УДК: 343.3/.7

DOI: <https://doi.org/10.32366/2523-4269-2021-75-2-124-131>

Щербіна Артем Валентинович,

аспірант

(Донецький державний університет

внутрішніх справ, м. Маріуполь)

ORCID: <https://orcid.org/0000-0001-8600-1829>

ГЕНЕЗА ТА ПЕРЕДУМОВИ РОЗВИТКУ АВТОМАТИЗОВАНОЇ СИСТЕМИ ДОКУМЕНТООБІГУ СУДУ В УКРАЇНІ

У статті розглядаються особливості розвитку автоматизованої системи документообігу суду в Україні. Зазначається, що процес становлення досліджуваного феномену можна умовно поділити на кілька етапів. Звертається увага на те, що розвиток автоматизованої системи документообігу суду став одним із напрямів удосконалення процесу інформатизації та комп'ютеризації діловодства в державі, підтвердженням стрімкої еволюції технічного прогресу. На сьогодні зазначена система надає можливість не тільки прискорити процес роботи, а й дозволяє отримати швидкий доступ до необхідних документів, які знаходяться у вільному користуванні в інтернет-мережі. Однак саме спрощення інформаційної взаємодії призвело до виникнення низки ситуацій, які становлять загрозу кримінологічній безпеці України, у зв'язку з чим у 2009 році було прийнято рішення про криміналізацію незаконного втручання в роботу автоматизованої системи документообігу суду. Захист інформації, яка належить судовій системі, є не менш важливим та може розглядатися як один із напрямів захисту нашої держави.

Ключові слова: інформаційна безпека; інтернет-мережа; кримінальне законодавство; кримінальне правопорушення; автоматизована система документообігу суду; діджиталізація.

Постановка проблеми. Історія кримінального законодавства починається майже одночасно з історією виникнення людства, а тому і їх розвиток відбувається синхронно та поетапно. Звичайно, це здебільшого стосується підходів до визнання того чи іншого діяння протиправним та кримінально караним, установлення меж кримінальної відповідальності тощо. Очевидним є той факт, що Особлива частина кримінального законодавства створена дійсно раніше, ніж Загальна, що обумовлено тривалим прогресом суспільства, а тому і, відповідно, тривалим визнанням необхідності структурованого та єдиного бачення схеми взаємодії з особою, яка вчинила суспільно небезпечне діяння. Більшість таких діянь уперше були визнані протиправними ще в давні часи та каралися згідно з тогочасним «законом». При цьому не можна залишити без уваги й те, що чинний Кримінальний кодекс України 2001 року (далі – КК України) має низку абсолютно нових кримінальних правопорушень, які з'явилися внаслідок зміни суспільного менталітету, технічного прогресу тощо. Одним із

таких кримінальних правопорушень є незаконне втручання в роботу автоматизованої системи документообігу суду, кримінальна відповідальність за яке передбачена ст. 376-1 КК України. Ураховуючи, що вказане діяння є абсолютно новим, вважаємо доцільним дослідити основні історичні передумови його виникнення та кримінально-правового захисту.

Аналіз останніх досліджень та публікацій. На сьогодні кримінальне правопорушення, передбачене ст. 376-1 КК України, залишається не достатньо дослідженим. Окремі аспекти висвітлено в працях таких учених, як В. І. Саранюк, В. А. Козак, О. В. Федорчук та ін.

Метою статті є дослідження генези та передумов розвитку автоматизованої системи документообігу суду в Україні та визначення перспектив подальшого розвитку й удосконалення вітчизняного кримінального законодавства.

Виклад основного матеріалу. На нашу думку, початком криміналізації досліджуваного феномену є прагнення законодавця до захисту інформації та закріплення дефініції «інформаційна безпека», що було вдало реалізовано шляхом внесення до Конституції України ст. 17, у якій встановлено, що захист суверенітету й територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [1]. Тому на конституційному рівні в державі було визнано пріоритетом забезпечення інформаційної безпеки. Варто зазначити, що на сьогодні підходи до вказаного поняття як в загальному, так і в кримінально-правовому сенсі є не повністю однозначними, що можна пояснити неповноцінною узгодженістю положень відповідних нормативно-правових актів.

