УДК 343.26

АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРЗАХИСТУ В УКРАЇНІ

Риженко Олег Сергійович,
аспірант кафедри адміністративного, господарського права та фінансово-економічної безпеки ННІ права,
Сумський державний університет

Науковий керівник:
Гаруст Юрій Віталійович,
д-р юрид. наук, доцент кафедри кримінально-правових дисциплін та судочинства ННІ права,
Сумський державний університет

У статті наведений аналіз норм чинного законодавства та проектів національного законодавства, а також його практичне застосування в галузі кіберзахисту, яке являється однією із частин безпеки держави в інформаційному просторі. Дослідження вказаного питання має актуальний характер через необхідність створення дієвого механізму з метою запобігання вчиненню правопорушень в інформаційному просторі. Питання захисту інформації має важливу роль у розвитку держав. З розвитком нових технологій розвиваються нові способи вчинення злочинів в кіберпросторі. Вказані правопорушення становлять загрозу не тільки окремим громадянам але і державній безпеці в цілому. У світі не розроблені надійні системи запобіганню вчинення правопорушень в інформаційному просторі. Будь-яка система захисту, яку втілено в життя в легальний спосіб потребує законодавчого врегулювання, саме тому вказане питання є досить важливим не тільки для України, а і для всього світу.

Кіберзахист має свою специфіку, оскільки інформаційний простір не має жодних меж та кордонів, що робить його надзвичайно зручним для вчинення протиправних дій. До протиправної діяльності в інформаційному просторі відносяться злочини в різних сферах господарювання, атаки хакерів на сайти державних органів та місцевого самоврядування, бази даних фінансових установ, а також спроби порушити суспільно-політичний лад у державі різними способами. Вказані злочини вчиняються не обов'язково в межах країни, суб'єкти більшості злочинів у сфері інформаційного простору знаходяться за межами країни.

Проведено аналіз норм конституційного, адміністративного та кримінального права, які у своїй сукупності становлять досить розгалужену та недосконалу систему кіберзахисту України.

Ключові слова : кіберзахист, інформаційний простір, кіберзлочин, кіберзагроза, кіберпростір, захист інформації.

Ryzhenko O. S. Administrative and Legal Regulation of Cyber Defense in Ukraine. The article gives an analysis of the norms of the current legislation and draft national legislation, as well as its practical application in the field of cyber defense, which is one of the parts of state security in the information space. The study of this issue is actual because of the need to create an effective mechanism to prevent the commission of offenses in the information space. The issue of information security plays an important role in the development of States. With the development of new technologies, new ways of committing crimes in cyberspace are developing. The indicated offenses pose a threat not only to individual citizens, but also to state security in general. The world has not developed reliable systems to prevent the commission of offenses in the information space. Any

system of protection that is implemented in a legal way requires a legislative settlement, which is why the mentioned issue is very important not only for Ukraine but also for the whole world.

Cybersecurity has its own specifics, since the information space has no borders and borders, which makes it extremely convenient for committing unlawful actions. Unlawful activities in the information space include crimes in various areas of business, attacks by hackers on the sites of state bodies and local self-government, databases of financial institutions, as well as attempts to disturb the social and political system in the state in various ways. The specified crimes do not necessarily occur within the country, the subjects of most crimes in the area of information space are outside the country.

The analysis of the norms of constitutional, administrative and criminal law, which in their totality constitute a rather ramified and imperfect system of cyber defense of Ukraine, was conducted.

Keywords : cyber defense, information space, cybercrime, cyber threats, cyberspace, information protection.

На сьогоднішній день питання захисту інформації відіграє чи не найважливішу роль у розвитку держав, а також визначенні рівня життя їх населення. Разом з розвитком нових технологій та інформаційного простору розвиваються та з'являються нові способи та методи вчинення злочинів в кіберпросторі. Вказані правопорушення ставлять загрозу не тільки окремим громадянам але і державній безпеці в цілому.

