УДК 346:338.49-021.131(477)
DOI https://doi.org/10.32782/2524-0374/2020-3/49

ПРОПОЗИЦІЇ ЩОДО ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ У ЄДИНІЙ СУДОВІЙ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ

PROPOSALS FOR LEGAL SUPPORT OF INFORMATION PROTECTION IN THE UNIFIED JUDICIAL INFORMATIONAL AND TELECOMMUNICATION SYSTEM

Георгієвський Ю.В., д.ю.н.,
завідувач наукового відділу правового забезпечення
галузевого інноваційного розвитку
Науково-дослідний інститут правового забезпечення інноваційного розвитку
Національної академії правових наук України,
доцент кафедри адміністративного права
Національний юридичний університет імені Ярослава Мудрого

Стаття присвячена розробці пропозицій щодо удосконалення правового забезпечення захисту інформації у Єдиній судовій інформаційно-телекомунікаційній системі. Аналізуючи Концепцію побудови Єдиної судової інформаційно-телекомунікаційної системи та керуючись приписами Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, автор визначає недоліки правового регулювання захисту інформації, що міститься у Єдиній судовій інформаційно-телекомунікаційній системі. Серед пропозицій щодо виправлення нормативних прогалин автор вважає доцільним передбачити забезпечення функції захисту інформації та інформаційних ресурсів від несанкціонованих дій та витоку; поширити дію захисту не лише на інформацію, що міститься у Єдиній судовій інформаційно-телекомунікаційній системі, але й на програмне забезпечення, що призначено для обробки цієї інформації; чітко визначити і закріпити відповідальність за забезпечення захисту інформації. В статті підсумовано, що нагальною проблемою залишається відсутність нормативного визначення поняття «єдина судова інформаційно-телекомунікаційна система», що порушує баланс між засобами захисту інформації в Єдиній судовій інформаційно-телекомунікаційній системі та її змістом, структурою, властивостями оброблюваної інформації, умовами та режимом експлуатації. Зазначені недоліки вважається доцільним усунути нормативними змінами до Концепції побудови Єдиної судової інформаційно-телекомунікаційної системи та подальшим відображенням в Положенні про неї. Результати дослідження засвідчили відсутність попереднього здійснення розробником Концепції побудови Єдиної судової інформаційно-телекомунікаційної системи процедури визначення й аналізу загроз, що мала передувати побудові системи захисту інформації. Підсумовано, що цей факт ускладнює розробку системних та ефективних засобів захисту від загроз та актуалізує необхідність виконання цього етапу в рамках подальшого розроблення та затвердження Положення про Єдину судову інформаційно-телекомунікаційну систему.

Ключові слова: захист інформації, Єдина судова інформаційно-телекомунікаційна система, правове забезпечення, інформаційно-телекомунікаційна система, програмне забезпечення, витік інформації, несанкціонований доступ.

The article is dedicated to the development of proposals for improving the legal protection of information in the Unified Judicial Informational and Telecommunication System. Analyzing the Conception of building the Unified Judicial Informational and Telecommunication System and guided by the provisions of the Law of Ukraine "On Information Protection in Informational and Telecommunication Systems" and the Rules for Information Protection in Informational, Telecommunication, Informational and Telecommunication Systems, the author identifies shortcomings in legal regulation of information protection contained in the Unified Judicial Informational and Telecommunication System. Among the proposals to correct regulatory gaps, the author considers it appropriate to provide for the protection of information and informational resources from unapproved actions and leakages; extend the protection not only on the information contained in the Unified Judicial Informational and Telecommunication System, but also on the software designed to process that information; clearly define and consolidate responsibility for ensuring the protection of information. The article concludes that the lack of normative definition of "unified judicial informational and telecommunication system" remains a pressing problem, which violates the balance between the means of information protection in the Unified Judicial Informational and Telecommunication System and its content, structure, properties of processed information, conditions and mode of operation. These shortcomings are considered appropriate to eliminate by regulatory changes to the Conception of building the Unified Judicial Informational and Telecommunication System and further reflected in its Regulations. The results of the study showed the lack of prior implementation by the developer of the Conception of building the Unified Judicial Informational and Telecommunication System the procedure of identifying and analyzing threats, which had to precede the construction of an information protection system. It is concluded that this fact complicates the development of systematic and effective means of information protection against threats and highlights the need to implement this stage in the further development and approval of the Regulation of the Unified Judicial Informational and Telecommunication System.

