УДК 346.93
DOI https://doi.org/10.32782/pdu.2023.2.38

А. Ю. Ковальчук
д.ю.н., професор, начальник відділу, Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України
ORCID: https://orcid.org/0000-0003-4807-2436

Б. В. Чернявська
доктор філософії у праві, доцент кафедри теорії та історії держави і права юридичного факультету Національної академії управління, Київ, Україна;
Запрошений науковий співробітник Vrije Universiteit Amsterdam, Нідерланди
ORCID: https://orcid.org/0000-0001-8263-7483

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ ДАНИХ У ГОСПОДАРСЬКОМУ СУДОЧИНСТВІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПРОБЛЕМИ

У статті порушуються питання щодо розробки додаткових заходів щодо правового та організаційного захисту Єдиної судової інформаційно-телекомунікаційної системи. Інформаційна сфера стає все більш важливою для забезпечення національної безпеки і безпеки суспільства в цілому, а також для захисту і відновлення порушених прав і свобод людини. Широке використання інформаційних технологій у всіх сферах життя надає нові можливості, але також відкриває двері для потенційних загроз та кібератак. Особливо судові органи на сьогодні повинні приділити особливу увагу надійному захисту інформації в сучасних умовах.

Захист і відновлення прав і свобод осіб, які постраждали від збройної агресії, має велике значення для відновлення людського потенціалу в Україні. Тому автори акцентують необхідність заходів щодо захисту інформації, яка зберігається в Єдиній судовій інформаційно-телекомунікаційній системі. Важливим є розробка та впровадження ефективних заходів кібербезпеки, а також надання навчання та інструкцій з питань кібербезпеки для підвищення обізнаності персоналу стосовно потенційних загроз та запобіжних заходів. Це включає встановлення політик доступу до інформації, обмеження привілеїв, та надання доступу лише необхідному персоналу. Використання спеціалізованого програмного забезпечення для моніторингу мережі та системи для виявлення потенційних загроз та незвичайної активності є також критичним. Робиться висновок про необхідність подальшого вдосконалення системи правового та організаційного захисту Єдиної судової інформаційно-телекомунікаційної системи.

Ключові слова: *електронні докази, електронний документ, інформаційні технології, права і свободи людини, Єдина судова інформаційно-телекомунікаційна система, судочинство.*

Актуальність теми. Повномасштабне вторгнення РФ на територію України, що триває із 24 лютого 2022 року, супроводжується численними актами агресії у кіберпросторі. Відповідно до оприлюднених Державною службою спеціального зв'язку та захисту інформації України даних, від 15 лютого 2022 року Україна зазнала понад 3 000 DDoS-атак; постійно розповсюджується шкідливе програмне забезпечення, здійснюються фішингові розсилки та інші прояви війни у кіберпросторі. Особливо, актуалізується захист Єдиної судової інформаційно-телекомунікаційної системи (далі – ЄСІТС) яка впроваджується у систему сучасного судочинства. Така проблема стає гострішою у зв'язку російською агресією й необхідністю відновлення й захисту прав і свобод, осіб, як стали жертвами злочинних дій. Слід розуміти у таких справах особливість й особливу вразливість електронних доказів й системи їх збереження й захисту.

