

## ПОНЯТТЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ДОКУМЕНТООБІГУ СУДУ ТА СОЦІАЛЬНА-ПРАВОВА НЕОБХІДНІСТЬ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ЇЇ НОРМАЛЬНОГО ФУНКЦІОНУВАННЯ

**ЩЕРБІНА Артем Валентинович - аспірант кафедри кримінального права та кримінології факультету № 1 Донецького державного університету внутрішніх справ**

**УДК: 343.3/.7  
DOI 10.32782/EP.2021.2.16**

*У статті автор розглядає поняття автоматизованої системи документообігу суду та досліджує соціальнo-правову необхідність кримінально-правової охорони її нормального функціонування. Вказується, що вивчення соціальної обумовленості кримінально-протиправних феноменів дозволяє своєчасно криміналізувати або декриміналізувати діяння, уникаючи при цьому виникнення у кримінальному законодавстві «мертвих» та «дрімаючих» норм. Саме соціальна обумовленість та історизм обумовлюють наступність у праві. На сьогодні в Україні більшість державних органів та установ ежe переходять на електронний спосіб ведення документації та ділового листування. Такий підхід дозволяє зберегти максимальну прозорість між учасниками та певним чином сприяє процесу боротьби з корупційними проявами. Створення єдиних аналітичних та інформаційних баз – достатньо дієвий спосіб забезпечити безпеку юридичних та фізичних осіб, шляхом збереження інформації, яка може бути використана як доказ від видалення та внесення неправдивих відомостей. Зазначається, що наразі наша країна регулярно проводить реформи майже у всіх сферах, не є винятком і реформування судової системи. На сьогодні не можна говорити про повну досконалість останньої. Український законодавець ще не в повній мірі готовий перейняти максимальну кількість позитивних напрацювань міжнародної та європейської спільноти та повніс-*

*тю позбавити судову систему суб'єктивізму та рудиментарних поглядів на відповідальність. Однак, криміналізація незаконного втручання в автоматизовану систему документообігу суду дозволило одним кроком вирішити декілька проблем: децю удосконалити судову систему в світлі її реформування та децю наблизитись до вимог міжнародної та європейської правової спільноти. Підсумовується, що автоматизована система документообігу суду наразі є єдиною інформаційно-аналітичною базою, яка здатна прискорити, полегшити та забезпечити обмін та отримання спеціальними (та в окремих випадках – загальними) суб'єктами необхідних даних у межах тих чи інших проваджень. Поява будь-якого нового феномену рано чи пізно призводить до виникнення нових форм кримінально-протиправної діяльності, у зв'язку із чим у 2009 році виникла гостра потреба такого кримінально-правового захисту.*

*Ключові слова: автоматизована система документообігу суду, криміналізація, кримінальне законодавство, кримінальне правопорушення, соціальна обумовленість, ретроспективний аналіз, комп'ютерне кримінальне правопорушення.*

### **Постановка проблеми**

У сучасних умовах законодавцеві важко своєчасно реагувати на нові тенденції, зміни менталітету та стрімкий розвиток технологічного прогресу. Саме у зв'язку із цим низка

фактичних кримінальних правопорушень залишається поза увагою юридично, через що кримінально-правова заборона такого роду суспільно небезпечних діянь встановлюється через деякий (часто – тривалий) часовий проміжок. Саме тому для науки кримінального права дуже цінним є вивчення соціальної обумовленості та безпосередньої сутності кожного окремого протиправного діяння, а також понятійно-категоріального апарату його безпосереднього предмета (за умови наявності такого). Ця теза стосується і досліджуваного нами кримінального правопорушення, яке полягає у незаконному втручанні в роботу автоматизованої системи документообігу суду, котре для чинного Кримінального кодексу України 2001 року є відносно новим суспільно небезпечним діянням.

#### **Аналіз останніх досліджень та публікацій**

На сьогодні кримінальне правопорушення, передбачене ст. 376-1 КК України, залишається не в повній мірі дослідженим. Окремі аспекти зустрічаються в працях таких учених як В.І. Саранюк, В.А. Козак, О.В. Федорчук та ін.