Key words: information protection, Unified Judicial Informational and Telecommunication System, legal support, informational and telecommunication system, software, information leakage, unapproved access.

Постановка проблеми. Аналіз останніх досліджень і публікацій. Дослідники різних галузей знань суголосні в думці про те, що в сучасних державах інформація є стратегічним національним ресурсом, а інформаційна безпека виходить на перше місце в системі національної безпеки, у зв'язку з чим, формування й проведення єдиної державної політики в цій сфері вимагає пріоритетного розгляду [1].

Активні процеси інформатизації, що відбуваються в українському суспільстві, цифровізація державних послуг та становлення інститутів електронної демократії [2] набули нового значення за умов пандемії коронавірусу та встановлення карантину в Україні. Ситуація соціального дистанціювання особливо гостро актуалізувала запит суспільства на безперебійне виконання функцій держави «в режимі онлайн», технічну можливість якого забезпечує діяльність різноманітних інформаційно-телекомунікаційних систем.

Разом із тим, проблемами розвитку електронного урядування в Україні на законодавчому рівні залишаються низька якість управління розробленням, впровадженням, підтримкою функціонування та розвитком інформаційно-телекомунікаційних систем (бази даних, реєстри тощо) та ресурсів (центри обробки даних, телекомунікаційні мережі тощо) органів влади; а також несформованість базової інформаційно-телекомунікаційної інфраструктури електронного урядування як техніко-технологічної основи для реалізації всіх проектів і завдань у зазначеній сфері [3].

Розробка інформаційно-телекомунікаційних систем пов'язана із застосуванням сучасних інформаційних технологій, що, з одного боку, надають нові можливості

з обробки, передачі та зберігання інформації, підвищуючи рівень доступності інформаційних ресурсів для користувача, а з іншого, можуть бути не тільки корисними, але й небезпечними для інформаційних систем та мереж [4]. У той же час, активний «перехід» адміністративних послуг та державних сервісів у режим онлайн супроводжується появою нових безпекових викликів, що пов'язані з поширенням таких видів протиправної діяльності як кіберзлочинність, фішинг, комп'ютерне шахрайство, несанкціонований доступ, несанкціоноване перехоплення тощо. Варто враховувати і те, що обсяг оперативної інформації (у тому числі, конфіденційної, службової, секретної), що міститься і обробляється в інформаційно-телекомунікаційних системах, у подальшому буде зростати, зважаючи на закріплення цього напряму на рівні численних нормативно-правових актів та нещодавнє створення профільного Міністерства цифрової трансформації України.

У цьому зв'язку проблема комплексного захисту сучасних інформаційно-телекомунікаційних систем, які застосовуються у роботі органів державної влади, набуває особливого значення як для цих органів, так і для правників-науковців, оскільки стає засадничою передумовою формування національної безпеки України в інформаційній сфері. Як справедливо зазначають дослідники у галузі інформаційного права [5], первинним етапом побудови комплексної системи захисту інформації у сучасних інформаційно-телекомунікаційних системах стає розробка відповідного нормативно-правового забезпечення. Саме **тому метою даної наукової розвідки** є розробка пропозицій щодо удосконалення правового забезпечення захисту досі нерозробленої Єдиної судової інформаційно-телекомунікаційної системи (далі – ЄСІТС) як інформаційно-телекомунікаційної системи та інформації, що міститься у ній.

