НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ІТ-ПРАВО ПІД ЧАС ГІБРИДНОЇ ВІЙНИ: ВІД ПОШУКУ ПАРАДИГМИ ДО ПРАГМАТИЧНИХ РІШЕНЬ

Колективна монографія

За редакцією
Є. Харитонова, О. Харитонової, І. Давидової

Одеса
Фенікс
2025

УДК 340:004:327:355
І-87

Рекомендовано рішенням вченої ради
Національного університету «Одеська юридична академія»
(протокол № 9 від 30 червня 2025 р.)

Рецензенти:

Майданик Р. А. – академік НАПрН України, доктор юридичних наук, професор, професор кафедри цивільного процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка;

Соколов А. В. – доктор технічних наук, професор, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»;

Маковій В. П. – кандидат юридичних наук, професор, завідувач кафедри цивільно-правових дисциплін Одеського державного університету внутрішніх справ.

І-87 **ІТ-право під час гібридної війни: від пошуку парадигми до прагматичних рішень** : кол. монографія / за заг. ред. проф.: Є. Харитонова, О. Харитонової, І. Давидової. – Одеса : Фенікс, 2025. – 588 с.
ISBN 978-617-8430-70-2

Монографія є продовженням циклу праць колективу кафедри цивільного права Національного університету «Одеська юридична академія», присвячених результатам досліджень цивілістичних шкіл університету від часу їхнього формування до гібридної війни, що триває нині. У третьому томі аналізуються в контексті гібридної війни: проблеми визначення концепту «ІТ-право», особливості правового регулювання відносин, що виникають у зв'язку з використанням інформаційних технологій, особливості механізму цивільно-правового регулювання у сфері ІТ, чинник симулякру, значення та роль інформаційного середовища як стратегічного ресурсу, правові рамки для цифрових активів і перспективи цифрової власності, ІТ-правочини, порушення прав інтелектуальної власності в Інтернет, протидія кіберзагрозам у гібридній кібервійні, загрози вербування неповнолітніх через соцмережі та месенджери та юридичні заходи запобігання таким загрозам, правове регулювання стартапів, е-кредитування, цивільно-правова відповідальність за шкоду, завдану кібератаками, забезпечення інформаційної безпеки електронного судочинства в умовах гібридної війни в Україні та ін.

Авторський колектив концентрував увагу на обґрунтуванні необхідності комплексного вирішення практичних питань впорядкування інформаційно-технологічні відносини в умовах гібридної російсько-української війни. Автори прагнули розкрити особливості правового регулювання цих відносин і запропонувати власне бачення шляхів вирішення проблем, що виникають у цій сфері. Усвідомлюючи спірність низки висновків і пропозицій, автори розраховують на продовження плідних дискусій з проблем правового регулювання інформаційних технологій, зокрема в умовах гібридної війни.

Монографія може бути цікавою науковцям, практикуючим юристам, викладачам, аспірантам, здобувачам вищої освіти, а також широкому загалу небайдужих українців, які цікавляться проблемами правового регулювання у сфері ІТ, зокрема під час гібридної війни.

УДК 340:004:327:355

ISBN 978-617-8430-70-2

ЗМІСТ

Авторський колектив

Харитонов Євген (ORCID ID: 0000-0001-5521-0839), доктор юридичних наук, професор, член-кореспондент НАПрН України, зав. кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з О. Харитоновою, І. Давидовою); розділ 2 (у співав. з О. Харитоновою); розділ 3 (у співав. з О. Харитоновою); розділ 4 (у співав. з О. Харитоновою); розділ 5 (у співав. з О. Харитоновою); розділ 11 (у співав. з О. Харитоновою); розділ 14 (у співав. з О. Харитоновою);

Харитонова Олена (ORCID ID: 0000-0002-9681-9605), докторка юридичних наук, професорка, членкиня-кореспондент НАПрН України, зав. кафедри права інтелектуальної власності і патентної юстиції НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, І. Давидовою); розділ 2 (у співав. з Є. Харитоновим); розділ 3 (у співав. з Є. Харитоновим); розділ 4 (у співав. з Є. Харитоновим); розділ 5 (у співав. з Є. Харитоновим); розділ 11 (у співав. з Є. Харитоновим); розділ 14 (у співав. з Є. Харитоновим);