**Метою статті** є дослідження поняття автоматизованої системи документообігу суду, соціально-правова необхідність кримінально-правової охорони її нормального функціонування та визначення перспектив подальшого розвитку та удосконалення вітчизняного кримінального законодавства.

#### **Виклад основного матеріалу**

Учені правильно вказують, що під час криміналізації нових суспільно небезпечних діянь слід з'ясовувати, яких саме додаткових ресурсів і у якому обсязі потребуватиме втілення в життя нової кримінально-правової заборони. Водночас для визначення соціальної обумовленості наявної норми це не має принципового значення. За умови відсутності процесуальних ресурсів не можна казати про таку обставину соціальної обумовленості, як можливість боротьби із суспільно небезпечним діянням за допомогою

кримінально-правових засобів. Взаємозалежність наведених обставин убачається такою: спочатку слід визначитися з тим, можливо чи неможливо боротися з діянням за допомогою кримінально-правових засобів? І лише потім з'ясовувати, чи є на таку боротьбу ресурси? У разі негативної відповіді на перше поставлене питання, актуальність відповіді на друге втрачається. При цьому перша названа обставина передбачає можливість доказування діяння, а друга – орієнтує на наявність певного державного апарату, установ, фахівців, відповідних норм кримінального процесуального законодавства. Для охоронних кримінально-правових норм наявність ресурсів щодо здійснення кримінального переслідування має обов'язкове значення, для заохочувальних норм і норм-дефініцій наявність ресурсів для їхньої реалізації окремого значення не має, а для регулятивних норм – має факультативне значення [1, с. 137-138]. Вказана позиція ще раз наочно підтверджує те, що вивчення соціальної обумовленості кримінально протиправних феноменів дозволяє своєчасно криміналізувати або декриміналізувати діяння, уникаючи при цьому виникнення у кримінальному законодавстві «мертвих» та «дрімаючих» норм. Саме соціальна обумовленість та історизм обумовлюють наступність у праві. Отже, враховуючи вищевказане, вважаємо за доцільне розглянути більш детально соціальну обумовленість кримінального правопорушення, яке полягає у незаконному втручанні в роботу автоматизованої системи документообігу суду, розпочинаючи дослідження із встановлення поняття та сутності автоматизованої системи документообігу суду.

Так, відповідно до Положення про автоматизовану систему документообігу суду, затвердженого Рішенням Ради суддів України від 26.11.2010 № 30, під автоматизованою системою документообігу суду (далі – АСДС) необхідно розуміти сукупність комп'ютерних програм і відповідних програмно-апаратних комплексів, що входять до складу Єдиної судової інформаційної системи, та забезпечують виконання завдань, визначених цим Положенням, у тому числі таких, як: функціонування документообігу

суду та органів системи правосуддя; обмін інформацією між ними та з іншими органами державної влади; обмін з єдиною централізованою базою даних судової влади; оприлюднення інформації за допомогою офіційного веб-порталу судової влади України; захист інформації від несанкціонованого доступу, тощо [2]. Таким чином, автоматизована система документообігу суду є складною інформаційно-аналітичною базою, котра вміщує в себе сукупність даних, необхідних для реалізації судовою системою покладених на неї завдань. Основною рисою АСДС є те, що вона є *сукупністю комп'ютерних програм і відповідних програмно-апаратних комплексів*, що спрощує несанкціонований доступ до її даних особам, які мають відповідні знання та навички програмування.

Відповідно до вищевказаного Положення, АСДС та інші підсистеми мають у тому числі забезпечувати: 1) автоматизацію діловодства в судах та ОСП, у тому числі обмін інформаційними ресурсами у межах окремих органів, між судами, ОСП та учасниками судового процесу; 2) реєстрацію вхідної та вихідної кореспонденції, внутрішніх документів, судових справ, матеріалів судового провадження, скарг, заяв, клопотань та інших передбачених законом процесуальних документів, що подаються до суду і можуть бути предметом судового розгляду, в порядку їх надходження та фіксування етапів руху інформаційних ресурсів; 3) ведення єдиних довідників АСДС, обов'язкових для використання всіма судами та ОСП, у тому числі довідника учасників судової справи; 4) викладення (формування) оригіналів електронних судових рішень, виконавчих документів, інших документів у формі ЕД, створення ЕКПД доказів, процесуальних та інших документів, що подаються у паперовій формі, розмітка створених документів... [2]. На сьогодні в Україні більшість державних органів та установ уже переходять на електронний спосіб ведення документації та ділового листування. Такий підхід дозволяє зберегти максимальну прозорість між учасниками та певним чином сприяє процесу боротьби з корупційними проявами. На нашу думку, створення єдиних аналітичних та інформаційних баз – це достатньо дієвий

спосіб забезпечити безпеку юридичних та фізичних осіб, шляхом збереження інформації від видалення та внесення неправдивих відомостей.

