УДК 351.746:007(574)

Максим Гребенюк,
канд. юрид. наук, доцент, заслужений юрист України,
керівник Міжвідомчого науково-дослідного
центру з проблем боротьби з організованою
злочинністю при Раді національної безпеки і оборони України

ДЕЯКІ ПИТАННЯ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ОГЛЯД КРАЩИХ ПРАКТИК ЗАРУБІЖНОГО ДОСВІДУ

У статті розглядається питання необхідності посилення світової кібербезпеки як складової частини інформаційної та національної безпеки кожної держави. Однією з проблем, що потребує розв'язання на глобальному рівні, є те, що натепер у жодній країні світу немає кодифікованого законодавства, яке регламентує сферу Інтернет.

На основі аналізу новел зарубіжного законодавства у сфері забезпечення кібербезпеки автором констатовано, що більшість країн світу активно опікуються цією проблематикою, постійно удосконалюючи національне законодавство та вживаючи заходів, що спрямовані на розбудову власної національної системи кібербезпеки. З урахуванням кращих практик зарубіжного досвіду, зокрема позитивного досвіду Республіки Казахстан, автором обґрунтовано необхідність правового регулювання відносин у мережі Інтернет з метою посилення інформаційної та кібербезпеки.

Ключові слова: забезпечення кібербезпеки, об'єкти критичної інфраструктури, мережа Інтернет, державне регулювання, кіберінциденти, інформаційно-комунікаційні технології.

Постановка проблеми. Сьогодні, з огляду на стрімке поширення у глобальному вимірі інформаційних та телекомунікаційних мереж, техніко-технологічного розвитку, актуальним залишається питання посилення кібербезпеки. При цьому необхідною умовою розвитку інформаційного суспільства є саме кібербезпека держави, за якою може стояти практично невичерпаний перелік проблем, починаючи від організаційно-технічних, економічних і закінчуючи правовими.

Світовий досвід підвищення ефективності боротьби з кіберзлочинністю демонструє потребу у створенні системи глобального обміну інформацією у захищеному форматі. Як свідчать результати оприлюднених досліджень та численних суспільних опитувань, питання запобігання кіберзлочинності непокоїть не тільки державу в цілому, а й кожного окремо взятого пересіченого її громадянина. У цьому сенсі вивчення досвіду боротьби з кіберзлочинами зарубіжних країн видається досить актуальним.

Аналіз останніх досліджень та публікацій. Наукова проблематика, винесена в заголовок статті, в різних аспектах вивчається багатьма вченими. Особлива увага проблемі приділяється в провідних західних країнах. Вивчення стану наукової розробленості проблем співпраці та взаємодії компетентних органів різних держав у боротьбі з кіберзлочинністю та питання забезпечення кібербезпеки вітчизняними вченими та дослідниками також не стоїть на місці. Окремі аспекти цього наукового напряму розглядалися у фундаментальних працях таких науковців, як: Д.С. Бірюкова, В.Л. Бурячка, В.М. Бутузова, В.Д. Гавловського, М.В. Гуцалюка, Д.В. Дубова, В.В. Петрова, О.В. Орлова, О.Д. Довганя, В.П. Шеломенцева та інших. Водночас отримані результати цих досліджень потребують додаткового узагальнення та висвітлення з урахуванням кращих практик новел зарубіжного законодавства про кібербезпеку, яке постійно удосконалюється, що вказує на актуальність та своєчасність проведеного авторами наукового дослідження у форматі наукової статті.

Метою статті є висвітлення концептуальних засад забезпечення кібербезпеки та боротьби з кіберзлочинністю, виходячи з аналізу сучасного законодавства Казахстану та огляду його новел.

Виклад основного матеріалу. У сучасних умовах питання забезпечення кібербезпеки не обмежуються лише організацією системи захисту інформації на окремому об'єкті критичної інформаційної інфраструктури, а й передбачають створення єдиної системи захисту кібернетичного простору як складової частини інформаційної та національної безпеки будь-якої держави світу.

При цьому, виходячи із сучасних викликів та загроз, з метою забезпечення контролю

© М. Гребенюк, 2019

за національним сегментом кіберпростору політикум будь-якої держави постійно вдосконалює організаційно-правові та технікоекономічні механізми забезпечення безпеки кіберпростору та інформаційно-телекомунікаційних мереж. Ситуація ускладнюється тим, що нині у світі здійснюються численні спецоперації у кіберпросторі, кібератаки, які супроводжуються незаконним збором інформації та особистих даних про службовців, приватний бізнес-сектор, громадян, які організовуються як спецслужбами іноземних держав, так і окремими хакерами, що фінансуються державними структурами розвинених країн та міжнародними терористичними організаціями. Одночасно застосовуються різні методи маніпуляції людьми і технологіями з використанням Інтернет-мереж.