Так, у Законі України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 року вказано, що інформаційна безпека є невід’ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. До об’єктів інформаційної безпеки цей закон відносить: інформаційні ресурси, канали інформаційного обміну й телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни. Отже, інформаційна безпека в цьому нормативно-правовому акті розуміється як комплекс заходів, спрямованих на забезпечення захисту інформації від неправомірного витоку, перекручення, знищення тощо [2]. Зазначений нормативно-правовий акт визначає, що посягання на інформаційну безпеку є передусім кримінально караним діянням з огляду на рівень суспільної небезпечності, котра вимірюється державними масштабами. При цьому не можна не вказати, що досліджуваний феномен захищається і суміжними галузями права.

Приблизно той самий зміст досліджуване поняття має і в Рішенні Ради голів урядів Співдружності Незалежних Держав (далі – СНД) про Концепцію інформаційної безпеки держав-учасниць Співдружності Незалежних Держав у військовій галузі. Хоча термін «інформаційна безпека» визначається в цьому документі як «стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави», але використовується як близький за змістом до поняття «захист інформації». Про це насамперед свідчить визначення системи забезпечення інформаційної безпеки, яка розуміється як сукупність правових, організаційних і технічних заходів, органів, сил, засобів та норм, спрямованих на попередження або істотне ускладнення заподіяння шкоди власнику інформації, а також перелік методів забезпечення інформаційної безпеки, який фактично є переліком методів забезпечення захисту інформації [3, с. 12]. Отже, з контексту стає очевидним, що законодавець, коли йдеться про інформаційну безпеку, акцентує увагу на необхідності залучати комплекс заходів та засобів, здатних сприяти захисту тієї чи іншої інформації.

В Указі Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31 липня 2000 року поняття інформаційної безпеки вже не обмежується тільки захистом інформаційного ресурсу. Так, до завдань щодо гарантування інформаційної безпеки держави належить недопущення поширення інформації, розповсюдження якої заборонено

відповідно до законодавства. Отже, забезпечення інформаційної безпеки розуміється не тільки як захищеність інформаційного ресурсу, а й захищеність суспільства від розповсюдження «негативної» інформації (порнографія, пропаганда культу насильства та жорстокості тощо). Закон України «Про основи національної безпеки України» від 19 червня 2003 року використовує поняття «інформаційна безпека» у ще ширшому значенні. Про це свідчить зміст визначених у ньому загроз та напрямів державної політики в інформаційній сфері [3, с. 12]. Так, до загроз національній безпеці в інформаційній сфері Закон відносить: 1) прояви обмеження свободи слова та доступу громадян до інформації; 2) поширення через засоби масової інформації культу насильства, жорстокості, порнографії; 3) комп'ютерну злочинність та комп'ютерний тероризм; 4) розголошення інформації, яка становить державну та іншу передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; 5) намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації. Основними ж напрямками державної політики з питань національної безпеки Закон визначає: 1) забезпечення інформаційного суверенітету України; 2) удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; 3) активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України; 4) забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері та переслідування журналістів за політичні позиції; 5) вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України [3, с. 13]. Не можна ігнорувати той факт, що на сьогодні інформація – це один із потужних засобів впливу на суспільство. Саме інформаційна війна часто призводить до всесвітніх колапсів та здійснює деструктивний вплив на політичну та економічну систему держави.

Логічним продовженням такого підходу законодавця є визначення інформаційної безпеки, яке подано в Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 9 січня 2007 року: це «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації». Таке тлумачення достатньо чітко фіксує відхід законодавця від вузького розуміння інформаційної безпеки як технічного захисту інформації, її визначення сформульоване як стан захищеності від загроз інформаційного та технологічного характеру [3, с. 14]. Підтримуємо запропоновану дефініцію, оскільки вона охоплює максимальну кількість варіантів посягання на інформаційну безпеку.

Указом Президента України № 514/2009 від 8 липня 2009 року було затверджено Доктрину інформаційної безпеки України. Як слушно зазначає О. Г. Братель, цей документ становить «сукупність офіційних поглядів на мету, функції, принципи та методи забезпечення національної безпеки України в інформаційній сфері» [4, с. 37]. Розглянемо детальніше його положення. По-перше, підкреслюється подвійне значення інформаційної безпеки: 1) як невід'ємної складової кожної зі сфер національної безпеки; 2) як самостійної сфери національної безпеки. По-друге, класифікація життєво важливих інтересів в інформаційній сфері здійснюється за суб'єктом, тобто доктриною виокремлюються інтереси особи, суспільства та держави. До інтересів особи в доктрині віднесено: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та