АСДС та інші підсистеми мають також забезпечувати ... 5) збереження інформаційних ресурсів в електронному архіві та їх автоматизоване надсилання (відповідно до Протоколів обміну, затверджених адміністратором) до Єдиного державного реєстру судових рішень, Єдиного державного реєстру виконавчих документів та ЦБД, у тому числі для підготовки та автоматизованого формування статистичних даних, узагальнюючих та аналітичних показників, звітності про стан здійснення судочинства тощо; 6) об'єктивний та неупереджений розподіл судових справ за допомогою модуля автоматизованого розподілу в судах загальної юрисдикції між суддями з урахуванням спеціалізації та рівномірного навантаження для кожного судді, за принципом випадковості та в хронологічному порядку надходження судових справ; 7) об'єктивне та неупереджене визначення присяжних за допомогою модуля автоматизованого розподілу в судах загальної юрисдикції у порядку черговості, з урахуванням граничних меж їх зайнятості та в хронологічному порядку надходження судових справ...[2]. Останнє є дуже цікавим моментом, який вказує на прагнення створити алгоритм, який дозволить уникнути конфлікту інтересів, знизить корупційні ризики тощо.

Система також надає можливість забезпечувати ...8) надсилання через контакт-центр виконавчих документів, судових рішень, повідомлень, судових повісток, судових повісток-повідомлень та інших процесуальних документів або їх веб-адрес у Єдиному державному реєстрі судових рішень учасникам судового процесу та іншим особам за допомогою електронної пошти або інших засобів зв'язку (зокрема мобільного), які забезпечують фіксацію повідомлення або виклику;- 9) надання особам інформації про стан розгляду судових справ за допомогою електронного кабінету, контакт-центру та веб-порталу у випадках, встановлених законом; 10) розміщення на веб-порталі оголошень про виклик у суд осіб (відповідача, третьої

особи, свідка), зареєстроване місце проживання (перебування), місцезнаходження чи місце роботи яких невідоме; оприлюднення у випадках, встановлених законом, іншої інформації на веб-порталі, веб-сайтах Вищої ради правосуддя та Вищої кваліфікаційної комісії суддів України; 11) видачу паперових копій судових рішень та виконавчих документів на підставі наявних у АСДС даних; 12) інші можливості, створені адміністратором відповідно до взятих на себе договірних зобов'язань [2]. Таким чином, АСДС забезпечує повноцінне збереження та надає можливий (відповідно до положень чинного українського законодавства) доступ до судових інформаційних ресурсів. Тобто ми можемо говорити про те, що система робить судовий процес максимально прозорим та відкритим для ознайомлення (за можливості) кожним зацікавленим користувачем.

Для функціонування АСДС та інших підсистем адміністратор здійснює: технічний супровід та підтримку працездатності АСДС та інших підсистем у цілому, згідно з вимогами цього Положення; створення, вдосконалення та супроводження АСДС та інших підсистем; адміністрування централізованих ресурсів судів та органів системи правосуддя, надання до них доступу; забезпечення зберігання та захисту даних централізованих ресурсів, у тому числі шляхом визначення концепції захисту від несанкціонованого доступу та засобів і методів забезпечення цілісності їх баз даних; координацію і супроводження створення комплексної системи захисту інформації інформаційно-телекомунікаційної системи в органах, що використовують АСДС та інші підсистеми, як складову інформаційно-телекомунікаційної системи; затвердження єдиної політики безпеки використання АСДС, обов'язкових до застосування цими органами; підтримку сервісу обміну обліково-статистичними та реєстраційно-контрольними картками, електронними документами суду, органу системи правосуддя з ЦБД у відповідності до протоколів обміну, затверджених адміністратором; виконання цих та інших функцій, передбачених цим Положенням та взятими на себе договірними зобов'язаннями [2]. Отже, основне