Слушно вказує А. Марущак, що кількість злочинів у сфері інформаційних технологій постійно зростає, у зв'язку з чим серйозне занепокоєння викликає використання та розповсюдження програм-вірусів, «троянів», фішингових програм, поширення фактів несанкціонованого доступу до державних інформаційних ресурсів, викрадення інформації з баз даних, знищення та модифікація даних в інформаційних системах, перехоплення інформації тощо [1, с. 127].

Оригінальним видається досвід Уганди. Так, з 1 липня 2018 року в цій країні набув чинності закон, яким запроваджено податок на користування соціальними мережами «Facebook», «WhatsApp», «Viber», «Twitter» Користувачі зобов'язані платити 200 угандійських шилінгів на день ($ 0,05). Кошти, одержані від податку, повинні використовуватися для посилення захисту кіберпростору та розширення життєзабезпечення мереж електропостачання, щоб громадяни «могли ще частіше користуватися соціальними мережами».

Таким чином, у кожній країні існує власне національне тлумачення поняття «кібербезпека». Як наслідок, відрізняються і підходи до формування стратегій кібербезпеки. Проте керівні документи, що охоплюють питання кібербезпеки, як правило, передбачають:

– побудову державної системи управління у сфері забезпечення кібербезпеки;

– визначення відповідного механізму (в основному суспільно-державного партнерства), що дає змогу приватним і державним зацікавленим сторонам обговорювати проблеми забезпечення безпеки національних інформаційних інфраструктур;

– регламентацію стратегічних засад політики безпеки та регулюючих механізмів, чіткий розподіл завдань, прав і відповідальності для приватного і державного секторів (наприклад, обов'язкове інформування про кіберінциденти, оцінка загроз, розробка критеріїв віднесення об'єктів до критичної інформаційної інфраструктури тощо).

Нині більшість держав світу успішно проводять політику посилення кібербезпеки та її складників. У міжнародному форматі можна виділити три основні моделі правового врегулювання поширення інформації в мережі Інтернет [3].

1. Перша модель передбачає тотальний, жорсткий контроль держави над мережею Інтернет. Такої моделі дотримується, наприклад, КНР, де практично весь Інтернет перебуває під повним державним контролем. Окремі елементи китайського досвіду сьогодні впроваджуються в практичну площину в країні-агресорі РФ.

2. Друга модель передбачає відповідальність провайдера за будь-які дії користувача. Наприклад, у Франції провайдери зобов'язані надавати відомості про авторів сайтів на вимогу третіх осіб. Крім того, у Франції ще з 1978 року існує спеціальний орган (Національна комісія інформатики і свобод), який зобов'язаний контролювати, щоб інформація в мережі не порушувала права і свободи людини.

3. Третя модель регулювання безпеки в мережі Інтернет передбачає звільнення провайдера від відповідальності в тому разі, якщо він виконує певні умови, пов'язані з характером надання послуг і взаємодії із суб'єктами інформаційного обміну. Так, у Німеччині відповідальність провайдерів за розміщення нелегального контенту на Інтернет-ресурсах, що знаходяться в їх мережі, настає лише в разі, якщо вони самі є власником інформації або свідомо поширювали її з посиланням на інші джерела. Така модель також активно використовується в Японії.

За таких умов можна констатувати, що кожна країна світу вибирає власну модель розбудови національної системи кібербезпеки. Наприклад, Казахстан у цьому сенсі не є винятком.

Розглянемо досвід цієї країни у сфері організаційно-правового забезпечення кібербезпеки. Так, у своєму посланні до народу Казахстану від 31 січня 2017 року Президент Н. А. Назарбаєв доручив Комітету національної безпеки і Уряду країни створити систему «Кіберщит Казахстану». На виконання політичної волі керівництва постановою Уряду Казахстану від 30 червня 2017 року № 407 була затверджена Концепція кібербезпеки під кодовою назвою «Кіберщит Казахстану» [4]. Концепція заснована на оцінці поточної ситуації у сфері інформатизації

державних органів, автоматизації державних послуг, перспектив розвитку «цифрової» економіки і технологічної модернізації виробничих процесів у промисловості, розширення сфери надання інформаційно-комунікаційних послуг. Концепція визначає основні напрями реалізації державної політики у сфері захисту електронних інформаційних ресурсів, інформаційних систем та мереж телекомунікацій, забезпечення сталого й безпечного використання інформаційно-комунікаційних технологій.

