Інформаційна і національна безпека

УДК 342.9

КОСТЕНКО О.В., головний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ТА РОЗВИТОК КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ НА СУЧАСНОМУ ЕТАПІ

Анотація. *У статті проаналізовано проблеми законодавчого регулювання сфери кібернетичної безпеки України на досвіді сучасних кібернетичних загроз та кібератак, що здійснювалися на державні інформаційні ресурси протягом останніх років. Досліджено критичні галузі, в яких інформаційні системи виявилися найбільш вразливими для кібернетичниж атак. Висвітлено проблему понятійно-категоріального апарату основних нормативно-правових актів сфери кібернетичної безпеки, цифрового підпису та відсутність кореляції кібернетичних злочинів із юридичною відповідальністю суб'єктів за порушення у сфері кібернетичної безпеки. Запропоновано рекомендації щодо вжиття відповідних заходів в сфері забезпечення кібернетичної безпеки України.*

Ключові слова: *кібернетична безпека, кібернетичний злочин, електронний підпис, електронні довірчі послуги.*

Summary. *The article analyzes the problems of legislative regulation of the sphere of cyber security in Ukraine based on the experience of modern cyber threats and cyber attacks that have been carried out on state information resources in recent years. Critical areas in which information systems were the most vulnerablehave to cyber-attacks have been investigated. The problem of conceptual and categorical apparatus of the basic regulatory legal acts of the sphere of cyber security is covered, as well as digital signature and lack of correlation of cybercrime with the legal liability of subjects for cyber-security offenses. Recommendations on taking appropriate measures in the field of cyber security of Ukraine at the present stage are offered.*

Keywords: *cyber security, cybercrime, electronic signature, electronic trust services.*

Аннотация. *В статье проанализированы проблемы законодательного регулирования сферы кибернетической безопасности Украины на опыте современных кибернетических угроз и кибератак, которые осуществлялись на государственные информационные ресурсы на протяжении последних лет. Исследованы критические области, в которых информационные системы оказались наиболее уязвимы к кибернетическим атакам. Освещена проблема понятийно-категориального аппарата основных нормативно-правовых актов сферы кибернетической безопасности, цифровой подписи и отсутствие корреляции кибернетических преступлений с юридической ответственностью субъектов за нарушения в сфере кибернетической безопасности. Предложены рекомендации относительно употребления соответствующих мер в сфере обеспечения кибернетической безопасности Украины.*

Ключевые слова: *кибернетическая безопасность, кибернетическое преступление, электронное подпись, электронные доверительные услуги.*

Постановка проблеми. На сьогодні впровадження інформаційно-комунікаційних технологій у всі сфери діяльності є пріоритетним напрямом інноваційного розвитку всіх країн світу та сучасного інформаційного суспільства. В той же час, інформаційні технології стають зброєю іноземних спецслужб, злочинних угруповань та окремих

кримінальних елементів. Втручання в інформаційні системи, кібератаки на інформаційні ресурси, реєстри, бази даних, електронні системи управління державними органами та підприємствами критичної інфраструктури стали невід'ємною частиною сучасного суспільства. Боротьба із кібернетичними злочинами вийшла на рівень загальнонаціональних та загальносвітових проблем. Україна останні роки потерпає від численних кібернетичних атак, хоч і вживає відповідні заходи у сфері забезпечення кібернетичної безпеки. Вочевидь, на сучасному етапі доцільно переглянути систему кібернетичної безпеки з метою її удосконалення у відповідності із новітніми ризиками та загрозами.

Результати аналізу досліджень і наукових публікацій. У наукових працях вітчизняних та зарубіжних технічних фахівців та правознавців проблеми правового регулювання у сфері кібернетичної безпеки висвітлено достатньо широко, що відображено в працях Е. Авер'янової, Д. Азарова, Ю. Белського, В. Болгова, С. Бородіна, В. Бутузова, В. Вєхова, Н. Гадіона, О. Гладуна, О. Користіна, Л. Краснова, М. Карчевського, О. Копатіна, М. Литвинова, Ю. Ляпунова, С. Максимова, А. Музики, А. Новікова, П. Смагіна, Є. Скулишина, М. Погорецького.

Однак недостатньо дослідженими лишаються питання, пов'язані з проблемами кореляції кібернетичних злочинів із юридичною відповідальністю суб'єктів за порушення у сфері кібернетичної безпеки, аналізу та протидії кібернетичним загрозам на сучасному етапі.