обслуговування системи здійснює спеціально уповноважена особа, якою нормативно-правовий акт визначає оператора. Таким чином, **автоматизована система документообігу суду** – це інформаційно-аналітичний комплекс, котрий забезпечує реалізацію прозорого та корупційно безпечного документально-супроводження взаємовідносин між судовою системою, юридичними і фізичними особами та державою. Суспільна небезпечність посягання на нормальне функціонування АСДС є очевидною, оскільки шкода в такому випадку завдається всім суб'єктам судового процесу. Враховуючи вказане, пропонуємо зупинитись більш детально на розгляді соціальної обумовленості криміналізації посягання на роботу АСДС, розпочавши із розгляду кримінальних правопорушень у межах інформаційно-аналітичної сфери.

Відтак, більша частина суспільно небезпечних маніпуляцій у відношенні АСДС вчиняється за допомоги комп'ютерної техніки. На сьогодні такого роду кримінальні правопорушення є відносно новими, що обумовлено нещодавною популяризацією електронно-обчислювальних машин. Учені вказують, що під комп'ютерною злочинністю слід розуміти суспільно небезпечну діяльність чи бездіяльність, яка здійснюється з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки з метою спричинення збитків майновим або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадським формуванням і громадянам, а також правам особи. Розповсюдження загальних комп'ютерних знань, постійне підвищення технічних характеристик та супутнє зниження цін на обладнання, застосування комп'ютерів, мабуть, чи не в усіх професіях, розвиток машинних мов високого рівня, які легко засвоюються будь-якою зацікавленою особою, і, як наслідок, постійне зростання кількості користувачів, зумовило зростання масштабів протизаконних дій, пов'язаних з використанням ЕОМ [3, с. 223]. Ми абсолютно погоджуємось із вказаною дефініцією та зі свого боку хочемо додати, що вона достатньо влучно характеризує низку способів, за допомогою яких може бути здійснено

незаконне втручання в роботу автоматизованої системи документообігу суду.

Дійсно, збільшення кількості кримінальних справ, пов'язаних з комп'ютерними злочинами, спостерігається практично у всіх промислово розвинутих країнах. Основні причини вчинення злочинів у сфері використання ЕОМ, як і багатьох інших видів злочинності, слід шукати в економічних відносинах, у їх суперечливості. За деякими оцінками дослідників, нині економічний характер разом з корисливою мотивацією злочинної поведінки мають 4/5 криміногенних детермінант. Наявність великої кількості безробітних, у тому числі й осіб, що володіють достатніми професійними навичками, здатних здійснювати кваліфіковані злочини у сфері використання комп'ютерів, є загальною проблемою для країн колишнього СРСР, де рівень фізико-математичної освіти завжди був високим, а рівень безробіття після розпаду СРСР значно підвищився. Формування нової галузі суспільних відносин вимагає, у свою чергу, аналізу та доповнення діяльності щодо протидії вчиненню правопорушень і злочинів [3, с. 223]. Що стосується розглядуваного нами кримінального правопорушення, тут можна яскраво виділити його ядро, котре становить корисливий мотив, якого може переслідувати його суб'єкт. Також окремо може переслідуватись посткримінальна потреба уникнути певного обсягу покарання шляхом зміни та/або знищення інформації від якої залежить подальша доля справи. У цьому контексті ми можемо говорити про те, що соціальна обумовленість досліджуваного протиправного діяння є складною, розгалуженою, *історично несформованою* структурою. Ми акцентуємо увагу на відсутності вичерпного ретроспективного досвіду боротьби з незаконним втручанням у роботу АСДС, що обумовлено тим, що правопорушення є новою чинною кримінального законодавства. Отже, *першою підставою криміналізації діяння в межах соціальної обумовленості є відсутність інших ефективних засобів протидії, окрім кримінально-правової заборони*.