Зазначимо, що одним із наочних прикладів застосування інформаційно-телекомунікаційних систем у забезпеченні діяльності інститутів електронної демократії в Україні варто визнати Єдину судову інформаційно-телекомунікаційну систему (далі – ЄСІТС), розробка і реалізація якої спрямована на запровадження в Україні системи електронного судочинства.

Зауважимо, що ЄСІТС як технологічна новела судової системи України поки не стала предметом системних наукових досліджень у галузі права. Наявні наукові дослідження, що присвячені аналізу особливостей розробки і запровадження ЄСІТС (роботи О. Берназюка [6] та М. Гетманцева [7]) мають здебільшого оглядово-теоретичний характер, що ознайомлюють читачів із процесуальними особливостями запровадження ЄСІТС, її основними змістовими компонентами, значенням для судової системи України в цілому. У той же час, недослідженими в українському науково-правничому дискурсі залишаються прикладні питання, пов'язані з розробкою пропозицій щодо удосконалення правового забезпечення ЄСІТС та окремих аспектів в цьому напрямі – зокрема, щодо правового забезпечення захисту інформації, що міститься у ЄСІТС. Ця проблематика в умовах активізації роботи над предметною розробкою ЄСІТС (відповідно до повідомлення Вищої ради правосуддя від 27.03.2020 року [8]) набуває прикладного характеру, оскільки може бути врахована під час затвердження Положення про Єдину судову інформаційно-телекомунікаційну систему.

Виклад основного матеріалу. Варто нагадати, що відправлення правосуддя судами за допомогою ЄСІТС було запроваджено Законом України «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» [9], що набув чинності наприкінці 2017 р. Незважаючи на те, що Єдина судова інформаційно-телекомунікаційна система мала запрацювати в Україні ще з 01.03.2019 року [10], проте це рішення було відкликано [11]. Серед напрямів, які вдалось реалізувати на шляху її запровадження наразі варто відзначити лише:

– затвердження оновленої Концепції[1] побудови ЄСІТС (Наказ Голови Державної судової адміністрації України від 07.11.2019 року № 1096 [12]);

– тестування судами підсистеми «Електронний суд», що планується до запуску у червні 2020 року [13];

– впровадження системи відеоконференцзв'язку, що забезпечує можливість дистанційної участі сторін у судових засіданнях в режимі відео конференції поза межами суду, а також підтвердження (ідентифікацію) таких осіб шляхом використання електронного підпису [13] (при чому цей модуль почав роботу лише з травня 2020 року).

Наше попереднє дослідження, присвячене аналізу особливостей господарської діяльності державного підприємства «Інформаційні судові системи» (розробника ЄСІТС), засвідчило, що одним із чинників пролонгації розроблення і повноцінного запровадження ЄСІТС в Україні є «адміністративна монополія» цього державного підприємства на розроблення ЄСІТС. Окрім цього, чинником повільних темпів розроблення і запровадження ЄСІТС слід вважати і відсутність відповідної нормативно-правової бази, яка б у правовому полі регламентувала відповідальність розробника за порушення строків розроблення складників ЄСІТС. Наразі єдиним правовим актом, що дає уявлення про структуру, особливості діяльності та схематичний план розроблення Єдиної судової інформаційно-телекомунікаційної системи залишається Концепції побудови ЄСІТС, до аналізу якої ми пропонуємо звернутись, послуговуючись метою даного дослідження.

Перша проблема, яка привертає дослідницьку увагу під час системного аналізу положень Концепції, - це ***відсутність визначення поняття «єдина судова інформаційно-телекомунікаційна система»***. На наше переконання, формування такої дефініції та її закріплення у Положенні про ЄСІТС має не лише концептуально-теоретичне, але й практичне значення, оскільки вимоги до системи захисту інформаційно-телекомунікаційної системи визначаються, перш за все, змістом та структурою системи, властивостями оброблюваної у ній інформації, умовами та режимом її експлуатації тощо.