розповсюдження інформації; недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних; захищеність від негативного інформаційно-психологічного впливу [3, с. 14]. Необхідно звернути увагу на те, що апіорі наша держава основною метою створення системи захисту інформації насамперед убачає реалізацію плану дій із забезпечення національної безпеки. Утім, на нашу думку, захист інформації, яка належить судовій системі, є не менш важливим та може розглядатися як один із напрямів захисту нашої держави. Варто зазначити, що популяризація терміна «інформаційна безпека» почала відбуватися з розвитком засобів масової інформації (особливо інтернет-мережі), переходом до автоматизації документообігу в Україні та загальної діджиталізації. Не можна ігнорувати той факт, що комп'ютеризація значно спрощує процес ведення тих чи інших справ, робить доступ до необхідних документів максимально швидким та зручним. Саме так український законодавець наближається до європеїзації, розбудовуючи державу та враховуючи інтереси її громадян.

У загальному сенсі інтереси суспільства полягають у збереженні та примноженні духовних, культурних і моральних цінностей українського народу; забезпеченні суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди; формуванні й розвитку демократичних інститутів громадянського суспільства. Тлумачення поняття «державні інтереси» сформульовано так: недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур; ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригування державної політики в інформаційній сфері; побудова та розвиток інформаційного суспільства; забезпечення економічного та науково-технологічного розвитку України; формування позитивного іміджу України; інтеграція України у світовий інформаційний простір. По-третє, у доктрині визначено основні реальні й потенційні загрози інформаційній безпеці в певних сферах та основні напрями протидії їм. Таким чином, аналіз національного законодавства дає підстави стверджувати, що наявною є тенденція до розширення змісту законодавчого визначення поняття «інформаційна безпека». З розвитком інформатизації суспільства та вдосконаленням нормативно-правового забезпечення цих процесів розуміння інформаційної безпеки на законодавчому рівні пройшло шлях від вузького, найпростішого її визначення як технічного захисту інформації до складної розгалуженої системи [3, с. 15]. На нашу думку, з кримінально-правової точки зору *інформаційну безпеку* необхідно розуміти як *сукупність кримінально-правових засобів та заходів, які створюють алгоритм активної протидії протиправному посяганням на права, свободи та законні інтереси фізичних і юридичних осіб, а також держави та суспільства в цілому шляхом нанесення шкоди через негативний інформаційний вплив* (курсив мій. – А. Щ.). До того ж необхідно чітко усвідомити принципову різницю між інформаційною безпекою та безпекою інформації. На наш погляд, *безпекою інформації є стан захисту тих чи інших даних від несанкціонованого доступу з метою внесення неправдивих та/або несвоєчасних відомостей* (курсив мій. – А. Щ.). У межах досліджуваної ст. 376-1 чинного КК України, яка передбачає кримінальну відповідальність за незаконне втручання в роботу автоматизованої системи документообігу суду, доцільніше говорити про посягання саме на безпеку інформації. Варто також зазначити, що вказана стаття є новелою кримінального законодавства, яка стала логічним завершенням процесу прийняття низки нормативно-правових актів як з питань захисту інформації та інформаційної безпеки, так і вдосконалення роботи судової системи України.

Програмою інтеграції України до Європейського Союзу (далі – Програма), схваленої Указом Президента № 1072/2000 від 14.09.2000 р., було визначено пріоритетність співробітництва України з Європейським Союзом (далі – ЄС), зокрема і стосовно судової системи, та закріплено вирішення питання щодо запровадження в Україні системи органів адміністративної юстиції, у тому числі адміністративних судів, а також прийняття адміністративного процесуального законодавства. Серед іншого, Програма передбачала здійснення Україною дій для поліпшення доступу до інформації стосовно рішень судів [5].

Якщо починати розгляд законодавчої ієрархії зверху, то можна помітити основні засади такого інформаційного забезпечення як будь-яких державних установ, так й адміністративного судочинства в Конституції України від 28 червня 1996 року. Переважно в її приписах містяться загальні та непорушні права людини і громадянина та завдання держави, які формують її пріоритетну й основну політику забезпечення інформаційної безпеки та встановлення її основоположною функцією держави (ч. 1 ст. 17), кожному гарантується право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення (ч. 2 ст. 50) тощо. Однак Конституція України не визначає основ інформаційного забезпечення адміністративного судочинства, таке явище більш поширене на рівні законів України [1]. Серед законодавства, яке створює базис для формування інформаційного забезпечення тих самих окружних адміністративних судів України, слід виокремити Кодекс адміністративного судочинства України, який поступово з перебігом часу та нововведень умістив у себе основу інформаційної політики судового апарату, а також Закон України «Про судоустрій і статус суддів», що визначив організацію судової влади на всіх рівнях та в різних правових сферах правосуддя України [6; 7]. Отже, як бачимо, розвиток автоматизованої системи документообігу суду було розпочато ще до прийняття у 2001 році Кримінального кодексу України. Це було спрямовано насамперед на захист документації, яка належить судовій системі, а також на спрощення самого процесу документообігу.