Застосування інформаційно-телекомунікаційних технологій у судочинстві та захисті прав і свобод людини має великий потенціал для підвищення ефективності, доступності та прозорості судової системи. Разом з тим, лише за 2021-2023 роки були здійснені десятки кібератак на суддівську систему. Зокрема, у 2022 році хакерами була заблокована робота Єдиного державного реєстру судових рішень, електронного суду, вебпорталу «Судова влада України», поштового сервісу та ін. Значний проміжок часу після цієї атаки, спостерігалися проблеми з веб-програмою «Бронювання систем відеоконференцзв'язку» з іншими судами, що позбавляє можливості проведення судових засідань у такому режимі [1]. Були також і складнощі з підсистемою «Електронний суд». Нажаль, слід констатувати, що відповідно до офіційної статистики Офісу Генерального прокурора України, лише за останні 8 років кількість виявлених кіберзлочинів збільшилась майже в 7,5 разів (не враховуючи «класичні» правопорушення з використанням комп'ютерної техніки, а також зважаючи на рівень латентності кіберзлочинності). При цьому діяльність кіберзлочинців завдає значних збитків у тому числі судейської системі. За останні рік було здійснено значна кількість хакерських атак на системи електронної пошти судової системи. Фахівці ДП «Інформаційні судові системи» разом з ДП «Центр судових сервісів» здійснюють усі необхідні заходи, разом з тим це не завжди відбувається успішно. Нажаль, можна констатувати, що привабливість вчинення кіберзлочинів лише зростає рік у рік. Глобальні збитки від кіберзлочинності і витрати на захист від кіберзлочинів збільшилися за два роки більш ніж на 50% і в 2020 склали $ 1,1 трлн. або більше 1% світового ВВП [2]. У 2018 році збитки від діяльності кіберзлочинців становили $ 600 млрд. Такі економічні наслідки діяльності хакерів у мережі свідчать про постійне удосконалення методів вчинення кіберзлочинів з метою отримання надприбутків і уникнення відповідальності. Згідно з статистикою, з кожним днем в Україні збільшується кількість кібератак. У звіті Google про зміни ландшафту кіберзагроз внаслідок російської війни проти України йдеться про те, що минулого року ворог посилив кібератаки на українців на 250% порівняно з 2020 роком [3]. Виходячи з вищевизначеного вважаємо за необхідне переглянути організаційні й правові заходи захисту Єдиної судової інформаційно-телекомунікаційної системи.

Ступінь наукової розробки. Проблема, яка підіймається складається з двох частин, які розглядалися різними вченими окремо. Так дослідженням різних аспектів здійснення господарського судочинства займались відомі вчені Н. Блажівська, Білецька Л., Демчишин І., Руда Т., Казачук І. та ін. Окремі аспекти аналізу кіберзлочинності вивчали О.В. Амелін, О.М. Бандурка, В.В. Василевич, Б.М. Головкін, В.В. Голіна, М.В. Гуцалюк, О.М. Джужа, А. П. Закалюк, О.Г Кулик, О.М. Литвинов, В.В. Марков, Д.М. Прокоф'єва-Янчиленко, О.В. Таран, В.І. Трапезніков, В.О. Туляков та ін. Водночас, проблемам аналізу кібератак на судову систему не розглядалися, хоча проблема вже неоднарозово перешкоджала здійсненню правосуддя й порушенню прав і свобод людини.

Мета статті переглянути сучасні заходи захисту єдиної судової інформаційно-телекомунікаційної системи, з метою визначення потенційних загроз та вразливостей системи й можливості їх захисту.

Викладення основного матеріалу. Рішенням Вищої ради правосуддя № 1845/0/15-21 від 17.08.2021 року вводиться в дію Положення «Про порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи» [4], яке починає діяти відповідно до Закону України «Про судоустрій і статус суддів», процесуального законодавства України. ЄСІТС забезпечує широку спектр функціонування судової системи: ведення електронного діловодства, в тому числі рух електронних документів у межах відповідних органів та установ та між ними, реєстрацію вхідних і вихідних документів та етапів їх руху; централізоване захищене зберігання судових справ, процесуальних, інших документів та інформації в єдиній базі даних; захищене зберігання, автоматизовану аналітичну і статистичну