Послуговуючись формально-логічним підходом до визначення понять через зазначення роду та видових відмінностей, нам вважається доцільним послуговуватись синтезом визначень категорій «інформаційна система» та «телекомунікаційна система», наведених в Законі України «Про захист інформації в інформаційно-телекомунікаційних системах», розуміючи під інформаційно-телекомунікаційною системою – діючу як єдине ціле сукупність інформаційних (автоматизованих) та телекомунікаційних систем, в якій за допомогою технології обробки інформації та з використанням сукупності технічних і програмних засобів забезпечується обмін інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [14].

Для зазначення видових відмінностей поняття «єдина судова інформаційно-телекомунікаційна система» доцільно звернутись до переліку основних завдань ЄСІТС, наведених у Концепції, серед яких виокремлюють, зокрема: ведення в судах електронного діловодства; централізоване захищене зберігання судових справ; збереження судових справ та інших документів в електронному архіві; обмін документами та інформацією в електронній формі між судами, іншими органами системи правосуддя, учасниками судового процесу; автоматизацію роботи

[1] Зважаючи на відсутність затвердженого Положення про Єдину судову інформаційно-телекомунікаційну систему, фактично єдиним актом аналізу в рамках даної роботи є Концепція побудови ЄСІТС.

судів, органів та установ системи правосуддя; віддалений доступ користувачів ЄСІТС до будь-якої інформації, що в ній зберігається; розподіл справ; аудіо- та відеофіксацію судових засідань; ведення Єдиного державного реєстру судових рішень, Єдиного державного реєстру виконавчих документів; функціонування офіційного веб-порталу судової влади України, єдиного контакт-центру для управління запитами, іншими зверненнями; можливість автоматизованої взаємодії ЄСІТС з іншими інформаційно-телекомунікаційними системами тощо (наведений перелік не є вичерпним, детальніше див. [12]).

Як бачимо, на Єдину судову інформаційно-комунікаційну систему покладено широкий спектр завдань, що охоплюють діяльність не лише органів судової влади, але й технологічну взаємодію з іншими суб'єктами публічного адміністрування. Інформація, що міститься в ЄСІТС, потенційно може бути об'єктом різноманітних протиправних несанкціонованих дій з метою перешкоджання нормальному функціонуванню як судів, так і інших органів державної влади. При цьому, варто зазначити, що в Концепції побудови ЄСІТС і в майбутньому Положенні про ЄСІТС було б доречно окремо зазначити, що ця система ***забезпечуватиме функцію захисту інформації***, ***яка буде міститися в ЄСІТС, від несанкціонованих дій*** (наразі згадка про таку функцію відсутня).

У той же час у Концепції побудови ЄСІТС присутньою є недеталізована згадка про комплексну системи захисту інформації (далі - КСЗІ). Зазначимо, що комплексна система захисту інформації є одним із чотирьох складників цільової архітектури ЄСІТС. Вона представляє собою підсистему, що має реалізовувати в захищеному та відкритому середовищах ЄСІТС функціонал комплексу організаційних, програмних і технічних заходів для забезпечення конфіденційності, цілісності, доступності інформаційних ресурсів на всіх стадіях їх зберігання, оброблення та передачі [12].

Відповідно до Концепції побудови ЄСІТС забезпечення захисту інформаційних ресурсів ЄСІТС здійснюватиметься шляхом застосування засобів і методів технічного захисту інформації, впровадження організаційних та інженерно-технічних заходів комплексної системи захисту інформації, спрямованих на недопущення блокування інформації, несанкціонованого доступу до неї, її модифікації або спотворення [12]. Проте набір цих засобів та безпосередній об'єкт захисту видається нам обмеженим, оскільки відповідно до статті 2 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [14] об'єктом захисту в системі є не лише інформація, що в ній обробляється, ***а й програмне забезпечення,*** яке призначено для обробки цієї інформації (зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів). У зв'язку з цим, нам видається доречним передбачити у майбутньому Положенні про ЄСІТС припису про те, що комплексна система захисту ЄСІТС забезпечуватиме ***й захист програмного забезпечення, яке використовуватиметься для її функціонування***.