Закон України «Про внесення змін до деяких законодавчих актів України щодо запровадження автоматизованої системи документообігу в адміністративних судах» від 5 червня 2006 року започаткував та передбачив функціонування такої автоматичної системи, яка позитивно вплинула на діяльність судового апарату [7]. Додатком до цього Закону можна назвати Положення про автоматизовану систему документообігу суду, яке було затверджено Радою суддів України від 26 листопада 2010 року. Згідно з цим положенням автоматизована система документообігу суду становить сукупність комп'ютерних програм і відповідних програмно-апаратних комплексів судів та Державної судової адміністрації України, що забезпечує функціонування документообігу суду, обіг інформації між судами різних інстанцій та спеціалізацій, передачу інформації до центральних баз даних залежно від спеціалізації судів, захист від несанкціонованого доступу тощо [6]. Саме така система є основою для сучасної бази, яка постійно оновлюється відповідно до вимог захисту та інших необхідних для її існування характеристик. Пізніше саме Кодексом адміністративного судочинства було встановлено головну мету автоматизованої системи, її завдання та порядок функціонування в ст. 15-1, що прямо вказало на її провідну роль у системі інформаційного забезпечення і окружних адміністративних судів. Ще одним складником системи є Єдиний реєстр судових рішень, ведення якого забезпечується Державною судовою адміністрацією України, а основні його положення та правові засади – Законом України «Про доступ до судових рішень» від 22 грудня 2005 року [7]. До речі, Єдиний реєстр судових рішень на сьогодні є достатньо популярним ресурсом, який надає доступ до найважливіших документів судів України, при цьому персональні дані, які відповідно до вимог нормативно-правових актів України не мають бути розповсюджені, надійно захищені. У реєстрі викладена виключно загальна інформація, яка не може жодним чином негативно вплинути на права та інтереси суб'єктів захисту. У цьому контексті можна стверджувати про диференційований та виважений підхід законодавця до безпеки інформації та захисту персональних даних.

Завдяки цьому адміністративне судочинство мало змогу швидко та ефективно розвивати внутрішню систему взаємозв'язків між судами, що впливало й на швидкість прийняття рішень у справах. Порядок формування та ведення реєстру було затверджено Кабінетом Міністрів України в постанові від 25 травня 2006 року [7]. У цьому документі також було визначено питання стосовно його фінансування, особливості програмного забезпечення, повноваження адміністраторів і держателів реєстру та інші умови функціонування, за яких його робота буде злагодженою та максимально ефективною в ході змін, доповнень або інших дій, які вплинуть на його існування [7]. На підставі зазначеного можна зробити висновок, що

саме з 2006 року розпочався активний розвиток автоматизованої системи документообігу суду, що зумовило необхідність кримінально-правової охорони.

Саме тому в ч. 1 Закону України від 5 червня 2009 року № 1475-VI «Про внесення змін до деяких законодавчих актів України щодо запровадження автоматизованої системи документообігу в адміністративних судах» було вказано на необхідність доповнити Кримінальний кодекс України статтею 376-1 такого змісту: «Стаття 376-1. Незаконне втручання в роботу автоматизованої системи документообігу суду. 1. Умисне внесення неправдивих відомостей чи несвоєчасне внесення відомостей до автоматизованої системи документообігу суду, несанкціоновані дії з інформацією, що міститься в автоматизованій системі документообігу суду, чи інше втручання в роботу автоматизованої системи документообігу суду, вчинене службовою особою, яка має право доступу до цієї системи, або іншою особою шляхом несанкціонованого доступу до автоматизованої системи документообігу суду, – караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк від одного до трьох років. 2. Дії, передбачені частиною першою цієї статті, вчинені за попередньою змовою групою осіб, – караються обмеженням волі на строк від трьох до п'яти років або позбавленням волі на строк від трьох до шести років, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк від двох до трьох років» [8]. Станом на 2021 рік ця редакція статті залишається актуальною та лише очікує зміни у зв'язку з прийняттям відповідних нормативно-правових актів.

