УДК 343.98

Ю.Ю. Нізовцев, *консультант-експерт Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України*

ЩОДО НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ ПРОТИДІЇ НЕСАНКЦІОНОВАНИМ ВТРУЧАННЯМ У РОБОТУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Розглянуто нормативно-правові акти з протидії несанкціонованим втручанням у роботу інформаційно-телекомунікаційних систем, проаналізовано та висвітлено прогалини в нормативно-правовому регулюванні цієї сфери, проведено огляд нормативно закріпленого понятійного апарату, що використовується під час проведення судових комп'ютерно-технічних і телекомунікаційних експертиз.

Ключові слова: нормативно-правове регулювання, закон, інформаційно-телекомунікаційна система, кібертероризм, кіберзагроза, телекомунікаційна експертиза, комп'ютерно-технічна експертиза.

Рассмотрены нормативно-правовые акты по противодействию несанкционированным вмешательствам в работу информационно-телекоммуникационных систем, проанализированы и освещены пробелы в нормативно-правовом регулировании данной сферы, проведен обзор нормативно закрепленного понятийного аппарата, используемого при проведении судебных компьютерно-технических и телекоммуникационных экспертиз.

Considers regulations to counteract unauthorized intervention in the information and telecommunication systems, analyzed and highlighted gaps in the legal regulation of this sphere, a review of the regulatory fixed conceptual apparatus used during the court computer-engineering and telecommunications expertise.

Будь-яке важливе для функціонування держави явище потребує ефективного регулювання. Насамперед це стосується тих явищ, через які можуть виникати загрози національній безпеці держави. Зазвичай протидія таким загрозам потребує злагодженої роботи багатьох державних інститутів. Ефективність цієї роботи значною мірою залежить від якості її нормативної регламентації. Одним з видів таких загроз є кібератаки, значна кількість яких проти України упродовж останнього часу свідчить про наявність прогалин у сфері протидії несанкціонованим втручанням у роботу інформаційно-телекомунікаційних систем [1].

Метою цієї статті є аналіз нормативної бази протидії несанкціонованим втручанням у роботу інформаційно-телекомунікаційних систем і висвітлення виявлених недоліків.

Нормативно-правовою основою функціонування інформаційно-телекомунікаційних систем, технічного захисту оброблюваної в них інформації та кримінальної відповідальності за несанкціоноване втручання в їх роботу є Конституція України, закони України, акти Президента України, Кабінету Міністрів України, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, а також міжнародні договори України, згоду на обов'язковість яких надала Верховна Рада України. Саме цією нормативно-правовою базою керуються правоохоронні органи України під час протидії несанкціонованим втручанням у роботу інформаційно-телекомунікаційних систем. Для судових експертів важливу роль відіграє закріплений у зазначених нормативно-правових актах понятійний апарат, який використовують під час проведення комп'ютерно-технічних і телекомунікаційних експертних досліджень ознак несанкціонованих втручань у роботу інформаційно-телекомунікаційних систем.

Згідно з частиною першою ст. 17 Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу [2].

Відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації регулює Закон України «Про інформацію» [3].

Закон України «Про авторське право і суміжні права», у свою чергу, охороняє особисті немайнові права і майнові права авторів та їх правонаступників, пов'язані зі створенням та використанням творів науки, літератури і мистецтва (авторське право), а також права виконавців, виробників фонограм і відеограм та організацій мовлення (суміжні права) [4]. Цей Закон, зокрема, визначає, що комп'ютерна програма — це набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах).

Закон України «Про телекомунікації», встановлюючи правову основу діяльності у сфері телекомунікацій, визначає повноваження держави щодо управління та регулювання цієї діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у цій діяльності або користуються телекомунікаційними послугами [5].

Загальні засади формування, виконання та коригування Національної програми інформатизації визначено у Законі України «Про Національну програму інформатизації» [6].

Закон України «Про електронний цифровий підпис» визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають під час його використання [7].

Основні організаційно-правові засади електронного документообігу та використання електронних документів встановлює Закон України «Про електронні документи та електронний документообіг» [8].

Відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах регулює Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [9].

Закон України «Про основи національної безпеки України» визнає комп'ютерну

злочинність і комп'ютерний тероризм однією із загроз національним інтересам і національній безпеці України [10].

Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку караються згідно з Кримінальним кодексом України (далі — КК України), а саме [11]:

– несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку — згідно зі ст. 361;

– створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут — згідно зі ст. 361^1 КК України;

– 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, — згідно зі ст. 361^2 КК України;

– 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, — згідно зі ст. 362 КК України;

– порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, — згідно зі ст. 363 КК України;

– перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку — згідно зі ст. 363^1 КК України.

Одним із основоположних міжнародних документів щодо узгодження боротьби з комп'ютерними злочинами є Конвенція про кіберзлочинність, ратифікована Україною 07.09.2005 р. [12].

З метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави навесні 2016 року Указом Президента України затверджено Стратегію кібербезпеки України [13]. А для подолання комплексу проблем у сфері забезпечення кібербезпеки, враховуючи її кризовий стан, що загрожує національній безпеці, Указом Президента України від 13 лютого 2017 року було введено в дію рішення Ради національної безпеки і оборони України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» [14].

Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах визначено загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів та інформації, яку закон визначає як таку, що має бути захищеною, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [15]. При цьому правові та організаційні засади технічного захисту важливої для держави, суспільства і особи інформації, охорона якої забезпечується державою відповідно до законодавства, визначено у Положенні про технічний захист інформації в Укра-

їні [16]. Механізм формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури України, у свою чергу, визначено у Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави [17].

Терміни та визначення понять у сфері технічного захисту інформації, які є обов'язковими для використання в усіх організаційних і нормативних документах, у тому числі зі стандартизації, а також рекомендованими для використання у довідковій та навчально-методичній літературі щодо технічного захисту інформації, встановлено у ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення» (чинний від 01.01.98 р.) [18].

Нормативний документ системи технічного захисту інформації (далі — НД ТЗІ) 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» визначає методологічні основи (концепцію) вирішення завдань щодо захисту інформації в комп'ютерних системах і створення нормативних та методологічних документів, що регламентують питання визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу, створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу, оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача [19].

НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» встановлює терміни і визначення понять у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Ці терміни є обов'язковими для застосування в усіх видах документації і літератури з питань технічного захисту інформації [20].

Зазначені документи не лише визначають основні терміни, які застосовують у сфері використання інформаційно-телекомунікаційних систем, а й регулюють відносини та встановлюють відповідальність за злочини у цій сфері.

Проте, незважаючи на доволі велику кількість нормативно-правових актів у сфері, про яку йдеться, не всі питання ними врегульовано.

Так, згідно зі ст. 361 та 361^1 КК України шкідливі програмні засоби — це програмні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що може призвести до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації.

Водночас низка інших нормативних документів містить визначення окремих різновидів програмного забезпечення, яке за багатьма ознаками може вважатися шкідливим, без зазначення співвідношення цих визначень із визначенням загального поняття «шкідливий програмний засіб», наведеним у КК України. Так, у ДСТУ 3396.2-97 визначено поняття комп'ютерного вірусу та програмної закладки, а в НД ТЗІ 1.1-003-99, крім зазначених, ще й поняття люка та троянського коня.

Згідно з ДСТУ 3396.2-97 комп'ютерний вірус — це програма, яка розмножується та поширюється самочинно і може порушувати цілісність інформації, програмне забезпечення та (чи) режим роботи обчислювальної техніки, а програмна закладка — це потай впроваджена програма, яка створює загрозу для інформації, яку містить комп'ютер.

Відповідно до НД ТЗІ 1.1-003-99:

– комп'ютерний вірус — це програма, яка має здатність до самовідтворення і, як правило, здатна здійснювати дії, які можуть порушити функціонування комп'ютерної системи і/або зумовити порушення політики безпеки;

– програмна закладка — це потайно впроваджена програма або недокументовані властивості програмного забезпечення, використання яких може призвести до обходу комплексу засобів захисту (далі — КЗЗ) і/або порушення політики безпеки;

– люк — залишені розробником недокументовані функції, використання яких дозволяє обминути механізми захисту;

– троянський кінь — програма, яка, будучи авторизованим процесом, окрім виконання документованих функцій, здатна здійснювати приховані дії від особи авторизованого користувача в інтересах розробника цієї програми.

Аналізуючи зазначені визначення, нескладно дійти висновку, що без їх упорядкування до єдиної системи проблематично розраховувати на однозначне об'єктивне їх тлумачення усіма працівниками, задіяними у цій сфері, зокрема і судовими експертами, які мають справу у своїй роботі з ознаками наведених різновидів шкідливих програм під час проведення експертизи потенційно шкідливого програмного забезпечення.