Варто звернути увагу на те, що визначені в Концепції побудови ЄСІТС завдання щодо забезпечення захисту інформаційних ресурсів ЄСІТС від протиправних дій в цілому відповідають приписам Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [14], в тому числі, щодо захисту від блокування інформації, знищення, порушення цілісності інформації та несанкціонованих дій щодо інформації в цій системі. Проте, на наше переконання, було б доречним передбачити і в Концепції побудови ЄСІТС, і в майбутньому Положенні організаційні та інженерно-технічні заходи, засоби і методи захисту інформації, яка міститься в ЄСІТС, ***від витоку*** цієї інформації. Відповідно до зазначеного закону під витоком інформації розуміється результат дій, внаслідок яких інформація в інформаційно-телекомунікаційній системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї. Зважаючи на це, видається важливим внесення відповідних змін до Концепції побудови ЄСІТС та визначення ***функції захисту*** інформаційних ресурсів, які містимуться в ЄСІТС, ***від витоку*** в майбутньому Положенні про цю систему.

В науковій літературі під захистом інформації розуміють «цілеспрямовану діяльність власників інформації, спрямовану на виключення чи суттєве обмеження можливостей її витоку, нав'язування, блокування або знищення» [15, с. 126]. Це визначення акцентує нашу увагу на значущій ролі такого суб'єкта як власник інформації у формуванні стратегій захисту інформації в інформаційно-телекомунікаційних системах. Це знайшло своє відображення у статті 9 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [14], відповідно до якої ***відповідальність за забезпечення захисту інформації***, яка міститься в інформаційно-телекомунікаційній системі, покладається на власника цієї системи. У зв'язку з цим, вкрай важливим видається визнання Державної судової адміністрації України (або іншого органу судової влади) власником ЄСІТС у відповідному Положенні про неї.

Таке акцентування пояснюється тим, що наразі в умовах відсутності ЄСІТС в судах функціонує Автоматизована система документообігу суду (далі - АСДС), в Положенні про неї, затвердженому рішенням Ради суддів України від 26.11.2010 року № 30 [16], відсутнє визначення власника цієї системи, а ДСА України визнається володільцем інформації АСДС. Така нормативна прогалина створює ризики управлінської безвідповідальності, адже володілець інформації, яка міститься в інформаційно-телекомунікаційній системі, не несе відповідальності за незабезпечення належного захисту інформації, що міститься системі. Послуговуючись тим, що зазначеною нормою передбачено утворення власником системи служби захисту інформації або призначення осіб, на яких покладається забезпечення захисту інформації та контролю за ним, нам ***уявляється доречним визначення власником ЄСІТС саме ДСА України,*** адже утворення такої служби захисту інформації, яка міститься в ЄСІТС, не передбачено законодавством України про судоустрій щодо інших органів судової влади. Перевага нашого висновку підкріплена тим, що відповідно до статті 10 наведеного закону, ДСА України як розробник Концепції побудови ЄСІТС та Положення про неї, за погодженням з Адміністрацією Держспецзв'язку (що є спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації), може встановлювати особливості захисту інформаційних ресурсів або інформації з обмеженим доступом, що міститимуться в ЄСІТС.

Привертають увагу окремі аспекти невідповідності Концепції побудови ЄСІТС Правилам забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, що затверджені Постановою КМУ від 29.03.2006 року № 373 [17].