Метою статті є визначення потенційних напрямів сучасних кібернетичних загроз для інформаційних ресурсів та розробка рекомендації щодо вжиття відповідних заходів в сфері забезпечення кібернетичної безпеки України.

Виклад основного матеріалу дослідження. Законом України "Про основні засади забезпечення кібербезпеки України" [1] визначено правові та організаційні основи захисту життєво важливих інтересів людини і громадянина, суспільства і держави та національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, а також засади координації їхньої діяльності із забезпечення кібербезпеки.

Підпунктом 2 пункту 3 статті 8 Закону визначено, що функціонування національної системи кібербезпеки забезпечується шляхом створення нормативно-правової і термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу і НАТО.

Нормативно-правова база у сфері забезпечення кібербезпеки перебуває на етапі становлення і, зокрема, включає: закони України "Про основні засади забезпечення кібербезпеки України", "Про Державну службу спеціального зв'язку та захисту інформації України", "Про телекомунікації"; Указ Президента України "Про рішення Ради національної безпеки і оборони України від 27.01.16 р. "Про Стратегію кібербезпеки України" від 15.03.16 р. № 96/2016; постанову КМ України від 11.04.12 р. № 295, якою затверджено "Правила надання та отримання телекомунікаційних послуг"; постанову КМ України від 12.04.02 р. № 522, якою затверджено "Порядок підключення до глобальних мереж передачі даних"; постанову КМ України від 29.03.06 р. № 373, якою затверджено "Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах"; постанову КМ України від 16.11.02 р. № 1772, якою затверджено "Порядок взаємодії органів виконавчої влади з питань захисту

державних інформаційних ресурсів в інформаційних та телекомунікаційних системах"; постанову КМ України від 23.08.16 р. № 563, якою затверджено "Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави"; наказ Адміністрації Держспецзв'язку від 10.06.08 р. № 94, яким затверджено "Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах"; наказ Адміністрації Держспецзв'язку від 02.12.14 р. № 660, яким затверджено "Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах"; наказ Адміністрації Держспецзв'язку від 15.01.16 р. № 20, яким затверджено "Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті" та інші.

Згідно щорічного плану Державною службою спеціального зв'язку та захисту інформації України здійснюються заходи з оцінки стану захищеності інформаційних систем в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності. Заходи полягають в детальному аналізі мереж і систем з точки зору можливого втручання потенційних зловмисників та правопорушень.

Однак, кількість інцидентів в інформаційно-телекомунікаційних системах протягом останніх років не зменшується. Зокрема, в умовах воєнного конфлікту з РФ здійснювалися численні атаки на цифрові ресурси України. Наприклад, серед відомих випадків слід виокремити найбільш гучні кібератаки: 2014 р. – атаковано інформаційно-телекомунікаційну систему Центральної виборчої комісії; 2015 р. – атаковано енергетичні компанії України; 2016 р. – атаковано "Укренерго", а також урядові сайти та внутрішні мережі Міністерства фінансів України, Держказначейства України та Пенсійного фонду України; 2017 р. – кібератака комп'ютерним вірусом "Petya" [2]. Протягом 2014 – 2019 рр. в ході гібридної війни РФ проти України згідно з відомостями ЗМІ було виявлено і нейтралізовано понад 10 тисяч кібератак проти України [3].

Також слід зауважити, що згідно з проектом Середньострокового плану пріоритетних дій Уряду до 2020 року до ключових проблем у сфері створення Національної телекомунікаційної мережі та забезпечення кібербезпеки було віднесено:

– необхідність забезпечити надійне функціонування існуючих систем, мереж і комплексів спеціального зв'язку з одночасним проведенням заходів з поетапного (фрагментарного) переоснащення систем, мереж і комплексів спеціального зв'язку;

– відсутність можливості інтеграції розподілених ресурсів спеціальних інформаційно-телекомунікаційних систем;

– відсутність єдиних підходів до розвитку захищених електронних комунікацій у державних органах, у тому числі в державних органах сектору безпеки та оборони, та до модернізації інформаційної інфраструктури державних органів;

– неможливість гарантовано задовольнити потреби державних органів у послугах захищених електронних комунікацій у мирний час, в особливий період та в умовах воєнного стану та впровадити єдині підходи до розвитку захищених електронних комунікацій у державних органах, у тому числі в державних органах сектору безпеки та оборони;

– неможливість підвищити ефективність оперативно-технічного управління системами (мережами) та забезпечити належний рівень захисту інформації (кіберзахисту)

в електронних комунікаційних мережах у державних органах, у тому числі в державних органах сектору безпеки та оборони;

– відставання технологічного рівня розвитку систем (мереж) і комплексів спеціального зв'язку від сучасного рівня розвитку у сфері електронних комунікацій;

– відсутність транспортної платформи для подальшої розбудови захищеного інформаційного суспільства в Україні;

– недостатній рівень забезпечення безпеки інформаційного обміну, що здійснюється в інтересах управління державою, та захисту об'єктів критичної інформаційної інфраструктури (ІТС) та її інформаційних ресурсів в умовах посилення загроз у кіберпросторі.