Також існує неузгодженість понять «виток» і «витік». Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» містить поняття «виток інформації». Відповідно до цього Закону виток інформації — це результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї. Водночас ДСТУ 3396.2-97 визначає поняття «витік інформації» як неконтрольоване поширення інформації, що призводить до її несанкціонованого одержання. Виходячи із семантики, ці поняття є тотожними. Проте у деяких випадках щодо них можуть виникнути певні непорозуміння. Отже, ці поняття також потребують узгодження.

В українському законодавстві немає чіткого визначення таких понять, як «кібертероризм» і «кібердиверсія». Як зазначалося вище, у КК України передбачено кримінально-правову відповідальність за низку злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку.

З огляду на суспільну небезпеку, зумовлену втручанням у роботу інформаційних систем критичної інфраструктури держави, багато науковців, серед яких В.А. Мазуров, С.О. Гнатюк, В.М. Бутузов, В.А Голубєв та інші, вважають за потрібне законодавчо закріпити кримінальну відповідальність за новий різновид особливо небезпечних злочинів — кібертероризм. Натомість у ст. 258 КК України вже визначено відповідальність за «класичний» тероризм, а отже, думка щодо виокремлення нового складу злочину є дискусійною.

Доцільно навести кілька аргументів на користь виокремлення цього складу злочину. Способи вчинення тероризму та кібертероризму різні. Відповідно, різними є і знаряддя вчинення цих злочинів та процес їх підготовки. Це зумовлює різні тактики їх розслідування, різні види експертиз, які потрібно призначати, залучення правоохоронців різних служб (слідчих, оперативних співробітників, спеціалістів, експертів) тощо. Отже, думка щодо виокремлення кібертероризму в окремий склад злочину є достатньо обґрунтованою та має право на реалізацію.

Слід також зазначити, що у червні 2015 року Парламентська Асамблея Ради Європи ухвалила Резолюцію № 2070 (2015) «Зміцнення співпраці у протидії кібертероризму та іншим масштабним атакам в Інтернеті» [21], п. 3 якої містить заклик до країн-членів Ради Європи запровадити визначення кібертероризму та передбачити відповідальність за нього. Відповідно до цієї Резолюції було підготовлено два законопроекти щодо внесення змін до КК України [22].

У проекті Закону України «Про внесення змін до Кримінального кодексу України (щодо посилення відповідальності за кібертероризм та кіберзлочини)» (законопроект від 10.07.2015 р. № 2328а) передбачено частину другу ст. 258 КК України викласти у новій редакції [23]:

«2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони пов'язані з несанкціонованим втручанням в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку об'єкта підвищеної небезпеки, або якщо вони призвели до заподіяння значної майнової шкоди чи інших тяжких наслідків, —

караються позбавленням волі на строк від семи до дванадцяти років з конфіскацією майна або без такої».

Статтю 361 КК України запропоновано доповнити новими частинами третьою і четвертою такого змісту:

«3. Дії, передбачені частинами першою або другою цієї статті, якщо вони пов'язані з несанкціонованим втручанням в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку об'єкта підвищеної небезпеки та призвели до заподіяння значної майнової шкоди чи інших тяжких наслідків, —

караються позбавленням волі на строк від семи до дванадцяти років з конфіскацією майна або без такої.

4. Дії, передбачені частинами першою, другою або третьою цієї статті, що призвели до загибелі людини, —

караються позбавленням волі на строк від десяти до п'ятнадцяти років або довічним позбавленням волі з конфіскацією майна або без такої».

Проектом Закону України «Про внесення змін до Кримінального кодексу України (щодо встановлення відповідальності за кібертероризм)» (законопроект від 24.07.2015 р. № 2439а) запропоновано ввести до КК України нову статтю 258^6 [24]:

Стаття 258^6. Кібертероризм

1. Кібертероризм, тобто умисна атака на інформацію, яка обробляється комп'ютером, комп'ютерну систему чи комп'ютерні мережі, що створює небезпеку для життя і здоров'я людей або призводить до інших тяжких наслідків, якщо такі дії були скоєні з політичних мотивів, з метою порушення суспільної безпеки, залякування населення, провокації військового конфлікту, — караються позбавленням волі на строк від п'яти до десяти років з конфіскацією майна або без такої.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, — караються позбавленням волі на строк від семи до дванадцяти років з конфіскацією майна або без такої.

