіх інших країн, тому що не розроблено ефективної системи захисту для запобігання вчиненню правопорушень (злочинів) через віртуальний простір. В будь-якому разі легально створена й запроваджена структура захисту має бути регламентована законодавством країн, саме тому вкрай важливим є питання правового регулювання в цій сфері.

Дослідження тематики, пов'язаної з проблемами кібербезпеки, здійснює багато науковців, зокрема В.М. Богуш, В.М. Бутузов, К.Ю. Галинська, Л.П. Коваленко, Є.В. Ющук. При ознайомленні з їхніми дослідженнями можна дійти висновку, що наявний стан кібербезпеки в Україні не відповідає законодавству європейського простору. І тому для інтеграції в Європейський Союз необхідно удосконалити національне законодавство в сфері інформаційних технологій та перевести його на вищій рівень, що забезпечить безпеку держави в інформаційному просторі і буде сприяти міжнародному співробітництву у кібернетичній сфері.

Метою статті є спроба проаналізувати чинне національне законодавство в галузі кібербезпеки як однієї зі складових безпеки держави, а також віднайти недоліки та шляхи вдосконалення правової системи країни в цілому згідно з проведеним аналізом.

Віртуальний простір не має меж і кордонів, в ньому будь-хто набуває широких можливостей у сфері його використання, саме це робить кіберпростір надзвичайно зручним для здійснення протиправної діяльності. Це й злочини в різних сферах господарювання та управління, це й хакерські атаки на урядові сайти та банківські бази даних, це й спроби порушити суспільно-політичний лад у суспільстві через поширення дезінформації чи пропаганди. Для забезпечення інформаційної безпеки в Україні застосовується досить розгалужена нормативно-правова база. Її складають Конвенція Ради Європи про кіберзлочинність [1]; Закони України «Про інформацію» [7], «Про основи національної безпеки України» [8], «Про Державну службу спеціального зв'язку та захисту інформації України» [3], «Про телекомунікації» [10], «Про захист інформації в інформаційно-телекомунікаційних системах» [6], «Про доступ до публічної інформації» [4], «Про оборону України» [9], «Про засади внутрішньої і зовнішньої політики» [5]; Укази Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» від 6 травня 2015 року» [11] та «Про рішення Ради національної

безпеки і оборони України «Про нову редакцію Воєнної доктрини України» від 2 вересня 2015 року» [12]; окремі положення Кримінального Кодексу України, окремі Постанови та Рішення Кабінету Міністрів України. Тепер перейдемо до більш детального розгляду зазначених нормативно-правових актів.

Конвенція Ради Європи про кіберзлочинність передбачає міжнародне співробітництво і спільну кримінальну політику, що буде спрямована на захист суспільства від кіберзлочинності, шляхом створення відповідного законодавства та налагодженням міжнародного співробітництва між Державами, що є Сторонами Конвенції. Кожна Сторона Конвенції має вживати таких законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за вчинення злочинних протиправних діянь, що зазначені в її положеннях. До правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем відносяться незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями.

До правопорушень, пов'язаних з комп'ютерами, Конвенція відносить підробку та шахрайство. Підробка означає навмисне створення (без права на це), введення, перетворення, знищення або приховування комп'ютерних даних, що призводить до створення недійсних даних з метою того, щоб вони вважались дійсними, щоб з ними проводилися б законні дії, як з дійсними.

Шахрайством є навмисне вчинення (без права на це) дій, що призводять до втрати майна іншої особи шляхом будь-якого введення, зміни, знищення чи приховування комп'ютерних даних; будь-якого втручання у функціонування комп'ютерної системи з шахрайською або нечесною метою набуття економічних переваг для себе чи іншої особи.

Також Конвенція класифікує ряд правопорушень, що пов'язані зі змістом (стосовно дитячої порнографії) та з порушенням авторських і суміжних прав. Зазначені в Конвенції положення щодо додаткової відповідальності і санкцій за спробу, допомогу і співучасть у здійсненні кібернетичної злочинної діяльності, окремо встановлена Конвенцією корпоративна відповідальність (відповідальність юридичних осіб за злочини в цій сфері).