По-перше, відповідно до Концепції побудови ЄСІТС у рамках створення комплексної системи захисту інформації передбачена двохфакторна автентифікація користувачів, в тому числі за допомогою електронного цифрового підпису користувача. При цьому, суть цієї двохфакторної процедури автентифікації у Концепції не розкривається, що було б доречним для спрощення її розуміння, як розробником ЄСІТС, так і майбутніми користувачами. Так само Концепцією не передбачено здійснення процедури ідентифікації користувачів інформації. Відповідно до при-

писів вищезазначених Правил, автентифікація – це процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора, а ідентифікація – це процедура розпізнавання користувача в системі за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, що сприймається системою. Як бачимо, автентифікація та ідентифікація є різними процедурами, що мають нормативно встановлюватися окремо.

По-друге, Концепція побудови ЄСІТС передбачає моніторинг та кореляції подій інформаційної безпеки – збір даних для комплексного аналізу щодо подій інформаційної безпеки, які виникають в системі, організацію моніторингу подій в журналах реєстрації подій та здійснення безперервного аудиту стану інформаційної безпеки в ЄСІТС [12]. Проте у Концепції не розкрито способи здійснення зазначених процедур, не передбачено розроблення та функціонування в ЄСІТС обов'язкової реєстрації автоматичним способом результатів ідентифікації та автентифікації користувачів, результатів виконання користувачем операцій з обробки інформації, спроб несанкціонованих дій з інформацією, фактів надання та позбавлення користувачів права доступу до інформації та її обробки, результатів перевірки цілісності засобів захисту інформації тощо. Врахування цих функціональних напрямів в рамках діяльності комплексної системи захисту інформації у ЄСІСТ нам вбачається вкрай актуальним та необхідним, враховуючи той факт, що «захист інформації має бути забезпечений на всіх стадіях життєвого циклу інформаційно-телекомунікаційної системи, на всіх технологічних етапах оброблення інформації і в усіх режимах функціонування» [1, с.112].

По-третє, в Концепції побудови ЄСІТС не йдеться про необхідність створення служби захисту інформації та щодо покладеного на службу обов'язку розробити План (технічне завдання) захисту інформації. Цей аспект відповідно до зазначених Правил має визначатися та погоджуватися з Адміністрацією Держспецзв'язку вже на етапі створення ЄСІТС. Доречним вбачається передбачити в Концепції, що План захисту ЄСІТС визначатиме завдання захисту, класифікації інформації, яка оброблятиметься в ЄСІТС, загальний опис технології обробки інформації, визначення моделі загроз для інформації, яка міститься в ЄСІТС, основні вимоги щодо захисту інформації та правил доступу до неї, перелік документів забезпечення захисту інформації в ЄСІТС тощо.

Відповідно до ДСТУ 3396.0-96 побудові системи захисту інформації передують такі етапи: а) визначення й аналіз загроз; б) розроблення системи захисту інформації; в) реалізація плану захисту інформації; г) контроль функціонування та керування системою захисту інформації [18]. Результати нашого дослідження засвідчили фактичну відсутність етапу визначення й аналізу загроз, що мало передувати побудові системи захисту інформації в ЄСІТС. Це, з одного боку, унеможливлює розробку системних та ефективних засобів захисту від загроз, а з іншого, актуалізує обов'язковість виконання цього етапу в рамках подальшого розроблення та затвердження Положення про ЄСІТС.

Висновки. Перспективи продовження та повторення карантину в Україні сприяють активізації розроблення і запровадження Єдиної судової інформаційно-комунікаційної системи, появі якої має передувати розвиток комплексної системи правових засад та технологічних засобів захисту інформації, що міститься в ній. Аналіз моделі правового регулювання захисту інформації у ЄСІТС, викладеного у Концепції, засвідчив наявність декількох нормативних прогалин, що потребують правового регулювання. Серед пропозицій щодо виправлення нормативних прогалин нам вважається доцільним передбачити забезпечення функції захисту інформації та інформаційних ресурсів від несанкціонованих дій та витоку; поширити дію захисту не лише на інформацію, що міститься у ЄСІТС, але й на програмне забезпечення, яке призначено для обробки цієї інформації; чітко визначити і закріпити відповідальність за забезпечення захисту інформації; привести функціональні напрями комплексної системи захисту інформації у відповідність до нормативних приписів Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, що затверджені Постановою КМУ від 29.03.2006 року № 373. Нагальною проблемою залишається відсутність нормативного визначення поняття «єдина судова інформаційно-телекомунікаційна система», що порушує баланс між засобами захисту інформації в ЄСІТС та її змістом, структурою, властивостями оброблюваної інформації, умовами та режимом експлуатації, що варто було б усунути або змінами до Концепції, або відображенням в Положенні про ЄСІТС.