Зазначені проблеми, за оцінками фахівців, були пов'язані зі щорічним недофінансування заходів, передбачених відповідними державними цільовими програмами розвитку у сферах спеціального зв'язку, захисту інформації та електронних комунікацій. При цьому, не вирішення цих проблем продовжить сталу тенденцію відставання технологічного рівня розвитку систем (мереж) і комплексів спеціального зв'язку від сучасного рівня розвитку у сфері електронних комунікацій та кіберзахисту, що призведе до погіршення стану інформаційної безпеки держави та негативно вплине на ефективність управління державою.

В сучасних умовах, як видається, до найбільш важливих ***напрямів кіберзахисту*** слід віднести: *об'єкти критичної інфраструктури; суб'єкти фінансової системи (НБУ, Мінфін, Держказначейство); інформаційні ресурси, реєстри, системи і бази даних.*

Нині в Україні налічується понад 350 публічних електронних реєстрів, які перебувають у власності більш ніж 80 державних установ (Міністерств, служб, агентств тощо). При цьому, значні обсяги персональних даних громадян дублюються і накопичуються у численних базах даних, які далеко не завжди контролюються чи перебувають у власності держави [4]. Загалом, національна система захисту персональних даних у зв'язку зі стрімким розвитком інформаційних технологій та введенням в дію (травень 2018 р.) "Пакету захисту даних ЄС" [5] потребує кардинального перегляду.

Заходи щодо розвитку інформаційних систем у сфері Міністерства фінансів України і Держказначейства заплановані та виконуються відповідно до розпоряджень КМ України від 08.02.17 р. № 142-р "Про схвалення Стратегії реформування системи управління державними фінансами на 2017 – 2020 роки" [6] та від 24.05.17 р. № 415-р "Про затвердження плану заходів з реалізації Стратегії реформування системи управління державними фінансами на 2017 – 2020 роки" [7], згідно з якими створено інтегровану інформаційно-аналітичну систему для обміну інформацією та консолідації фінансової звітності з використанням баз даних та інформаційних систем фінансових відомств.

Водночас, залишається актуальним питання розвитку національної інформаційної системи управління державними фінансами, а також казначейською системою управління державним та місцевими бюджетами із централізованим ядром та резервним дата-центром. Події, пов'язані з гібридною війною засвідчили, що централізована система з одним ядром може ефективно відключати окуповані території від фінансових ресурсів України, натомість діюча децентралізована система управління державними та місцевими бюджетами дозволяє автономно працювати регіональним сегментам.

Такий же недолік притаманний інформаційним ресурсам, управління та регулювання, що здійснюється Міністерством юстиції України. Найбільш складний стан справ з цифровізацією спостерігався у сфері нотаріату. Це було обумовлено суттєвими вадами системи електронного нотаріату, що не дозволяло здійснювати належний державний контроль над важливими для громадян і суспільства функціями нотаріату [8].

Як відомо, нині існують цифрові підписи, які мають безліч різновидів. Суспільні відносини у цій сфері регулюються Законом України “Про електронні довірчі послуги”. Також законодавством знято обмеження, яке стосувалося заборони використання державними органами електронних підписів від різних центрів акредитації. Це скасувало монополію, але водночас призвело до виробничої неузгодженості в питаннях використання електронних підписів. Зокрема, це стало актуальним на етапі запуску відомчих систем електронного документообігу та їх адаптації й підключення до загальнодержавної інформаційної шини “Трембіта” [9]. Слід зауважити, що “Трембіта” – це українська назва системи “X-Road” естонської розробки, яка забезпечує обмін даними між електронними державними реєстрами різних держорганів у режимі реального часу. До “Трембіти” підключено 17 органів державної влади, серед яких Міністерство юстиції України, Міністерство соціальної політики України, Міністерство закордонних справ України, Рахункова палата України, Державна міграційна служба України, Пенсійний фонд та інші.