Якщо розглядати кримінальну відповідальність, то можна побачити, що Конвенція встановлює її для кожного з визначених у ній злочинів відповідно до внутрішнього законодавства держав-учасниць згідно з юрисдикційною належністю. Таким чином, основне завдання в забезпеченні інформаційної безпеки, протидії і заподіянні кіберзлочинів покладається на правову систему кожної з держав-учасниць окремо, і наявність в них недоліків є турботою нормотворців цих країн. Вагомою і беззаперечною перевагою ратифікації цієї Конвенції для всіх сторін-учасників є, звичайно, міжнародне співробітництво. Тут застосовуються екстрадиція, загальні принципи взаємної допомоги з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі щодо кримінального правопорушення, добровільне надання інформації [1].

Закон України «Про інформацію» передбачає обмеження права на інформацію в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Стаття 28 цього Закону зазначає, що інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини [7].

Доречно, що стосовно інформації у віртуальному просторі положення вищерозглянутої Конвенції про кібербезпечність дають змогу притягнути правопорушників до кримінальної відповідальності згідно з вітчизняним законодавством.

Закон України «Про основи Національної безпеки України» розглядає комп'ютерну злочинність та комп'ютерний тероризм як одну із загроз національним інтересам і національній безпеці України [8].

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» покладає на Державну службу спеціального зв'язку обов'язок забезпечити функціонування команди реагування на комп'ютерні надзвичайні події України – CERT-UA. До її функцій належать накопичення та аналіз даних про вчинення чи спроби вчинення протиправних дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, про їх наслідки та інформування правоохоронних органів для вжиття запобіжних заходів та припинення злочинів у кібернетичній сфері [3].

Закон України «Про телекомунікації» передбачає серед прав операторів та провайдерів телекомунікацій право відключення на підставі рішення суду кінцевого обладнання, якщо воно використовується абонентом для вчинення протиправних дій чи дій, що загрожують державній безпеці. Також оператори телекомунікацій, незалежно від форм власності, насамперед надають у користування на договірних засадах ресурси своїх мереж державній системі урядового зв'язку, національній системі конфіденційного зв'язку, органам з надзвичайних ситуацій, безпеки, оборони, Нацполіції, Національному антикорупційному бюро України, Держбюро розслідувань у порядку, встановленому ЦОВЗ. Статтею 41 для персоналу операторів і провайдерів телекомунікацій встановлюється відповідальність за порушення вимог законодавства України щодо збереження таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами

зв'язку або через комп'ютер, а також інформації з обмеженим доступом щодо організації та функціонування телекомунікаційних мереж в інтересах національної безпеки, оборони та охорони правопорядку. Цим Законом споживачам телекомунікаційних послуг гарантовано право на безпеку телекомунікаційних послуг, проте немає прав без обов'язків, тому Законом передбачено обов'язок споживачів не допускати використання кінцевого обладнання для вчинення протиправних дій або дій, що суперечать інтересам національної безпеки, оборони та охорони правопорядку [10].

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» дає визначення поняттю несанкціонованих дії щодо інформації в системі і визначає їх як дії, що провадяться з порушенням порядку доступу до інформації, установленого відповідно до законодавства. Відповідальність щодо забезпечення захисту систем покладається на власника, і він повинен повідомити про спроби чи факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом спеціально уповноваженому центральному органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованому йому регіональному органу [6].

Закон України «Про доступ до публічної інформації», так само як і Закон України «Про інформацію», встановлює обмеження щодо доступу до інформації, але ж в цьому випадку до публічної інформації. Це робиться тільки в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [4].

Закон України «Про оборону України» в сфері кібернетичної безпеки серед заходів підготовки держави до оборони в мирний час включає захист інформаційного простору України та її входження у світовий інформаційний простір, створення розвинутої інфраструктури в інформаційній сфері. Генеральний штаб Збройних Сил України, відповідно до цього Закону, бере участь не лише в організації використання і контролю за повітряним та водним просторами, а й за інформаційним простором держави. В свою чергу, Міністерства та інші органи виконавчої влади у взаємодії з Міністерством оборони України у межах своїх повноважень повинні узгоджувати з Генеральним штабом Збройних Сил України питання використання інформаційного простору держави [9].

Закон України «Про засади внутрішньої і зовнішньої політики» визначає одними з основних засад внутрішньої політики у сфері національної безпеки і оборони забезпечення життєво важливих інтересів людини і громадянина, суспільства і держави; своєчасне виявлення, запобігання і нейтралізацію реальних та потенційних загроз національним інтересам у зовнішньополітичній, оборонній, соціально-економічній, енергетичній, продовольчій, екологічній та інформаційній сферах [5].