В світлі останніх подій актуальним це питання є не лише для України, але і для всіх інших країн, навіть для досить економічно-розвинених. Як показали останні події (втручання у виборчий процес президента США на початку 2017 року через електронну мережу та хакерські атаки інформаційних систем по всьому світі у цьому ж році), що на даний час у світі не розроблені надійні системи запобіганню вчинення правопорушень різного характеру в інформаційному просторі. Будь-яка система захисту, яку створено і втілено в життя в легальний спосіб потребує законодавчого врегулювання в країнах, саме тому вказане питання є досить важливим не тільки для України, а і для всього світу.

Дослідження питань пов'язаних з проблемами кіберзахисту, здійснює багато вчених, наприклад Бутузов В.М., Галинська К.Ю., Богуш В.М., Коваленко Л.П., Ющук Є.В. та інші. Виходячи з досліджень вказаних науковців та власного вивчення нормативно-правової бази нашої країни можна з впевненістю сказати, що стан кіберзахисту в Україні не тільки не відповідає законодавству європейського простору, його практично не існує, а ті норми, які хоча і опосередковано врегульовують вказану сферу на практиці не діють.

З метою належного забезпечення кіберзахисту нашої країни, а також інтеграції до Європейського Союзу потребує вдосконалення законодавство в сфері захисту інформації, а також його ефективне впровадження в життя, що у свою чергу забезпечить належний рівень безпеки держави в інформаційному просторі і забезпечить належний рівень міжнародного співробітництва в різних сферах з застосуванням кібернетичного простору.

Кіберзахист має свою специфіку, оскільки інформаційний простір не має практично жодних меж та кордонів, що робить його надзвичайно зручним не тільки для здійснення законних операцій у різних сферах суспільного життя осіб та державного управління але і для вчинення протиправної діяльності. До протиправної діяльності в інформаційному просторі відносяться злочини в різних сферах господарювання, атаки хакерів сайти державних органів та місцевого самоврядування, бази даних фінансових установ, а також спроби порушити суспільно-політичний лад у державі різними способами. При чому вказані злочини вчиняються не обов'язково в межах країни, суб'єкти більшості злочинів у сфері інформаційного простору знаходяться за межами країни.

На сьогодні в Україні існуюча нормативно-правова система кіберзахисту має розгалужений характер, що робить інформаційний простір зручним для

вчинення злочинів.

Нормативно-правову базу захисту інформації в Україні можна розділити на міжнародні договори, згода на обов'язковість яких надана Верховною Радою України та національне законодавство України. У свою чергу національне законодавство можна розподілити за вертикаллю на такі групи: конституція України, окремі положення Кримінального кодексу України, Закони України, постанови та рішення Кабінету Міністрів України, Укази Президента України.

Провівши класифікацію законодавства в сфері захисту інформації по вертикалі, можна перейти до більш детального розгляду вищезазначених нормативно-правових актів, але не досить детального, якщо їх досить детально та прискіпливо розглядати, врахувавши всі переваги, недоліки та прогалини в регулюванні суспільних відносин, можна захистити не одну дисертацію.

Відповідно до Закону України «Про міжнародні договори України» міжнародний договір України – укладений у письмовій формі з іноземною державою або іншим суб'єктом міжнародного права, який регулюється міжнародним правом, незалежно від того, міститься договір в одному чи декількох пов'язаних між собою документах, і незалежно від його конкретного найменування (договір, угода, конвенція, пакт, протокол тощо) [4].

Прикладом законодавства у сфері кіберзахисту міжнародного характеру є Конвенція Ради Європи про кібезлочинність, яка передбачає міжнародне співробітництво і спільну політику в сфері кримінальної відповідальності, що спрямовується на захист суспільства від кіберзлочинів, шляхом створення відповідного законодавства та налагодження належного співробітництва між державами – Сторонами Конвенції. Кожна сторона Конвенції має вживати таких законодавчих та інших заходів, які можуть бути необхідним для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за вчинення злочинних протиправних діянь, що зазначені в її положеннях. До правопорушень проти конфіденційності, цілісності та доступності комп’ютерних даних і систем відносяться незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями.