ЛІТЕРАТУРА

1. Нашинець-Наумова А. Організація системи захисту інформації суб'єктів господарювання. *Підприємництво, господарство і право*. Випуск №2/2016. С. 110-116.
2. Бринцев О. В. «Електронний суд» в Україні. Досвід та перспективи : монографія / О. В. Бринцев. Х. : Право, 2016. 72 с.
3. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження КМУ від 20.09.2017 р. №649-р. URL : https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80.
4. Чунарьова А.В., Чунарьов А.В. Аналіз нормативно-правового забезпечення захисту інформації сучасних ІКСМ. Науково-практичний журнал «Захист інформації» № 2, 2012. С. 6-8.
5. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособие. – М.: Горячая линия – Телеком, 2004. – 280 с.
6. Берназюк О. Єдина судова інформаційно-телекомунікаційна система: поняття та структура. *Підприємництво, господарство і право*. №6/2019. С. 326-330.
7. Гетманцев М.О. Єдина судова інформаційно-телекомунікаційна система: реальність і виклики сьогодення. *Підприємництво, господарство і право*. 2017. №4. С. 179-183.
8. Про повернення на доопрацювання проекту Положення про Єдину судову інформаційно-телекомунікаційну систему : рішення Вищої ради правосуддя №624/0/15-19 від 18 лютого 2019 року. URL : http://www.vru.gov.ua/act/17577.
9. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів : Закон України від 03.10.2017 № 2147-VIII. URL : https://zakon.rada.gov.ua/laws/show/2147-19 (дата звернення 20.04.2020).
10. Щодо створення та забезпечення функціонування Єдиної судової інформаційно-телекомунікаційної системи: повідомлення Державної судової адміністрації України. *Голос України*. 2018. №229 (6984). URL : http://www.golos.com.ua/edition_archive/2018-12.
11. Про повернення на доопрацювання проекту Положення про Єдину судову інформаційно-телекомунікаційну систему : рішення Вищої ради правосуддя №624/0/15-19 від 18 лютого 2019 року. URL : http://www.vru.gov.ua/act/17577.
12. Наказ Державної судової адміністрації України від 07 листопада 2019 року №1096 Про забезпечення створення і функціонування Єдиної судової інформаційно-телекомунікаційної системи. URL : https://dsa.court.gov.ua/dsa/inshe/esits/N_1096_19.
13. Відповідь на запит на публічну інформацію Георгієвського Ю.В. ДСА від 18.05.2020 № інф/Г-427-20-426/20.
14. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 року № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. ст.286.

15. Шепета О. Адміністративно-правові засади технічного захисту інформації : дис. … канд. юрид. наук : спец. 12.00.07 «Теорія управління; адміністративне право і процес; фінансове право; інформаційне право» / О. Шепета ; Нац. академія Служби безпеки України. – К., 2011. – 215 с.

16. Положення про автоматизовану систему документообігу суду : Рішення Ради суддів України 26.11.2010 року № 30 (у редакції рішення Ради суддів України від 02 березня 2018 року № 17). URL : https://court.gov.ua/sudova-vlada/969076/polozhenniapasds/ (дата звернення 05.05.2020).

17. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова КМУ від 29 березня 2006 р. N 373. URL : https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF (дата звернення 05.05.2020).

18. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. – К. : Держстандарт України, 1997. – 15 с.