Також існує масштабна проблема цифровізації, яку нині відносять до другорядних – проблема ідентифікації особи державного службовця і визначення кола його електронних повноважень. Проблема пов’язана з тим, що в державних органах у системах управління електронним документообігом відсутній цифровий підпис загальнодержавного зразка, який має містити інформацію про державного службовця або службовця органу місцевого самоврядування: реквізити держслужбовця, посаду, повноваження і термін його дії та інші необхідні дані для організації роботи з електронними документами в міжвідомчому обміні цими документами.

Питання про надання державним службовцям цифрових підписів відповідно до займаної посади, як видається, доцільно віднести до повноважень не окремих держорганів, а до функцій Національного агентства України з питань державної служби, відповідні повноваження якого внести до Закону “Про електронні довірчі послуги”. Надання посадовій особі органу державного управління надійного засобу електронної ідентифікації – державного кваліфікованого цифрового підпису із зафіксованими в сертифікаті відповідними повноваженнями, правами та обов’язками, стане основою державного електронного документообігу, а також забезпечить персоніфікований електронний обмін інформацією між громадянами та державою відповідно до законів України “Про звернення громадян”, “Про інформацію”, “Про доступ до публічної інформації” [10]. Використання стандартизованих кваліфікованих цифрових підписів органами державного управління також забезпечить електронний документообіг між відповідними органами країн-членів ЄС та Україною.

Зазначені проблеми є досить важливими для громадян, суспільства і держави та забезпечення їх кібербезпеки. Однак, відсутність врегульованої законодавством юридичної відповідальності за скоєння кіберзлочинів та кіберправопорушень, у т.ч. за несанкціоноване використання чи викрадення електронних підписів, електронних печаток тощо, перешкоджає ефективному вирішенню вказаних питань.

Як свідчить аналіз досліджень, законодавством України визначено поняття “кіберзлочин”, “кіберзлочинність”, “кібертероризм”. Водночас, ці визначення не завжди узгоджуються з кримінальним і адміністративним законодавством в частині кримінальної та адміністративної відповідальності за скоєння злочинів і правопорушень у кіберпросторі або з його використанням.

Наразі Кримінальний кодекс України оперує терміном “злочини у сфері використання електронно-обчислюваних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку”, використання якого передбачено нормами міжнародного

права у т.ч. Конвенцією про кіберзлочинність. Тривалий час використання цього терміну вважалось обґрунтованим через загальність поняття та можливість уніфікованої класифікації значної кількості злочинів у комп'ютерному середовищі. Однак, з розвитком інформаційних технологій, інформаційних ресурсів, продуктів і послуг, запровадження нових термінів у цій сфері та поширення кіберзлочинності, вказаний підхід, як видається, потребує перегляду.

Поряд з цим, за оцінками фахівців, рівень латентності злочинів цього виду може складати переважну більшість від офіційних даних, що пов'язано з такими основними причинами:

– складнощі технічного й оперативного характеру, що не дозволяють своєчасно і достовірно встановлювати осіб, причетних до скоєння кіберзлочинів та технологій, які вони застосовують для скоєння правопорушень у цій сфері;

– значна кількість потерпілих не повідомляє про скоєння кіберзлочинів стосовно них або їх інформаційних ресурсів;

– наслідки кіберзлочинів далеко не завжди виявляються в момент їх скоєння, а значно пізніше та без належної оцінки спричиненої шкоди.

Зазначене можна наочно засвідчити на прикладі потенційних викликів і загроз для реалізації перспективного, за нашими оцінками, проекту "Країна в сматфоні".

Зокрема, за цим проектом, як видається, має бути здійснена масштабна цифровізація, у т.ч. цифрова ідентифікація громадян з наданням кожному громадянину унікального електронного ID, кваліфікованого електронного підпису на SIM-карті мобільного пристрою, доступу до цифрових ресурсів, систем електронної освіти та електронного здоров'я. Шлюзом для зв'язку держави і громадянина може бути мобільний додаток в смартфоні, викрадення якого за чинним законодавством класифікується як звичайна крадіжка за (ст. 185 КК України).

Водночас, внаслідок викрадення смартфону із вказаним мобільним додатком громадянину може бути спричинена суттєва матеріальна, моральна та інша шкода, у т.ч. злочинці фактично незаконно заволодівають конфіденційними персональними даними та електронним ідентифікатором громадянина або його цифровим підписом, які ототожнюють його фізичну і віртуальну особистість в кіберпросторі, можуть здійснювати незаконні електронні операції із фінансами та майном, брати участь у виборах (при запровадженні системи електронного голосування) тощо.