3. Вчинення акту кібертероризму, який призвів до травмування, каліцтва або загибелі людей, — карається позбавленням волі на строк від десяти до п'ятнадцяти років, або довічним позбавленням волі, з конфіскацією майна або без такої.

4. Особа, або група осіб, які брали участь у підготовці акту кібертероризму, але які добровільно попередили правоохоронний орган про підготовку такого акту до його здійснення, якщо їхні дії призвели до запобігання акту тероризму, звільняються від кримінальної відповідальності, якщо в їхніх діях немає складу іншого злочину».

Проте зміни до КК України дотепер не прийнято.

Думка авторів законопроектів про ухвалення змін до КК України щодо встановлення кримінальної відповідальності за кібертероризм є доволі слушною, адже внесення цих змін дасть змогу на законодавчому рівні забезпечити захист інформаційних (автоматизованих), інформаційно-телекомунікаційних систем, електронних реєстрів і баз даних державної форми власності, об'єктів критичної національної інформаційної інфраструктури.

Проте слід зазначити, що обидва законопроекти не позбавлені певних недоліків. Зокрема, вбачається, що у разі прийняття законопроекту № 2328а може виникнути конкуренція кримінально-правових норм частини другої ст. 258 і частини третьої ст. 361 КК України. Те саме стосується і ст. 258^6 запропонованого законопроекту № 2439а та ст. 361 КК України.

З огляду на зазначене найоптимальнішим є введення третьої та четвертої частин до ст. 361 КК України (як це і передбачено законопроектом № 2328а), а поняття «кібертероризм» разом з поняттям «кібердиверсія» закріпити в окремому нормативному акті, наприклад, у Стратегії кібербезпеки України.

Прийняття законопроекту (що передбачає внесення відповідних змін як до КК України, так і до Стратегії кібербезпеки України) дасть змогу не лише законодавчо визначити поняття кібертероризму, а й встановити кримінальну відповідальність за вчинення актів кібертероризму, що, у свою чергу, посилить заходи боротьби з кіберзлочинами, спрямованими на підрив національної безпеки, залякування населення, створення небезпеки для життя і здоров'я громадян тощо. Натомість зволікання у цьому питанні може зменшити ефективність роботи правоохоронних органів, призвести до неналежної кваліфікації вчинених діянь, що може створити небезпеку руйнування інформаційної інфраструктури критично важливих об'єктів України, призвести до катастроф, людських жертв та інших тяжких і особливо тяжких наслідків.

Підсумовуючи, слід зазначити, що українська нормативно-правова база містить доволі багато документів, які певним чином регламентують питання протидії несанкціонованим втручанням у роботу інформаційно-телекомунікаційних систем країни. Однак таке розмаїття нормативно-правових актів породжує низку проблем, пов'язаних насамперед з неузгодженістю окремих положень цих актів. Крім того, у багатьох документах фахівцям складно орієнтуватися. Усе це ускладнює проведення судово-експертних досліджень шкідливих програмних засобів, а також ознак несанкціонованих втручань у роботу інформаційно-телекомунікаційних систем, які вони спричиняють. Проте найбільшою проблемою, на думку автора, є невідповідність певних положень українського законодавства сучасним реаліям і рекомендаціям світової спільноти, насамперед стосовно зазначених вище змін до чинного законодавства в частині криміналізації кібертероризму, що є особливо актуальним в умовах зростання кількості кібератак, спрямованих на об'єкти критичної інфраструктури України [25].

Список використаної літератури

1. *Ткачук А.* Украина в последнее время является основным объектом кибератак со стороны России [Электронный ресурс] / А. Ткачук. — Режим доступа : http://censor.net.ua/video_news/428105/ukraina_v_posledneee_vremya_yavlyaetsya_osnovnym_obektom_kiberatak_so_storony_rossii_tkachuk_video.

2. *Конституція* України : станом на 15 берез. 2016 р. [Електронний ресурс] / Верховна Рада України. — Офіц. вид. — Режим доступу : http://zakon0.rada.gov.ua/laws/show/254к/96-вр.

3. *Закон* України «Про інформацію» : станом на 6 груд. 2016 р. [Електронний ресурс] / Верховна Рада України. — Офіц. вид. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/2657-12.

4. *Закон* України «Про авторське право і суміжні права» : станом на 5 жовт. 2016 р. [Електронний ресурс] / Верховна Рада України. — Офіц. вид. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/3792-12.