Правове регулювання у сфері кібербезпеки також здійснюється Указами Президента України. Російська загроза, що має довгостроковий характер, та інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України обумовлюють необхідність створення нової системи забезпечення національної безпеки України, що й зумовило видачу Указу Президента «Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України від 6 травня 2015 року» від 26 травня 2015 року № 287/2015 та втрату чинності Указу Президента «Про Стратегію національної безпеки України» від 12 лютого 2007 року № 105/2007. Основні цілі та пріоритети «нової» Стратегії визначені до 2020 року. Відповідно до положень Стратегії основними 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 [11].

Указ Президента «Про рішення Ради національної безпеки і оборони України «Про нову редакцію Воєнної доктрини України» від 2 вересня 2015 року» визначає серед головних тенденцій інформаційного простору, що впливають на воєнно-політичну обстановку в регіоні довкола України такі, як модернізація та вдосконалення спеціальними службами іноземних держав систем і комплексів технічної розвідки, нарощування їх можливостей, спроби несанкціонованого доступу до об'єктів інформаційної інфраструктури України, інформаційна війна Російської Федерації проти України.

Цілеспрямований інформаційний (інформаційно-психологічний) вплив з використанням сучасних інформаційних технологій, спрямований на формування негативного міжнародного іміджу

України, а також на дестабілізацію внутрішньої соціально-політичної обстановки, загострення міжетнічних та міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин, Указ визначає як один із воєнно-політичних викликів. Серед основних завдань воєнної політики України Указом було виділено вдосконалення державної інформаційної політики у воєнній сфері. У розв'язанні завдань із забезпечення воєнної безпеки України у кібернетичному просторі зазначеним нижче державним органам надаються такі ролі:

1) *служба зовнішньої розвідки України* займається добуванням розвідувальної інформації, здійсненням спеціальних заходів впливу та протидії зовнішнім загрозам національній безпеці України у політичній, економічній, військово-технічній, науково-технічній, інформаційній та екологічній сферах; бере участь у боротьбі з тероризмом, міжнародною організованою злочинністю, незаконною торгівлею зброєю і технологіями її виготовлення;

2) *державна служба спеціального зв'язку та захисту інформації України* займається забезпеченням функціонування урядового зв'язку Верховного Головнокомандувача Збройних Сил України з посадовими особами Збройних Сил України, інших військових формувань, правоохоронних органів спеціального призначення під час їх перебування в пунктах управління, забезпечення кіберзахисту об'єктів критичної інфраструктури.

Також цим Указом передбачається поглиблення кооперації та співробітництва з НАТО і ЄС у сфері розвідки щодо протидії агресивній політиці Російської Федерації, міжнародним терористичним, релігійно-екстремістським та злочинним організаціям, залучення допомоги розвідувальних структур НАТО і ЄС, а також держав – членів НАТО і ЄС з питань реформування розвідувальних органів України, отримання доступу до інформаційних мереж, які поповнюються за рахунок розвідувальної інформації з різних джерел, у тому числі від держав – членів НАТО і ЄС [12].

Підводячи підсумки щодо змісту зазначених Указів Президента, можемо сказати, що їх основними цілями з урахуванням останніх подій в країні є забезпечення протидії протиправним агресивним діям з боку Російської Федерації, зокрема у сфері кібернетичної безпеки держави.

Кримінальна відповідальність за протиправні винні діяння у кібернетичній сфері встановлена Розділом XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України. Зокрема, встановлюється відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут; несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї; перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку [2].

Підсумовуючи викладене із нормативно-правових актів у сфері регулювання кібербезпеки України, вважаємо, що перше, що необхідно виправити, – це відсутність законодавчо закріпленої термінології в цій сфері, зокрема визначити поняття «кібератака», «кібернетична безпека», «кіберзлочин», «кіберзагроза», «кіберзахист». Також відсутні в законодавчому закріпленні й об'єкти кіберзахисту, проблемним є і питання виокремлення суб'єктів забезпечення кібербезпеки, останнє зумовлено надмірною розшарованістю законодавства й розкрито в ньому не в повній мірі. Взагалі немає визначення принципів, на основі яких має здійснюватися правове регулювання. Доцільним було б і поступове розширення класифікації правопорушень у цій сфері.