Законом України «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» від 3 жовтня 2017 року в роботу адміністративного судочинства було внесено низку позитивних змін, зокрема щодо інформаційного забезпечення. Так, у вказаному Законі було ухвалено пріоритетність інформаційного забезпечення в судах та створення Єдиної судової інформаційно-телекомунікаційної системи (далі – ЄСІТС), яка фактично бере на себе головну роль у розпорядженні судовим процесом [7]. Статтею 18 Кодексу адміністративного судочинства України було визначено порядок та умови роботи системи, наголошуючи на тому, що законодавець має на меті повністю відцифрувати та перевести в електронний формат судовий процес [7].

Висновки. Отже, розвиток автоматизованої системи документообігу суду став одним із напрямів удосконалення процесу інформатизації та комп'ютеризації діловодства в державі, підтвердженням стрімкої еволюції технічного прогресу. На сьогодні вказана система надає можливість не тільки прискорити процес роботи, а й дозволяє отримати швидкий доступ до необхідних документів, які знаходяться у вільному користуванні через інтернет-мережу (прикладом є Єдиний реєстр досудових рішень тощо). Однак саме спрощення інформаційної взаємодії призвело до виникнення низки ситуацій, які створюють загрозу кримінально-правовій та кримінологічній безпеці України, у зв'язку з чим у 2009 році було прийнято рішення про криміналізацію незаконного втручання в роботу автоматизованої системи документообігу суду.

Необхідно зазначити, що розвиток досліджуваного феномену пройшов достатньо короткий шлях, який можна умовно поділити на декілька етапів, які його зумовили: 1) етап становлення та розвитку технічного прогресу в українській державі (1996–2001 рр.) – визнання забезпечення інформаційної безпеки та безпеки інформації найважливішою функцією держави; 2) етап активного нормативно-правового розвитку (2001–2009 рр.) – прийняття основних нормативно-правових актів України, запровадження автоматизованої системи документообігу в судах; 3) етап загальної діджиталізації суспільства (2009 р. – сьогодні) – активне використання автоматизованої системи документообігу суду, встановлення кримінально-правового захисту.

Список використаних джерел

1. Конституція України від 28.06.1996 № 254к/96-ВР. URL: <http://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80> (дата звернення: 19.04.2021).
2. Про Концепцію Національної програми інформатизації : Закон України від 4 лютого 1998 року № 75/98-ВР. URL: <https://zakon.rada.gov.ua/laws/show/75/98-вр#Text> (дата звернення: 19.04.2021).
3. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. 528 с.
4. Братель О. Поняття та зміст доктрини інформаційної безпеки. *Право України*. 2006. № 5. С. 36–41.
5. Про схвалення Програми інтеграції України до Європейського Союзу : Указ Президента України від 14 вер. 2000 р. № 1072/2000. *Офіційний вісник Президента України*. URL: <https://zakon.rada.gov.ua/laws/show/1072/2000#Text> (дата звернення: 19.04.2021).
6. Щодо Положення про автоматизовану систему документообігу суду : рішення Ради суддів України від 26 лист. 2010 р. № 30. *Вісник Верховного Суду України*. 2010. № 51. URL: <https://zakon.rada.gov.ua/rada/show/v0025414-15#Text> (дата звернення: 19.04.2021).
7. Кліщенко В. О. Історико-правовий генезис інформаційного забезпечення діяльності окружних адміністративних судів України. URL: http://lsej.org.ua/2_2020/61.pdf (дата звернення: 19.04.2021).
8. Про внесення змін до деяких законодавчих актів України щодо запровадження автоматизованої системи документообігу в адміністративних судах : Закон України від 5 червня 2009 року № 1475-VI. URL: <https://zakon.rada.gov.ua/laws/show/1475-17#Text> (дата звернення: 19.04.2021).