обробку інформації; збереження судових справ та інших документів в електронному архіві; обмін документами та інформацією (надсилання та отримання документів та інформації, спільна робота з документами) в електронній формі між судами, іншими органами та установами в системі правосуддя, учасниками судового процесу, а також проведення відеоконференції в режимі реального часу; автоматизацію роботи судів, органів та установ у системі правосуддя, в тому числі автоматизоване формування в режимі реального часу основних аналітичних показників діяльності; автоматизацію процесів ведення бухгалтерського, статистичного, кадрового обліку, формування та консолідації фінансової, статистичної та управлінської звітності; автоматизацію процесів планування та виконання бюджетів; формування і ведення суддівського досьє (досьє кандидата на посаду судді) в електронній формі; віддалений доступ користувачів ЄСІТС до будь-якої інформації, що в ній зберігається, в електронній формі відповідно до диференційованих прав доступу; визначення судді (судді-доповідача) для розгляду конкретної справи у порядку, встановленому процесуальним законом; визначення присяжних для судового розгляду із числа осіб, які внесені до списку присяжних; відбір кандидатури арбітражного керуючого у справах про банкрутство; розподіл справ у Вищій раді правосуддя, Вищій кваліфікаційній комісії суддів України, їх органах; аудіо- та відеозапис судових засідань, засідань Вищої кваліфікаційної комісії суддів України, Вищої ради правосуддя, її органів, транслювання їх в інтернеті в порядку, визначеному законом; ведення Єдиного державного реєстру судових рішень; ведення Єдиного державного реєстру виконавчих документів; функціонування вебпорталу судової влади України, вебсайтів Вищої ради правосуддя та Вищої кваліфікаційної комісії суддів України; функціонування єдиного контакт-центру для управління запитами, іншими зверненнями; можливість автоматизованої взаємодії ЄСІТС з іншими автоматизованими, інформаційними, інформаційно-телекомунікаційними системами органів та установ у системі правосуддя, органів правопорядку, Національної асоціації адвокатів України, Міністерства юстиції України та підпорядкованих йому органів та установ, інших органів та установ; можливість учасникам справи брати участь у судовому засіданні в режимі відеоконференції; інші функції, передбачені цим Положенням. Таке широке коло застосування ЄСІТС вимагає відповідних заходів захисту: технічного, правового та організаційного характеру.

Проблема, яка на сьогоднішній день актуалізується полягає у недостатності правових й організаційних заходів захисту ЄСІТС, а особливо інформації, персональних даних та електронних доказів, які були занесені до систем. У зв'язку з військовою агресією Російської Федерації проти України, а також відповідно до пункту 20 частини першої статті 106 Конституції України, Закону України «Про правовий режим воєнного стану» Указом Президента України від 24.02.2022 №64/2022 в Україні введено воєнний стан з 24.02.2022 у зв'язку з цим, 24.02.2022 року Державне підприємство «Національні інформаційні системи» на своєму офіційному веб-сайті повідомило про виникнення обставин непереборної сили (форс-мажорних) та тимчасово призупинило роботу Єдиних та Державних реєстрів Міністерства юстиції України (Реєстрів). Таке рішення прийнято з метою недопущення будь-яких несанкціонованих дій з інформацією Реєстрів зі сторони ворога та для забезпечення збереження та захисту відомостей, що в них містяться, а також у зв'язку із численними кібератаками. І лише починаючи з квітня 2022 року Державне підприємство «Національні інформаційні системи» частково почало відновлювати доступ до реєстрів виключно для уповноважених працівників державних органів. 16 березня 2023 року на офіційному веб-сайті Судової влади України повідомлено про те, що наразі триває кібератака рф на системи електронної пошти судової системи [5].

Неможливість здійснення господарського правосуддя судді відображають в судових рішеннях з посиланням на відповідні кібератаки. До прикладу, в ухвалі Господарського суду Кіровоградської області

від 16.03.2023 у справі №912/238/23 суд зазначив: «16.03.2023 близько 10:30 год із оголошення на офіційній сторінці ДП «ІСС» в соцмережі «Facebook» було з'ясовано про кібератаку на систему електронної пошти судової системи. У зв'язку із цією інформацією та з метою убезпечення АСДС від кібератаки, керівництвом суду було прийнято рішення про тимчасове відключення мережі суду від Інтернетзв'язку (Укртелеком) [6]. З огляду на вказане, в Господарському суді Кіровоградської області станом на 16.03.2023 з 10:30 год відсутній зв'язок з мережею Інтернет, не працює офіційна електронна пошта суду, захищена система ВКЗ, підсистема «Електронний суд», що в свою чергу призвело до збоїв у роботі суду, зокрема проведення судових засідань в режимі ВКЗ, доступу до Державних реєстрів, підписання електронним підписом електронних примірників судових рішень та направлення їх до ЄДРСР тощо» [7].