5. *Закон* України «Про телекомунікації» : станом на 6 жовт. 2016 р. [Електронний ресурс] / Верховна Рада України. — Офіц. вид. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/1280-15.

6. *Закон* України «Про Національну програму інформатизації» : станом на 25 груд. 2015 р. [Електронний ресурс] / Верховна Рада України. — Офіц. вид. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/74/98-вр.

7. *Закон* України «Про електронний цифровий підпис» : станом на 6 жовт. 2016 р. [Електронний ресурс] / Верховна Рада України. — Офіц. вид. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/852-15.

8. *Закон* України «Про електронні документи та електронний документообіг» : станом на 3 верес. 2015 р. [Електронний ресурс] / Верховна Рада України. — Офіц. вид. — Режим доступу : http://zakon0.rada.gov.ua/laws/show/851-15.

9. *Закон* України «Про захист інформації в інформаційно-телекомунікаційних системах» : станом на 27 берез. 2014 р. [Електронний ресурс] / Верховна Рада України. — Офіц. вид. — Режим доступу : http://zakon2.rada.gov.ua/laws/show/80/94-вр.

10. *Закон* України «Про основи національної безпеки України» : станом на 16 липня 2015 р. [Електронний ресурс] / Верховна Рада України. — Офіц. вид. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/964-15.

11. *Кримінальний* кодекс України : станом на 21 груд. 2016 р. [Електронний ресурс] / Верховна Рада України. — Офіц. вид. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/2341-14.

12. *Конвенція* про кіберзлочинність від 23.11.2001 р. [Електронний ресурс]. — Режим доступу : http://zakon5.rada.gov.ua/laws/show/994_575.

13. *Указ* Президента України від 15.03.2016 р. № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]. — Режим доступу : http://zakon3.rada.gov.ua/laws/show/96/2016.

14. *Указ* Президента України від 13.02.2017 р. № 32/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» [Електронний ресурс]. — Режим доступу : http://www.president.gov.ua/documents/322017-21282.

15. *Постанова* Кабінету Міністрів України від 29.03.2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [Електронний ресурс]. — Режим доступу : http://zakon2.rada.gov.ua/laws/show/373-2006-п.

16. *Указ* Президента України від 27.09.99 р. № 1229/99 «Про Положення про технічний захист інформації в Україні» [Електронний ресурс]. — Режим доступу : http://zakon2.rada.gov.ua/laws/show/1229/99.

17. *Постанова* Кабінету Міністрів України від 23 серпня 2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критич-

ної інфраструктури держави» [Електронний ресурс]. — Режим доступу : http://zakon0.rada.gov.ua/laws/show/563-2016-п.

18. *Захист* інформації. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2-97. [Електронний ресурс]. — [Чинний від 1998-01-01]. — Режим доступу : http://tzi.com.ua/478.html.

19. *Нормативний* документ системи технічного захисту інформації (НД ТЗІ) 1.1-003-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.99 р. № 22 [Електронний ресурс]. — Режим доступу: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106340.

20. *Нормативний* документ системи технічного захисту інформації (НД ТЗІ) 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.99 р. № 22 [Електронний ресурс]. — Режим доступу : http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102106&cat_id=46556&ctime=1344502446343.

21. *Resolution* 2070 (2015) «Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet» [Електронний ресурс]. — Режим доступу : http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21975&lang=en.

22. *У Раді* пропонують встановити кримінальну відповідальність за кібертероризм [Електронний ресурс] / Інформаційне агентство УНІАН — Режим доступу : http://www.unian.ua/politics/1106141-u-radi-proponuyut-vstanoviti-kriminalnu-vidpovidalnist-za-kiberterorizm.html.

23. *Проект* Закону про внесення змін до Кримінального кодексу України (щодо посилення відповідальності за кібертероризм та кіберзлочини) [Електронний ресурс]. — Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=55972.

24. *Проект* Закону про внесення змін до Кримінального кодексу України (щодо встановлення відповідальності за кібертероризм) [Електронний ресурс]. — Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=56183.

25. *СБУ:* Россия пытается разрушить финансовую инфраструктуру Украины новым классом APT вирусов. ВИДЕО [Электронный ресурс] // Информационное сопротивление. — Режим доступа : http://sprotyv.info/ru/news/kiev/sbu-rossiya-pytaetsya-razrushit-finansovuyu-infrastrukturu-ukrainy-novym-klassom-apt.