Нині кіберзлочини в Україні класифікуються за напрямами, пов'язаними з:

– несанкціонованим втручанням в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації (ст. 361 КК України);

– несанкціонованими діями з інформацією, яка обробляється 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 (ст. 362 КК України).

Країни з різними правовими системами по різному формують підходи щодо класифікації кіберзлочинів. Водночас, у державах-членах ЄС поширеною є класифікація цих злочинів за такими групами:

– комп'ютерні злочини (порушення авторських прав на програмне забезпечення, розкрадання даних, порушення роботи обчислювальних систем, розкрадання комп'ютерного часу тощо);

– злочини, “пов’язані з комп’ютерами” (переважно фінансове шахрайство);

– мережева злочинність (використання мереж для скоєння незаконних дій, у т.ч. поширення порнографії, торгівлі наркотиками, ухилення від митних зборів, відмивання коштів тощо).

Слід звернути увагу на ***класифікатор комп’ютерних злочинів*** розроблений фахівцями Інтерполу:

– несанкціонований доступ і перехоплення, комп’ютерний абордаж (несанкціонований доступ), перехоплення за допомогою спеціальних технічних засобів, крадіжка часу (ухилення від плати за користування), інші види несанкціонованого доступу та перехоплення;

– логічна бомба, троянський кінь, комп’ютерний вірус, комп’ютерний черв’як та інші види зміни даних;

– комп’ютерне шахрайство, шахрайство з банкоматами, комп’ютерна підробка, шахрайство з ігровими автоматами, маніпуляції з програмами введення-виведення, шахрайства з платіжними засобами, телефонне шахрайство та інші комп’ютерні шахрайства;

– незаконне копіювання, комп’ютерний саботаж з апаратним забезпеченням (порушення роботи ЕОМ) або з програмним забезпеченням (знищення, блокування інформації), розкрадання інформації, що становить комерційну таємницю, передача інформації, що підлягає судовому розгляду [11].

Різні юридичні школи пропонують класифікацію кіберзлочинів за способами втручання у процес передачі даних, за наслідками, спричиненими їх здійсненням, способами скоєння злочину тощо [12; 13].

В Україні також були спроби розширення відповідальності за злочини такого виду, зокрема, Кабінетом Міністрів України було підготовлено законопроект № 8304 від 19.04.18 р. “Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо розмежування підслідності злочинів, вчинених у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, державних інформаційних ресурсів і об’єктів критичної інформаційної інфраструктури”. Однак цей законопроект не стосувався питань класифікації кіберзлочинів.

Тобто, нині актуальним постає питання щодо опрацювання та публічного обговорення проблеми внесення змін і доповнень до кримінального і адміністративного законодавства, зокрема, розширення Розділу XVI “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку” Кримінального кодексу України.

Також актуальним залишається питання подальшого опрацювання питань правового регулювання і практики забезпечення кібернетичної безпеки в іноземних державах, насамперед США та країнах-членах ЄС, у т.ч. щодо юридичної відповідальності за злочини і правопорушення у кіберпросторі, в контексті розвитку національного законодавства.

З урахуванням викладених та інших проблем, до пріоритетних заходів щодо розвитку національної системи кібернетичної безпеки України видається за доцільне виднести наступне:

- створення Національного центру оперативно-технічного управління мережами телекомунікацій України відповідно до Закону України “Про телекомунікації”;
- внесення змін і доповнень до Закону України “Про основні засади забезпечення кібербезпеки України” в частині приведення його окремих положень до норм

Конституції України та рішень Конституційного Суду України щодо створення, функцій та повноважень Національного координаційного центру кібербезпеки як робочого органу Ради національної безпеки і оборони України, проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки, здійснення парламентського контролю за дотриманням законодавства щодо захисту персональних даних та доступу до публічної інформації у сфері кібербезпеки тощо;

- розроблення та внесення на розгляд до Верховної ради України проекту Закону "Про засади забезпечення інформаційної безпеки України" (відповідно до ч. 1 ст. 17 Конституції України), "Про внесення змін до Закону України "Про захист персональних даних" (щодо удосконалення системи захисту персональних даних та імплементації положень "Пакету захисту даних ЄС");
- розроблення та внесення на розгляд до Верховної Ради України проекту Закону України "Про електронний нотаріат", "Про внесення змін до Закону України "Про електронні довірчі послуги" (щодо підвищення рівня відповідальності за порушення прав та обов'язків користувачів електронних довірчих послуг);
- підготувати пропозиції щодо створення єдиної державної системи кваліфікованих електронних довірчих послуг державних службовців та подання їх на розгляд до Кабінету Міністрів України;
- розроблення та внесення на розгляд до Верховної Ради України проекту Закону України про внесення змін до Кримінального кодексу України та Кримінально процесуального кодексу України в яких передбачити види кіберзлочинів та правопорушень та види покарань за їх скоєння.