References

1. Konstytutsiia Ukrainy vid 28.06.1996 № 254k/96-VR [Constitution of Ukraine]. URL: <http://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80> (data zvernennia: 19.04.2021) [in Ukrainian].
2. Pro Kontseptsiiu Natsionalnoi prohramy informatyzatsii : Zakon Ukrainy vid 4 liutoho 1998 roku № 75/98-VR [About the concept of the National Informatization Program]. URL: <https://zakon.rada.gov.ua/laws/show/75/98-вр#Text> (data zvernennia: 19.04.2021) [in Ukrainian].
3. Karchevskiy, M. V. (2012). Kryminalno-pravova okhrona informatsiinoi bezpeky Ukrainy : monohrafiia [Criminal Protection of Information Security of Ukraine : monograph]. Luhansk : RVV LDUVS im. E. O. Didorenka. 528 s. [in Ukrainian].
4. Bratel, O. (2006). Poniattia ta zmist doktryny informatsiinoi bezpeky. [The concept and content of the doctrine of information security]. *Pravo Ukrainy*. № 5. S. 36–41 [in Ukrainian].
5. Pro skhvalennia Prohramy intehtatsii Ukrainy do Yevropeiskoho Soiuzu : Ukaz Prezydenta Ukrainy vid 14 ver. 2000 r. № 1072/2000 [On the approval of the Integration Program of Ukraine to the European Union : Decree of the President of Ukraine]. *Ofitsiyni visnyk Prezydenta Ukrainy*. URL: <https://zakon.rada.gov.ua/laws/show/1072/2000#Text> (data zvernennia: 19.04.2021) [in Ukrainian].
6. Shchodo Polozhennia pro avtomatyzovanu systemu dokumentoobihu sudu : rishennia Rady suddiv Ukrainy vid 26 lyst. 2010 r. № 30 [Regarding the Regulation on the Automated System of Documentation of the Court : the decision of the Council of Judges of Ukraine]. *Visnyk Verkhovnoho Sudu Ukrainy*. 2010. № 51. URL: <https://zakon.rada.gov.ua/rada/show/v0025414-15#Text> (data zvernennia: 19.04.2021) [in Ukrainian].
7. Klishchenko, V. O. Istoryko-pravovi henezys informatsiinoho zabezpechennia diialnosti okruzhnykh administratyvnykh sudiv Ukrainy [Historical and legal genesis of information

support of the district administrative courts of Ukraine]. URL: http://lsej.org.ua/2_2020/61.pdf (data zvernennia: 19.04.2021) [in Ukrainian].

8. Pro vnesennia zmin do deiakykh zakonodavchykh aktiv Ukrainy shchodo zaprovadzhennia avtomatyzovanoi systemy dokumentoobihu v administratyvnykh sudakh : Zakon Ukrainy vid 5 chervnia 2009 roku № 1475-VI [On amendments to some legislative acts of Ukraine regarding the introduction of an automated system of document circulation in administrative courts : Law of Ukraine]. URL: <https://zakon.rada.gov.ua/laws/show/1475-17#Text> (data zvernennia: 19.04.2021) [in Ukrainian].

Shcherbina Artem,
Graduate Student
(Donetsk State University of Internal Affairs, Mariupol)
ORCID: <https://orcid.org/0000-0001-8600-1829>

GENESIS AND PREREQUISITES OF THE DEVELOPMENT OF THE AUTOMATED COURT DOCUMENT SYSTEM IN UKRAINE

The article considers the peculiarities of the development of the automated court document management system in Ukraine. The author points out that the development of the studied phenomenon has passed a rather short way, which can be divided into several stages that led to it: 1) the stage of formation and development of technical progress in the Ukrainian state (1996–2001) – recognition of information security and information security the most important function of the state; 2) stage of active normative-legal development (2001–2009) – adoption of the basic normative-legal acts of Ukraine, introduction of the automated system of document circulation in administrative courts; 3) the stage of general digitalization of society (2009 – present) – the active use of the automated document management system of the court, the establishment of criminal protection. Attention is drawn to the fact that the development of an automated court document management system has become one of the ways to improve the process of informatization and computerization of office work in the country, confirming the rapid evolution of technical progress. Today, this system provides an opportunity not only to speed up the process, but also allows quick access to the necessary documents that are freely available via the Internet (an example is the Unified Register of pre-trial decisions, etc.). However, the simplification of information interaction has led to a number of situations that threaten the criminal law and criminological security of Ukraine, in connection with which in 2009 a decision was made to criminalize illegal interference in the automated document management system of the court. It turns out that the main purpose of creating an information protection system is, first of all, the implementation of an action plan to ensure national security. The protection of information belonging to the judiciary is no less important and can be considered as one of the areas of protection of our state. The popularization of the term «information security» began with the development of the media, the transition to document automation in Ukraine and general digitalization.

Key words: information security; Internet; criminal legislation; criminal offense; automated court document management system; digitalization.

Надіслано до редколегії 04.05.2021
Рекомендовано до публікації 11.05.2021