16.03.2023 Верховний Суд також не міг здійснювати розгляд справ, що відображено в ухвалі від 16.03.2023 у справі №906/90/21. У вказаній ухвалі Верховний суд зазначив «Судове засідання призначене на 16.03.2023 не відбулося, оскільки не працювала підсистема відеоконференцзв'язку, у якій стався технічний збій через здійснення кібератаки на ресурс Державного підприємства «Інформаційні судові системи» та Державного підприємства «Центр судових сервісів», про що складено Верховним Судом Акт від 16.03.2023 № 38/2023» [7].

Господарський суд Сумської області 16.03.2023 у зв'язку з кібератакою теж не зміг здійснити розгляд судових справ (ухвала від 16.03.2023 у справі №920/957/22) [8]. На даний час, згідно інформації розміщеної на сайті офіційному веб-сайті Єдиного державного реєстру судових рішень, доступ до нього здійснюється в обмеженому режимі. Також, у вказаному повідомленні зазначено, що для запобігання загрозам життю і здоров'ю суддів та учасників судового процесу, а також у разі виявлення ознак кіберзагрози, доступ до Реєстру або окремих рішень у ньому може бути обмежено [9].

Такі прикрі випадки неможливості здійснення правосуддя негативно впливають на стан забезпечення прав і свобод людини. Для їх усунення слід впроваджувати альтернативні можливості здійснення правосуддя. Поряд з системою додаткового захисту ЄСТІС.

Отже, слід констатувати, що судова інформаційно-телекомунікаційна система має різні вразливості, які можуть потенційно загрожувати безпеці даних та функціонуванню системи. Судові системи можуть стати об'єктом кібератак, таких як хакерські атаки, фішинг, віруси, зловмисні програми тощо. Це може призвести до несанкціонованого доступу до судових даних, втрати або пошкодження інформації, порушення конфіденційності та цілісності даних, а також перешкоджати нормальному функціонуванню системи. Використання програмного забезпечення в судових системах може створювати вразливості, які можуть бути використані зловмисниками, окрім того у системі забезпечення безпеки постійно втрачається організаційна складова – підбір, підготовка персоналу щодо кібербезпеки. Зловмисники можуть використовувати соціальну інженерію, щоб отримати несанкціонований доступ до судової інформації. Це може включати фальшиві електронні листи, підступні запити на інформацію або маніпулювання персоналом, щоб отримати доступ до системи. Особливо небезпечним визначаються проведення складних хакерських атак, коли залучаються особи, що мають доступ до судейської системи. Недостатня проінформованість персоналу про кіберзагрози може призвести до вразливостейсамої системи. Наприклад, використання слабких паролів, недостатня навички уникнення шахрайства в Інтернеті, недостатня увага до деталей можуть сприяти атакам на систему. Серед основних вразливостей системи ми хотіли б виділити систему електронного архівування. ЄСІТС дозволяють створювати електронні архіви правових документів, судових рішень, законів та інших нормативних актів. Особливого занепокоєння викликає усвідомлене псування й некоректне внесення інформації [10] співробітниками судової влади, що мають доступ до ЄСІТС.

Приписами статті 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах» встановлено, що

відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним. Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган. визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом; організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації; здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом; здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, електронних телекомунікаційних та інформаційно-комунікаційних системах та дає рекомендації з питань запобігання такій загрозі [11]. Розпорядником інформації, який відповідає за захист інформаційних систем судової системи є Державна судова адміністрація України. Разом з тим, до сфери управління Державної судовою адміністрацією України належить Державне підприємство «Інформаційні судові системи». Вказане підприємство створено з метою: надання послуг з технічного, технологічного забезпечення створення та супроводження програмного забезпечення ведення автоматизованих систем (електронних баз даних), у тому числі, державних реєстрів, що створюються відповідно до законів України, нормативно-правових актів Кабінету Міністрів України, наказів Уповноваженого органу управління; організації доступу фізичним та юридичним особам до автоматизованих систем державних реєстрів; організації збереження та захисту даних, що містяться в автоматизованих системах державних реєстрів; надання послуг з інформаційно-технічного забезпечення судів; задоволення потреб органів досудового розслідування, судових органів, інших державних органів, а також юридичних та фізичних осіб у забезпеченні їх належною, кваліфікованою і об'єктивною експертизою, орієнтованою на максимальне використання досягнень науки та техніки; підвищення ефективності здійснюваної діяльності, взаємовигідного співробітництва, забезпечення економічних, суспільно-корисних потреб та інтересів юридичних і фізичних осіб; забезпечення діяльності органів судової влади, у тому числі в умовах особливого періоду [12]. На виконання постанови Уряду від 04.04.2023 №299, у межах реалізації Стратегії кібербезпеки України, Адміністрацією Держспецзв'язку розроблено та затверджено Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Відповідний наказ від 03.07.2023 №570 розміщений на сайті Служби. Вказані рекомендації визначають: необхідний перелік заходів із кіберзахисту, яких можуть вживати суб'єкти забезпечення кібербезпеки послідовно за етапами реагування на кіберінциденти / кібератаки; мету та цілі виконання заходів; механізм застосування критеріїв, за якими визначається категорія (рівень) критичності кіберінциденту / кібератаки; принципи пріоритезації кіберінцидентів / кібератак; типовий перелік заходів із реагування на кіберінциденти / кібератаки для одночасного відстеження заходів до їх завершення тощо [13]. Впровадження цих методичних рекомендацій покладено на начальника Відділ інформаційно-технічного забезпечення, захисту інформації та баз даних суду, а саме: забезпечення кібербезпеки та захисту інформації в суді, кіберзахисту локального мережевого

середовища суду та організація роботи по захисту інформації, проектування, розроблення, супроводження та модернізації комплексної системи захисту інформації в суді; забезпечення контролю за розробленням проектної та технічної документації комплексної системи захисту інформації, організації робіт, пов'язаної із забезпеченням захисту персональних даних у базах даних від незаконної обробки та несанкціонованого доступу. Також, зазвичай, на начальника вказаного відділу покладається обов'язок з забезпечення формування довідкових матеріалів, презентацій, контекстної довідки по користуванню програмним забезпеченням та інформаційними системами, які впроваджені у суді. Тобто, вказана особа доводить до відома працівників суду, зокрема, і інформацію яких правил кібергігієни варто дотримуватися на робочому місці та як держслужбовцям уникнути участі в інформаційних маніпуляціях. Однак, вказана інформація містить більше інформативно-довідковий характер. На нашу думку, інформаційна компанія повинна носити системний характер й мати форму постійного процесу навчання, тренінгів, круглих столів та ін. На жаль, поза увагою законотворців, й інших владних структур залишається аспект забезпечення, кібергігієни та застосування заходів кіберзахисту працівниками суду. Саме поняття «забезпечення» визначає цілісний процес формування необхідних ресурсів, умов і заходів для досягнення певної мети або забезпечення правильної функціональності системи, процесу чи організації. В контексті безпеки, «забезпечення» означає застосування набору заходів та політик для запобігання загрозам, збереження цілісності та конфіденційності інформації, а також забезпечення безпеки фізичних та кібернетичних активів. Забезпечення включає в себе розробку, впровадження та забезпечення ефективності заходів безпеки, контроль доступу, моніторинг, аудит, навчання персоналу та інші дії, спрямовані на забезпечення безпеки та досягнення поставлених цілей. Усі складові цього процесу забезпечують люди, які піддаються різним формам маніпуляції, дезінформації,омані тощо. Окрім того, вчинення дій що призвели до витоку інформації можливо навіть поза розумінням жертви. Тому приділяти увагу свідомості, навченості основам кібергігієни співробітників суду є вкрай важливим й необхідним.