Висновки.

Вжиття запропонованих заходів поліпшить не тільки технічну складову системи кібернетичної безпеки України, але й модернізує правове регулювання суспільних відносин у даній сфері відповідно до вимог та реалій сьогодення, що в свою чергу сприятиме прискоренню розбудови національної спроможності кібернетичної безпеки.

Використана література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 12.08.2019).

2. Найгучніші хакерські атаки, як сколихнули всю Україну: вражаючі деталі. URL: https://24tv.ua/nayguchnishi_hakerski_ataki_yaki_skolihnuli_vsyu_ukrayinu_vrazhayuchi_detali_n1079849 (дата звернення 12.08.2019).

3. У ході кібервійни Росії проти України за останні три роки було здійснено понад 7 тисяч атак. URL: https://www.unian.ua/science/1915168-u-hodi-kiberviyni-rosiji-proti-ukrajini-za-ostanni-tri-roki-bulo-zdiysneno-ponad-7-tisyach-atak-ekspert.html (дата звернення 14.08.2019).

4. Державні секретарі прискорюватимуть впровадження "Трембітки". – (Державне агентство з питань електронного урядування України). URL: https://www.e.gov.ua/ua/news/derzhavni-sekretari-priskoryuvatimut-vprovadzhennya-trembiti (дата звернення 12.08.2019).

5. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: зб. документів / неоф. пер. з англ. І. Майстренко; за ред. В. Брижко; передмова В. Пилипчука. – (НДІ інформатики і права Національної академії правових наук України). Київ: ТОВ "Видавничий дім "АртЕк", 2018. 180 с.

Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / В.Г. Пилипчук, В.М. Брижко та ін.; за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ "Видавничий дім "АртЕк", 2017. 226 с.

6. Про схвалення Стратегії реформування системи управління державними фінансами на 2017 – 2020 роки: Розпорядження КМ України від 08.02.17 р. № 142-р. URL: https://zakon.rada.gov.ua/laws/show/142-2017-%D1%80 (дата звернення 12.08.2019).

7. Про затвердження плану заходів з реалізації Стратегії реформування системи управління державними фінансами на 2017 – 2020 роки: Розпорядження КМ України від 24.05.17 р. № 415-р. URL: https://zakon.rada.gov.ua/laws/show/415-2017-%D1%80 (дата звернення 12.08.2019).

8. Костенко О.В., Костенко В.В. Шляхи запровадження електронних довірчих послуг в нотаріальному процесі. *Південноукраїнський правничий часопис*. 2018. № 4. С. 118-122. URL: https://www.sulj.oduvs.od.ua/archive/2018/4/part_1/31.pdf (дата звернення 14.08.2019).

9. Взаємодія реєстрів. Інтероперабельність "Трембіта". – (Державне агентство з питань електронного урядування України). URL: https://www.e.gov.ua/ua/projects/vzayemodiya-reyest riv-interoperabelnist/trembita?v=5be989456869a (дата звернення 12.08.2019).

10. Костенко О.В. Сучасна правова модель суспільних відносин сфери електронних довірчих послуг в Україні. *International Journal of Innovative Technologies in Social Science.* 2(14), February 2019. С. 3-7. URL: http://archive.ws-conference.com/wp-content/uploads/ijitss01 71.pdf (дата звернення 14.08.2019).

11. Столяр О. Міжнародно-правові проблеми визначення та класифікації «кіберзлочинів». *Теория и практика*. 2017. С. 190-193. URL: https://www.jurnaluljuridic.in.ua/ archive/2017/4/43.pdf (дата звернення 14.08.2019).

12. Бельський Ю. Щодо визначення поняття кіберзлочину. *Юридичний вісник*. 2014. № 6. С. 414-418.

13. Костенко О.В., Костенко В.В. Електронні підписи та порядок визнання іноземних сертифікатів електронних підписів в законодавстві окремих країни Азії. *Науковий вісник публічного та приватного права*. 2019. № 1. С. 100-106.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~