Варто звернути увагу на те, що нормативно-правова база з питань протидії загальним комп'ютерним кримінальним правопо-

рушенням бере свій початок ще з ХХ століття та має більш тривалу історію. Перші спеціальні закони по боротьбі з комп'ютерною злочинністю було прийнято в 1973 р. в Швеції і в 1976 р. у США на федеральному рівні. Склади злочинів у сфері інформаційних технологій (комп'ютерних злочинів) було сформовано в 1979 р. на Конференції американської асоціації адвокатів у Далласі, до яких увійшли: використання або спроба використання комп'ютера, обчислювальної системи або мереж комп'ютерів з метою отримання грошей, власності або послуг шляхом прикриття фальшивими кодами або видання себе за іншу особу; умисна несанкціонована дія, що має за мету зміну, пошкодження, знищення або викрадення комп'ютера, обчислювальної системи, комп'ютерної мережі або систем математичного забезпечення, що містяться в них, програм або даних; умисне незаконне порушення зв'язку між комп'ютерами, обчислювальними системами або комп'ютерними мережами [4, с. 60]. Згодом поступово в багатьох країнах світу затверджено законодавчі акти стосовно цієї категорії злочинів. У лютому 1986 р. Бундестагом Німеччини було прийнято Другий Закон по боротьбі з економічною злочинністю. Завдяки цьому було закладено правову базу для ефективного кримінально-правового переслідування економічних правопорушень нового типу, перш за все злочинів, об'єктом або знаряддям яких є ЕОМ. Ряд нових статей, які введено цим законом, вміщують спеціально сформульовані склади комп'ютерних злочинів. Закон було введено в дію 1 серпня 1986 р [3, с. 224]. Отже, перші нормативно-правові акти достатньо вузько розглядали такого роду суспільно небезпечні діяння, захищаючи виключно самі електронно-обчислювальні машини, залишаючи без уваги інформацію, яка в них зберігається. Такий підхід можна пояснити відсутністю загальної зацікавленості у комп'ютерах як техніки, здатної спростити документообіг.

В Італії законодавчими актами введені основні положення відносно найбільш важливих комп'ютерних злочинів: Декрет-№ 518 від 29.12.92 р. «Використання положень Європейського Економічного Співто-

вариства за № 91/250 стосовно офіційного захисту комп'ютерних програм»: Закон № 547 від 23.12.93 «Зміна та внесення нових статей стосовно комп'ютерних злочинів у Кримінальний Кодекс». Комп'ютерний злочин, згідно з кримінальним законодавством Італії, – це злочин, скоєний з використанням комп'ютерних технологій, від персонального комп'ютера до портативних телефонних пристроїв, які створені на базі мікрочіпів. Законодавство Італії забезпечує захист урядових організацій, військових об'єктів, банків, компаній, фірм від несанкціонованого доступу в комп'ютерні мережі, протиправного використання захищених банків даних, незаконного копіювання топографій напівпровідників (чіпів), які злочинці використовують для встановлення кодів кредитних і телефонних карток, банківських рахунків тощо. Щорічні втрати в Італії від комп'ютерних злочинів складають сотні мільйонів лір. Характерним для поведінки комп'ютерних злочинців є використання програмного забезпечення, яке може автоматично набирати всі алфавітно-цифрові комбінації на основі принципу генератора випадкових чисел. Завдяки цій процедурі вони здатні встановити пароль, що дозволить увійти до системи [4, с. 109]. Франція володіє повним юридичним арсеналом для боротьби з такою категорією злочинності. У 1994 р. було сформовано Бригаду поліції з компетентного персоналу, яка спеціалізується на виявленні та розслідуванні комп'ютерних злочинів при тісному співробітництві із службами безпеки та цивільними організаціями [3, с. 224]. Італійське законодавство, на наш погляд, є більш виваженим та передбачає розгалужену систему кримінально протиправних діянь, які можуть визначатись як комп'ютерні, більше того, у країні передбачено захист урядових організацій, військових об'єктів, банків, компаній, фірм від несанкціонованого доступу в комп'ютерні мережі тощо, що свідчить про захист будь-якої інформації, яка може певним чином вплинути на нормальні взаємовідносини між державою та юридичними і фізичними особами.