Законодавство Казахстану декларує необхідність формування єдиного підходу до моніторингу забезпечення інформаційної безпеки державних органів, фізичних і юридичних осіб, а також вироблення механізмів попередження й оперативного реагування на кіберінциденти у тому числі в умовах надзвичайних ситуацій соціального, природного і техногенного характеру, введення надзвичайного або воєнного стану [5].

Під час розроблення Концепції врахований міжнародний досвід у галузі формування підходів до захисту національної інформаційно-комунікаційної інфраструктури як держав-лідерів у сфері розробки та використання інформаційно-комунікаційних технологій, так і країн, що прагнуть розширити сферу їх застосування для досягнення цілей соціально-економічного розвитку. При цьому в положеннях зазначеного програмного документа акцент зроблений на тому, що транснаціональна кіберзлочинність використовує ІТ-продукцію іноземного виробництва у своїх цілях з метою вчинення протиправних дій стосовно користувачів і операторів ІКТ-послуг і власників Інтернет-ресурсів, розміщених у національному сегменті, а також інформаційних систем, що взаємодіють із мережею Інтернет.

У положеннях Концепції анонсовано, що висока латентність і часто міжнародний характер кіберзлочинів підвищують їх суспільну небезпеку. Ситуація ускладнюється сформованими в суспільстві стереотипами про безкарність так званої «кіберзлочинності», неефективність вжитих державою заходів щодо зміцнення сфери безпечного використання ІКТ, обмежені можливості органів правопорядку щодо притягнення до відповідальності винних у скоєнні високотехнологічних злочинів, незважаючи на розвинені кримінально-правові інститути інформаційної безпеки. У глобальному масштабі здійснюється активна мілітаризація сфери ІКТ [5].

На цьому фоні виникають труднощі в доведенні причетності держав до використання ІКТ з порушенням принципів міжнародного права, спричинені значною мірою стихійно сформованим характером наявної міжнародної системи управління Інтернетом, а цифровий розрив, що зберігається між країнами, перешкоджає формуванню у світовому співтоваристві надійних

міжнародно-правових інструментів запобігання військовому використанню досягнень у сфері інформатизації і телекомунікацій. При цьому за своєю суттю арсенал, який використовується у військових цілях, не відрізняється від арсеналу програмно-технічних засобів, що використовуються кіберзлочинністю, про що свідчать масові випадки використання ІКТ в розвідувальних, підривних та інших цілях, що загрожують підтриманню міжнародного миру і безпеки.

Законодавством Казахстану встановлено, що кібербезпека має реагувати на такі потужні загрози, як:

– низька правова грамотність населення, працівників сфери ІКТ та керівників організацій з питань інформаційної безпеки;

– порушення державними і недержавними суб'єктами інформатизації та користувачами послуг у сфері ІКТ встановлених вимог, технічних стандартів і регламентів збору, обробки, зберігання та передачі інформації в електронній формі;

– ненавмисні помилки персоналу і технологічні збої, що чинять негативний вплив на інформаційні ресурси та системи, програмне забезпечення й інші елементи інформаційно-телекомунікаційної інфраструктури;

– діяльність міжнародних злочинних організацій, спільнот і окремих осіб щодо здійснення розкрадань у фінансово-банківській сфері, а також шкідливий вплив з метою порушення штатної роботи автоматизованих систем управління технологічними процесами промисловості, транспорту, енергетики, зв'язку та у сфері інформаційно-комунікаційних послуг;

– діяльність терористичних структур, розвідувальних і спеціальних служб іноземних держав, спрямована на підрив економічного потенціалу Республіки Казахстан шляхом здійснення розвідувального та підривного впливу на інформаційно-комунікаційну інфраструктуру.

Загалом очікується, що практичне впровадження положень Концепції дасть змогу забезпечити підтримку максимального рівня захищеності електронних інформаційних ресурсів, інформаційних систем та об'єктів інформаційно-комунікаційної інфраструктури від зовнішніх і внутрішніх загроз, сприятиме сталому розвитку країни в умовах глобальної економічної та інформаційної конкуренції.