У нас є гіпотеза, що категорія «адміністративний режим» є реальним, практичним уособленням дії групи норм права на конкретно визначеному об'єкті. Під об'єктом тут розуміємо групу суспільних відносин, що врегульовані нормами адміністративного права. При висуненні такої гіпотези та перевірці вказаної теорії слід керуватись певними прийомами, правилами і способами дослідження, що вкупі і характеризуватимуть метод дослідження [14].

Стає зрозумілим, що для вирішення зазначених недоліків є вкрай необхідним прийняття спеціального закону, який би врегульовував відносини, що виникають у кібернетичному просторі. В 2013 році були невдалі спроби прийняття законопроекту у цій сфері, але вже 19 червня 2015 року був поданий до розгляду доопрацьований проект № 2126а у новій редакції «Про основні засади забезпечення кібербезпеки в Україні». В ньому надається чимала термінологічна база у сфері кібернетичної безпеки, виокремлюються об'єкти та суб'єкти правовідносин, встановлюються принципи правового регулювання і, звичайно, закріплюється стаття з відповідальністю за порушення законодавства в сфері кібербезпеки. На даний момент законопроект знаходиться на стадії опрацювання комітетом Верховної Ради України [13]. Щодо розширення класифікації, то зрозуміло, що з часом поправки з внесенням додаткової класифікації мають відбуватися у Кримінальному кодексі України.

Таким чином, можна дійти висновку, що кіберпростір на сьогоднішній день відіграє важливу роль у забезпеченні нормального функціонування держав

світу й суспільства в цілому. Тому необхідність протидії кіберзагрозам, що можуть нанести шкоду національній безпеці України, потребує створення власної дієвої системи інформаційної безпеки.

Належно розроблена та втілена в життя категорія правового режиму кіберпростору могла б усунути надмірну розшарованість правового регулювання, більш чітко та послідовно визначити суб'єктів досліджуваних правовідносин та порядок їх взаємодії, юридичні гарантії забезпечення прав людини, форми, методи діяльності контролюючих суб'єктів, заходи юридичної відповідальності.

З позитивних моментів у правовому регулюванні є міжнародне співробітництво у сфері кібернетичної безпеки, що забезпечується Конвенцією «Про кіберзлочинність», але, на жаль, поки не усунені недоліки національного законодавства, положення цієї Конвенції не зможуть допомогти працювати механізму національної системи захисту від інформаційних загроз.

ЛІТЕРАТУРА:

1. Конвенції про кіберзлочинність : Конвенція від 7 вересня 2005 року № 284-IV [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/994_575.

2. Кримінальний кодекс України // Верховна Рада України; Кодекс від 5 квітня 2001 року № 2341-III [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2341-14.

3. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23 лютого 2006 року № 3475-I [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/3475-15.

4. Про доступ до публічної інформації : Закон України від 13 січня 2011 року № 2939-VI [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/2939-17.

5. Про засади внутрішньої і зовнішньої політики : Закон України від 1 липня 2010 року № 2411-VI [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/2411-17.

6. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 року № 80/94-ВР [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

7. Про інформацію : Закон України від 2 жовтня 1992 року № 2657-XII [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/2657-12.

8. Про основи національної безпеки України : Закон України від 19 червня 2003 року № 964-IV [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/964-15.

9. Про оборону України : Закон України від 6 грудня 1991 року № 1932-XII [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/1932-12.

10. Про телекомунікації : Закон України від 18 листопада 2003 року № 1280-IV [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/1280-15.

11. Про Стратегію національної безпеки України : Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року» : від 26 травня 2015 року № 287/2015 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/287/2015.

12. Про нову редакцію Воєнної доктрини України : Указ Президента України «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року» : від 24 вересня 2015 року № 555/2015 [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/555/2015.

13. Про основні засади забезпечення кібербезпеки України : Проект Закону України від 19 червня 2015 року № 2126а [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

14. Коваленко Н.В. Методологічні підходи до визначення поняття адміністративно-правового режиму / Н.В. Коваленко // Науковий вісник Дніпропетровського державного університету внутрішніх справ. – 2014. – № 1. – С. 170–177.