Висновки. Всі ці застосування ІКТ у судочинстві та захисті прав і свобод людини спрямовані на покращення доступності, ефективності та прозорості судової системи, забезпечення швидкого доступу до інформації, зменшення бюрократичних процедур і покращення якості правосуддя. Однак, важливо забезпечувати адекватний рівень захисту даних, приватності і кібербезпеки для забезпечення довіри до цих систем та захисту прав людини в онлайн-середовищі. Для захисту судових інформаційно-телекомунікаційних систем важливо приділяти увагу кібербезпеці, використовувати захисне програмне забезпечення, проводити регулярні аудити безпеки, навчати персоналу про правила кібербезпеки та дотримуватися суворих стандартів щодо обробки, збереження і передачі чутливих даних.

Список використаної літератури:

1. 5AAC: Робота судової системи після хакерської атаки. (2022) . URL: https://yur-gazeta.com/golovna/5aas-robota-sudovoyi-sistemi-pislya-hakerskoyi-ataki.html.
2. Кіберзлочини у 2020 році завдали збитків на трильйон доларів. (2020). URL:https://www.dw.com/uk/kiberzlochyny-u-2020-rotsi-zavdaly-svitu-zbytkiv-na-trylion-dolariv-doslidzhennia/a-55857766.
3. How the Ukraine Conflict Transformed the Cyber Threat Landscape. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf.
4. Про затвердження Положення про порядок функціонування окремих підсистем Єдиної судової інформаційно-телекомунікаційної системи. № 1845/0/15-21 від 17.08.2021. https://zakon.rada.gov.ua/rada/show/v1845910-21#Text.
5. ДП «Інформаційні судові системи» повідомляють про кібератаку рф на системи електронної пошти судової системи. URL: https://court.gov.ua/press/news/1396099/.
6. Ухвала Господарського суду Кіровоградської області від 16 березня 2023 року

у справі №912/238/23. URL: https://reyestr.court.gov.ua/Review/109588557.
7. Ухвала Верховного Суду у справі №906/908/21. URL: https://reyestr.court.gov.ua/Review/109645641.
8. Ухвала Господарського суду Сумської області 16.03.2023 у справі №920/957/22. URL: https://reyestr.court.gov.ua/Review/109589029.
9. Оксана Блажівська: недофінансування та колаборація – нові виклики судовій системі. URL: https://pl.arbitr.gov.ua/tu25/pres-centr/news/1322737/
10. Про захист інформації в інформаційно-комунікаційних системах. Закон України № 2801-IX від 1 грудня 2022 року. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
11. Витяг із Статуту Державного підприємства «Інформаційні судові системи» (затвердженого наказом Державної судової адміністрації України від 26 листопада 2019 року № 1142). URL: https://ics.gov.ua/ics/about/acts/.
12. Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. URL: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori.

Kovalchuk A., Cherniavska B. Ensuring the security of electronic data in economic litigation: legal and organizational problems

The article addresses issues related to the development of additional measures for the legal and organizational protection of the Unified Court Information and Communication System. The information sphere is becoming increasingly important for ensuring national security and the security of society as a whole, as well as for protecting and restoring violated human rights and freedoms. The widespread use of information technologies in all areas of life provides new opportunities but also opens the door to potential threats and cyberattacks. Particularly, judicial authorities must pay special attention to ensuring reliable information protection in modern conditions.

The protection and restoration of the rights and freedoms of individuals affected by armed aggression are of great significance for the recovery of human potential in Ukraine. Therefore, the authors emphasize the necessity of measures to protect the information stored in the Unified Court Information and Communication System. It is crucial to develop and implement effective cybersecurity measures, as well as to provide training and instructions on cybersecurity to increase the awareness of personnel regarding potential threats and preventive measures. This includes establishing access policies, limiting privileges, and granting access only to necessary personnel. The use of specialized software tools for monitoring networks and systems to detect potential threats and unusual activities is also essential. The conclusion is drawn about the need for further improvement of the legal and organizational protection system of the Unified Court Information and Communication System.

Key words: *electronic evidence, electronic document, information technologies, human rights and freedoms, Unified Court Information and Communication System, judicial proceedings.*