З 1 березня 1994 р. було введено в дію нову версію Кримінального Кодексу, який

докорінно змінив внутрішні закони про комп'ютерну злочинність. До Кримінального Кодексу були внесені статті з санкціями проти правопорушень, які пов'язані з обробкою інформації та із злочинами стосовно фальсифікації даних. Прийнятий 5 січня 1994 р. Закон «Godfrgan», який було названо на честь автора, вніс ясність та уточнив питання юриспруденції і практики стосовно несанкціонованого доступу та протидії функціонуванню систем, які приносять щорічних збитків, наприклад, страховим компаніям у розмірі 5 мільярдів франків. Єдиний закон, який передбачає покарання за комп'ютерні злочини - Кримінальний Кодекс Іспанії. Диспозиції статей Кодексу сформульовано відповідно до норм Державного Закону № 5/92 від 2 жовтня 1992 р., який регулює процеси персональної автоматизованої обробки даних і передбачає утворення органу захисту даних для контролю за виконанням цих норм. Специфічні комп'ютерні злочини вміщують правопорушення, у яких комп'ютерна система є об'єктом вчинення злочину. Прикладом цього виду злочинів може бути протизаконний доступ до комп'ютерної системи. До злочинів, які пов'язані з комп'ютерами, належать правопорушення, у яких комп'ютер виступає в ролі предмета або інструмента здійснення правопорушення. Одним з прикладів цієї категорії злочинів є крадіжка грошей з банку з використанням комп'ютера як інструмента вчинення злочину [3, с. 225]. Отже, ми можемо говорити про те, що певні ознаки комп'ютерного кримінального правопорушення у незаконному втручанні в роботу автоматизованої системи документообігу суду присутні. Тим не менше, основний акцент законодавець робить на захисті системи правосуддя, про що свідчить розміщення статті, якою передбачено кримінальну відповідальність за досліджуване діяння у відповідному розділі XVIII «Кримінальні правопорушення проти правосуддя». Таким чином, *другою підставою криміналізації діяння в межах соціальної обумовленості є необхідність кримінально-правової гарантії дотримання принципу верховенства права та належного здійснення правосуддя*, що гарантується ст. 6 Конвенції про захист прав

людини і основоположних свобод, якою передбачено право на справедливий і публічний розгляд справи упродовж розумного строку незалежним і безстороннім судом, встановленим законом, при визначенні цивільних прав і обов'язків особи чи при розгляді будь-якого кримінального обвинувачення, що пред'являється особі; окремого захисту потребують і права та законні інтереси суддів та інших осіб, причетних до судового процесу [5].

Не можна оминати увагою той факт, що ще *однією з підстав криміналізації діяння є рівень суспільної небезпеки*. Досліджуване нами кримінальне правопорушення, передбачене ст. 376-1 КК України, є достатньо розповсюдженим та протягом останніх років залишається актуальним, про що свідчать статистичні дані, викладені на сайті Генеральної прокуратури України. Так, у 2013 році було вчинено 1 кримінальне правопорушення, передбачене ст. 376-1 КК України, у 2014 – 8, у 2015 – 18, у 2016 – 37, у 2017 – 60, у 2018 – 83, у 2019 – 34, у 2020 – 30, станом на березень 2021 року досліджуване нами протиправне діяння було вчинено 14 разів [6]. Вказані цифри свідчать про те, що законодавцем було прийнято дуже своєчасне та правильне рішення внести у 2009 році такого роду суспільно небезпечне діяння до вітчизняного кримінального законодавства. Проте, нестабільні кількісно-якісні показники свідчать про не зовсім ефективний кримінально-правовий вплив та потребу у перегляді санкції ст. 376-1 КК України.

Цікавим аспектом є те, що наразі наша країна регулярно проводить реформи майже у всіх сферах, не є виключенням і реформування судової системи. На сьогодні ми не можемо говорити про повну досконалість останньої. Український законодавець, на жаль, ще не в повній мірі готовий перейняти максимальну кількість позитивних напрацювань міжнародної та європейської спільноти та повністю позбавити судову систему суб'єктивізму та рудиментарних поглядів на відповідальність. Однак, на нашу думку, криміналізація незаконного втручання в автоматизовану систему документообігу суду дозволило одним кроком вирішити декілька проблем: дещо удосконалити судо-

ву систему в світлі її реформування та дещо наблизитись до вимог міжнародної та європейської правової спільноти.