З метою реалізації Концепції Постановою Уряду Республіки Казахстан від 28 жовтня 2017 року № 676 було затверджено План заходів щодо реалізації Концепції кібербезпеки («Кіберщит Казахстану») до 2022 року [6]. Основними цілями цей стратегічний документ визначає:

– вивчення питання про внесення змін і доповнень до законодавчих актів у частині, що стосується створення умов щодо забезпечення державних закупівель для оборони країни і безпеки вітчизняним апаратно-програмним забезпеченням, у тому числі технічних рішень у сфері кібербезпеки;

– опрацювання питання щодо створення єдиного реєстру казахстанських програмних продуктів і продукції електронної промисловості Республіки Казахстан;

– опрацювання питання щодо розробки плану поетапної відмови від закордонного пропрієтарного програмного забезпечення і сертифікації;

ІТ-продуктів стосовно інформаційної безпеки;

– гармонізація міжнародних стандартів у сфері кібербезпеки, розробка національних стандартів у галузі інформаційно-комунікаційних технологій, інформаційної безпеки та кібербезпеки;

– опрацювання питання щодо проведення навчань з метою попередження й оперативного реагування на кіберінциденти у разі настання кризових ситуацій (надзвичайних ситуацій соціального, природного і техногенного характеру);

– розробка та затвердження методики визначення типології і моделей загроз кібербезпеці [6].

З метою практичної реалізації Концепції повноваження у сфері забезпечення кібербезпеки покладені на Міністерство оборонної й аерокосмічної промисловості Казахстану. У цій країні законодавчо визначено 798 об'єктів, які потребують посиленого інформаційного захисту, 219 з яких мають стратегічне значення та внесені у перелік об'єктів критичної інфраструктури. У 2018 році у Казахстані запрацював Національний центр промислової кібербезпеки, метою діяльності якого є забезпечення кібербезпеки об'єктів, які мають стратегічне значення для країни.

На виконання постанови Уряду Казахстану від 12 грудня 2017 року з 2018 року розпочала діяти державна програма «Цифровий Казахстан», яка розрахована до 2022 року включно, практична реалізація якої передбачає у тому числі створення Національного координаційного центру з інформаційної безпеки та Академії кібербезпеки. Також слід вказати, що створення ефективної системи «Кіберщит» передбачає вирішення стратегічного завдання щодо поетапного імпортозаміщення у сфері захисту інформації та розробки власної ІТ-продукції, забезпечення інформаційно-аналітичного та науково-дослідницького супроводу й розвитку державно-приватного партнерства.

Об'єктивно у Казахстані є серйозна проблема щодо організації та проведення конкурсних закупівель засобів захисту інформації, оскільки переважно тендери виграють казахські компанії, які є локальними партнерами провідних іноземних виробників. Отже, зарубіжні корпорації через своїх представників у Казахстані заважають розвиватися власній ІТ-індустрії. Тому актуальним завданням держави залишається динамічний трансфер технологій, а саме розробка вітчизняних засобів захисту програмно-технічних продуктів. Загальновідомо, що щорічні збитки від непрофесійного використання та шкідливого впливу на комп'ютерні системи становить сотні мільярдів доларів.

Оскільки для Казахстану гострою проблемою залишається повільний розвиток вітчизняної ІТ-індустрії, то перспективним напрямом має стати сфера захисту інформації, посилення спроможностей держави в цьому форматі. Також слід акцентувати, що в Казахстані здійснюється інституціоналізація заходів протидії кіберзлочинності, зокрема: реалізовується імплементація міжнародного законодавства щодо боротьби з кіберзлочинцями, створюються міжнародні інституції з проблем кібербезпеки тощо. Так, одним із важливих заходів правового характеру стало включення в новий Кримінальний кодекс і Кодекс про адміністративні правопорушення 2014 року окремих глав, присвячених правопорушенням у сфері інформатизації та зв'язку.

Таким чином, можна констатувати активізацію зусиль політикуму Казахстану стосовно систематизації деліктного законодавства в частині протидії правопорушенням у сфері високих інформаційних технологій. Враховуючи необхідність збільшення фінансових витрат, спрямованих на забезпечення кібербезпеки, з республіканського бюджету у 2018 році держава виділила 70 млрд тенге, які спрямували на розвиток загальнодержавної системи виявлення, припинення, технічного розслідування кібернападів та інформаційних атак на державні й приватні ІТ-ресурси, об'єкти критичної інформаційної інфраструктури Казахстану.