Конвенцією передбачено, що правопорушення пов’язані з комп’ютерами є підробка та шахрайство. Підробка означає навмисне створення, введення, перетворення, знищення або приховування комп’ютерних даних, що призводить до створення недійсних даних з метою того, щоб вони вважались дійсними або відповідно них проводилися законні дії, як з дійсними.

Шахрайство – це дії, що призводять до втрати майна іншої особи шляхом будь-якого введення, зміни, знищення чи приховування комп'ютерних даних, або втручання у функціонування комп'ютерної системи з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи.

Конвенцією передбачено класифікацію ряду правопорушень, що пов’язані зі змістом та з порушенням авторських прав і суміжних прав. Передбачені Конвенцією і положення щодо додаткової відповідальності і санкцій за спробу, допомогу і співучасть у здійсненні кібернетичної злочинної діяльності. Також, Конвенція окремо передбачає корпоративну відповідальність – відповідальність юридичних осіб у цій сфері.

Проаналізувавши норми Конвенції, можна дійти висновку, що основне завдання в забезпеченні інформаційної безпеки, протидії і заподіянні кіберзлочинів покладається на правову систему кожної з держав-учасниць окремо. Наявність недоліків в законодавстві є внутрішніми проблемами та турботою законотворців країн-учасниць Конвенції. Досить значною перевагою ратифікації Конвенції є міжнародне співробітництво між країнами-учасницями, видами якого є екстрадиція, загальні принципи взаємної допомоги з метою розслідування кримінальних правопорушень [2].

Перед тим як перейти до розгляду національного законодавства у сфері захисту інформації, слід зазначити, що за роки незалежності України питання кібернетичної та інформаційної безпеки розвивалося за

залишковим принципом. Нормативно-правові документи з регулювання цієї сфери розроблялися безсистемно, нерідко базувались на застарілих радянських нормах та вступали у протиріччя один з одним. Це призвело у свою чергу до гнітючого становища в системі кібернетичної безпеки та інформаційно-комунікаційних технологій взагалі. Україна кожен рік потрапляла в анти-рейтингові списки щодо піратства, розповсюдження шкідливого програмного забезпечення, DDoS та інше. Так, відповідно до дослідження корпорації Майкрософт, на 68% комп'ютерів в Україні встановлене неліцензійне програмне забезпечення. В той же час в центральних огрганах державної влади України використовують 60% неліцензійного програмного забезпечення. Як відомо «безкоштовний сир – лише в мишоловці», а відтак використання неліцензійного програмного забезпечення – це прямий шлях для надання доступу хакерам до ресурсів систем, на яких воно встановлено [16].

Конституція України передбачає, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо [1].

Незважаючи на те, що норми Конституції є нормами прямої дії які підлягають беззаперечному виконанню, інформаційна безпека у в Україні на даний час перебуває не на досить високому рівні.

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. Статтею 28 вказаного Закону передбачено, 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 [9].

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 [10].

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 функції належать накопичення та аналіз даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також про їх наслідки, інформування правоохоронних органів для вжиття заходів із запобігання та припинення злочинів у зазначеній сфері [5].

Закон України «Про телекомунікації» передбачає право операторів та провайдерів телекомунікацій відключення на підставі рішення суду кінцевого обладнання, якщо воно використовується абонентом для вчинення протиправних дій або дій, що загрожують інтересам державної безпеки. Оператори телекомунікацій, незалежно від форм власності, в першу чергу 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, Національної поліції, Національному антикорупційному бюро України, Державному бюро розслідувань у порядку, встановленому ЦОВЗ. Статтею 41 вказаного

Закону передбачено, що персонал оператора, провайдера телекомунікацій несе 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 [12].

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» визначає поняття несанкціонованих дій щодо інформації в системі – це 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 [8].

Закон України «Про доступ до публічної інформації» встановлює обмеження щодо доступу до публічної інформації. Вказане 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 [6].

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 [11].

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 [7].

Укази Президента України також здійснюють правове регулювання у сфері кіберзахисту.

Указ 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 основними цілями та пріоритетами «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 [13].

Указ Президента «Про рішення Ради національної безпеки і оборони України «Про нову редакцію Воєнної доктрини України» від 2 вересня 2015 року» визначив 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.