### Висновки

Таким чином, враховуючи все вищевказане, підсумуємо, що автоматизована система документообігу суду наразі є єдиною інформаційно-аналітичною базою, яка здатна прискорити, полегшити та забезпечити обмін та отримання спеціальними (та в окремих випадках – загальними) суб'єктами необхідних даних у межах тих чи інших проваджень. Поява будь-якого феномену рано чи пізно призводить до виникнення нових форм кримінально протиправної діяльності, у зв'язку із чим у 2009 році виникла гостра потреба кримінально-правового захисту АСДС. Підставами соціальної обумовленості криміналізації такого роду правопорушення стали наступні: 1) відсутність інших ефективних засобів протидії, окрім кримінально-правової заборони; 2) необхідність кримінально-правової гарантії дотримання принципу верховенства права та належного здійснення правосуддя; 3) рівень суспільної небезпеки; 4) удосконалення судової системи в світлі її реформування; 5) приведення законодавства у відповідність вимогам міжнародної та європейської правової спільноти.

### Література

1. Наумов А.В. Российское уголовное право. Общая часть : курс лекций. 2-е изд., перераб. и доп. Москва : БЕК, 1999. 590 с.
2. Положення про автоматизовану систему документообігу суду, затвердженого Рішенням Ради суддів України від 26.11.2010 № 30. URL: <https://zakon.rada.gov.ua/rada/show/vr030414-10#Text>
3. Школьний В. В. Деякі причини виникнення і розвитку злочинності у сфері використання ЕОМ / В. В. Школьний // Право і суспільство. - 2012. - № 2. - С. 222-227.
4. Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність: Навч. посібник. – К., 2002. 240 с.
5. Конвенція про захист прав людини і основоположних свобод, ратифікована ратифіковано Законом № 475/97-ВР від

17.07.97. URL: [https://zakon.rada.gov.ua/laws/show/995\\_004#Text](https://zakon.rada.gov.ua/laws/show/995_004#Text)

6. Генеральна прокуратура України. URL: [http://www.gp.gov.ua/ua/stst2011.html?dir\\_id=112173&libid=100820&c=edit&c=fo](http://www.gp.gov.ua/ua/stst2011.html?dir_id=112173&libid=100820&c=edit&c=fo)

*Shcherbina Artem, graduate student of the Department of Criminal Law and Criminology, Faculty № 1 (Donetsk State University of Internal Affairs)*

**THE CONCEPT OF AUTOMATED COURT DOCUMENTATION SYSTEM AND SOCIAL-LEGAL NEED FOR CRIMINAL AND LEGAL PROTECTION OF ITS NORMAL FUNCTIONING**

In the article the author considers the concept of automated document management system of the court and explores the social and legal necessity of criminal law protection of its normal functioning. It is pointed out that the study of the social conditionality of criminally illegal phenomena allows to criminalize or decriminalize acts in a timely manner, while avoiding the emergence of “dead” and “dormant” norms in criminal law. It is social conditionality and historicism that determine continuity in law. Today in Ukraine, most government agencies and institutions are already switching to electronic documentation and business correspondence. This approach allows to maintain maximum transparency between the participants and in some way contributes to the process of combating corruption. Creating a single analytical and information base

is a fairly effective way to ensure the security of legal entities and individuals, by storing information that can be used as evidence against the removal and entry of false information. It is noted that currently our country regularly carries out reforms in almost all areas, and the reform of the judiciary is no exception. To date, we can not talk about the complete perfection of the latter. The Ukrainian legislator is not yet fully ready to adopt the maximum number of positive developments of the international and European community and completely deprive the judiciary of subjectivism and rudimentary views on responsibility. However, the criminalization of illegal interference in the automated court document management system allowed to solve several problems in one step: to improve the judicial system in the light of its reform and to approach the requirements of the international and European legal community. It is concluded that the automated document management system of the court is currently the only information and analytical database that can speed up, facilitate and secure the exchange and receipt by special (and in some cases - general) subjects of the necessary data in certain proceedings. The emergence of any new phenomenon sooner or later leads to the emergence of new forms of criminal activity, due to which in 2009 there was an urgent need for such criminal protection.

**Key words:** *automated court document management system, criminalization, criminal legislation, criminal offense, social conditionality, retrospective analysis, computer criminal offense.*