Висновки

У більшості держав світу проблематика забезпечення кібербезпеки перебуває у фокусі

уваги політикуму та включає розробку та реалізацію організаційно-правових заходів, спрямованих на протидію та запобігання кіберзагрозам. Так, у Казахстані державна програма «Кіберщит» передбачає посилення заходів, спрямованих на забезпечення кібербезпеки та інформаційної безпеки державних електронних ресурсів. При цьому концепція цієї програми передбачає тільки державний захист інформаційних систем, а безпосереднім захистом приватних ІТ-ресурсів повинен займатися виключно кожен власник. Очікується, що у повному форматі система інформаційної безпеки «Кіберщит» запрацює у 2019 році, що дасть змогу значно мінімізувати наслідки кіберзагроз та максимально убезпечити об'єкти критичної інформаційної інфраструктури від нападів та інцидентів, здійснювати постійний моніторинг кіберпростору з превентивною метою, захищати державні органи від аварійного та позаштатного витоку даних.

Таким чином, можна констатувати, що в Казахстані швидкими темпами здійснюється формування складників національної системи кібербезпеки. Концепція «Кіберщит» перший стратегічний документ у Казахстані, який ретельно описує проблематику кібербезпеки та визначає заходи, практичне впровадження яких дасть можливість посилити безпеку в національному сегменті кіберпростору, гарантовано захистити державні інформаційні ресурси, забезпечити функціонування дієвого механізму адекватного реагування на загрози та виклики в сучасному цифровому світі.

Список використаних джерел:

1. Марущак А.І. Інформаційно-правові аспекти протидії кіберзлочинності. *Інформація і право*. 2018. №1 (24). С. 127-132.

2. Войціховський А. В. Міжнародне співробітництво у боротьбі з кіберзлочинністю. *Портал: Національна бібліотека імені В. І. Вернадського*. URL: http ://www.archive.nbuv.gov.ua/portal/.../PB-4_26.pdf.

2. Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур : Резолюция A/RES/64/211 ГА ООН от 21.12.2009 / Офіційний сайт ООН. URL: http://daccessddsny.un.org/doc/UNDOC/GEN/N09/474/51/PDF/N0947451.pdf?OpenElement.

3. Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза. *Криминология: вчера, сегодня, завтра*. 2012. № 24. С. 45-55.

4. Послание Президента Республики Казахстан Н. Назарбаева народу Казахстана от 31 января 2017 года / Официальный сайт Президента Республики Казахстан. URL: http://www.akorda.kz/ru/addresses/addresses_of_president/poslanieprezidenta-respubliki-kazahstan-nnazarbaeva-narodu-kazahstana-31-yanvarya-2017.

5. Концепция кибербезопасности («Кіберщит Казахстана»): утверждена постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407.

6. План мероприятий по реализации Концепции кибербезопасности («Кіберщит Казахстана») до 2022 года : утвержден Постановлением Правительства Республики Казахстан от 28 октября 2017 года № 676.

В статье рассматривается вопрос о необходимости усиления мировой кибербезопасности как составной части информационной и национальной безопасности любого государства. Одной из проблем, которая требует решения на глобальном уровне, является то, что сегодня ни в одной стране мира нет кодифицированного законодательства, регламентирующего сферу Интернет.

На основании анализа новелл зарубежного законодательства в сфере обеспечения кибербезопасности автором констатировано, что большинство стран мира активно занимаются этой проблематикой, постоянно совершенствуя национальное законодательство и принимая меры, направленные на развитие собственной национальной системы кибербезопасности. С учетом лучших практик зарубежного опыта, в частности положительного опыта Республики Казахстан, автором обоснована необходимость правового регулирования отношений в сети Интернет с целью усиления информационной и кибербезопасности.

Ключевые слова: обеспечение кибербезопасности, объекты критической инфраструктуры, сеть Интернет, государственное регулирование, киберинциденты, информационно-коммуникационные технологии.

The article discusses the need to strengthen the global cyber security as an integral part of the information and national security of any state. One of the problems that needs to be addressed globally is that there is no codified legislation regulating the Internet in any country in the world.

Based on the analysis of the novels of foreign legislation in the field of cyber security, the author stated that most countries of the world are actively engaged in this issue, constantly improving their national legislation and taking measures aimed at developing their own national cyber security system. Taking into account the best practices of foreign experience, in particular, the positive experience of the Republic of Kazakhstan, the author substantiates the need for legal regulation of relations in the Internet with the aim of enhancing information and cyber security.

Key words: ensuring cyber security, critical infrastructure objects, Internet network, state regulation, cyber incidents, information and communication technologies.