Указ визначає як один із воєнно-політичних викликів цілеспрямований інформаційний 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. Серед основних завдань воєнної політики України. Указом виділено вдосконалення державної інформаційної політики у воєнній сфері. У розв'язанні завдань із забезпечення воєнної безпеки України у кіберне-тичному просторі зазначеним нижче державним органам надаються такі ролі: 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; 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 [15].

Укази Президента України у сфері кіберзахисту покликані забезпечувати протидію протиправним агресивним діям з боку інших держав у сфері кібернетичної безпеки держави.

Кримінальним кодексом України передбачена відповідальність за протиправні винні діяння у кібернетичній сфері, а саме Розділом XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Так встановлюється відповідальність за несанкціоноване втручання в роботу електронно-обчисліовальних 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 [3].

Дослідивши викладені нормативно-правові акти можна дійти висновків, що в національному законодавстві України відсутні такі ключові поняття як, «кібератака», «кібернетична безпека», «кіберзлочин», «кіберзагроза», «кіберзахист» та ін.

Для вирішення вказаних прогалин є гостра необхідність в прийнятті спеціального закону, який би врегульовував відносини, що виникають у кібернетичному просторі. У Верховній Раді України 19 червня 2015 року 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 [17].

З усього вищевикладеного можна зробити висновок, що кібер-простір на сьогоднішній день відіграє важливу роль у забезпеченні нормального функціонування країн їх економічних систем та господарської діяльності. Тому є велика необхідність у створенні дієвої системи інформаційної безпеки, яка включатиме в себе досконалу нормативно-правову систему, відповідні відокремлені органи, які здійснюватимуть функції кіберзахисту, належне матеріально-технічне оснащення вказаних органів та міжнародне врегулвання і співробітництво в сфері кіберзахисту з метою захисту національних систем від інформаційних загроз.

Використана література :

1. Конституція України від 28.06.1996 [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/254.

2. Конвенція про кіберзлочинність від 07.09.2005 [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_575/page.

3. Кримінальний кодекс України від 05.04.2001 № 2341-III [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/2341-14.

4. Закон України «Про міжнародні договори України» від 26.06.2004 № 1906-IV [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/1906-15.

5. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 № 3475-IV [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/3475-15.

6. Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov.ua/laws/show/2939-17.

7. Закон України «Про засади внутрішньої і зовнішньої політики» від 01.07.2010 № 2411-VI [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/2411-17.

8. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР [Електронний ресурс]. Режим доступу : http://zakon3.rada.gov.ua/laws/show/80/94.

9. Закон України «Про інформацію» від 02.10.1992 № 2657-XII [Електронний ресурс]. Режим доступу:http://zakon3.rada.gov.ua/laws/show/2657-12.

10. Закон України «Про основи національної безпеки України» від 19.06.2003 № 964-IV [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/964-15.

11.Закон України «Про оборону України» від 06.12.1991 № 1932-XII [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov.ua/laws/show/1932-12.

12. Закон України «Про телекомунікації» від 18.11.2003 № 1280-IV [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/1280-15.

13.Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» від 26.05.2015 № 287/2015 [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/287/2015.

14.Проект Закону Країни «Про основні засади забезпечення кібербезпеки України» від 19.06.2015 № 2126а [Електронний ресурс]. Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

15.Указ Президента України «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року»: від 24.09.2015№ 555/2015 [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/549/2015.

16. Кібербезпека в Україні: 2016 та прогнози на майбутнє. ПашкоП.М. актуальні задачі та досягнення у галузі кібербезпеки. Матеріали Всеукраїнської науково-практичної конференції 23-25 листопада 2016, м. Кропивницький. [Електронний ресурс]. Режим доступу: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/5045/1/AUConferenceCyberSecurity_November2016_p21.pdf.

17. Правовий режим кібербезпеки в Україні. Коваленко Н.В. Актуальні проблеми вітчизняної юриспруденції № 3/2016 [Електронний ресурс]. Режим доступу: http://apnl.dnu.in.ua/3_2016/24.pdf.