Давидова Ірина (ORCID ID: 0000-0001-5622-671X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, О. Харитоновою); розділ 9;

Некіт Катерина (ORCID ID: 0000-0002-3540-350X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 7;

Сафончик Оксана (ORCID ID: 0000-0001-6781-8219), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 19;

Бааджи Наталія (ORCID ID: 0000-0002-9889-4879), кандидатка юридичних наук, доцента, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 10;

Берназ-Лукавецька Олена (ORCID ID: 0000-0002-2133-1672), кандидатка юридичних наук, доцента, доцентка кафедри цивільного права НУ «ОЮА»: розділ 17;

Галупова Лариса (ORCID ID: 0000-0001-6263-2773), кандидатка юридичних наук, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з А. Кирилюк);

Дрогозюк Крістіна (ORCID ID: 0000-0001-9254-9575), кандидатка юридичних наук, доцента, доцентка кафедри цивільного, нотаріального та виконавчого процесу НУ «ОЮА»: розділ 20;

Калітенко Оксана (ORCID ID: 0000-0003-1001-3561)**,** кандидатка юридичних наук, доцентка, професорка кафедри цивільного права НУ «ОЮА»: розділ 6;

Кирилюк Алла (ORCID ID: 0000-0002-3051-6599), кандидатка юридичних наук, доцентка, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з Л. Галуповою);

Омельчук Олександр (ORCID ID: 0000-0002-0082-3619), кандидат юридичних наук, доцент, доцент кафедри цивільного права НУ «ОЮА»: розділ 12;

Ткалич Максим (ORCID ID: 0000-0003-4224-7231), кандидат юридичних наук, доцент, доцент кафедри цивільного права Запорізького національного університету: розділ 21 (у співав. з Ю. Толмачевською);

Токарева Віра (ORCID ID: 0000-0002-8409-1477), кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права НУ «ОЮА»: розділ 13;

Толмачевська Юлія (ORCID ID: 0000-0002-7964-8875), докторка філософії (081 право): розділ 21 (у співав. з О. Ткаличем);

Фасій Богдан (ORCID ID: 0000-0002-8715-930X), кандидат юридичних наук, доцент, декан факультету судового та міжнародного права НУ «ОЮА»: розділ 18;

Розумейко Дмитро (ORCID ID: 0000-0001-8206-1031)**,** аспірант кафедри цивільного права НУ «ОЮА»: розділ 16;

Рябченко Вікторія (ORCID ID: 0009-0007-1542-6492)**,** аспірантка кафедри цивільного права НУ «ОЮА»: розділ 15.

Розділ 20

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЕЛЕКТРОННОГО СУДОЧИНСТВА В УМОВАХ ГІБРИДНОЇ ВІЙНИ В УКРАЇНІ

DOI

Крістіна Дрогозюк
кандидатка юридичних наук, доцентка

Вступ

Створення єдиного інформаційного простору, в межах якого відбувається накопичення, зберігання, дослідження та обмін даними, обумовило необхідність забезпечення інформаційної безпеки в усіх сферах суспільної та державної діяльності, зокрема, в сфері здійснення правосуддя.

В умовах сучасної трансформації суспільства, пов'язаної з масовим використанням інформаційних технологій, держава може розраховувати на лідерство у військовій, політичній, економічній та інших сферах, мати стратегічну і тактичну перевагу, гнучкіше регулювати економічні витрати на розвиток озброєнь і військової техніки, лише за умови наявності переваги в засобах забезпечення інформаційної боротьби[1].

Відповідно до ч.2 ст. 26 Закону України «Про правовий режим воєнного стану», в умовах воєнного стану скорочення або прискорення будь-якої форми судочинства заборонено. Попри відповідні положення законодавства, судова гілка влади все ж зазнала значного впливу війни та її наслідків, що внесло певні зміни у процес здійснення судочинства[2].

---

[1] Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. Ефективна економіка. 2015. № 4. URL: http:// http://www.economy.nayka.com. ua/ ?op=1&z=5514.

[2] Притуляк В. М. Підсистема електронний суд: особливості її функціонування в умовах воєнного стану. *Цивільне судочинство та виконавче провадження в умовах воєнного стану*: матеріали всеукр. наук.-практ. конф. ім. Ю. С. Червоного (Одеса, 16 грудня 2022 р.). Одеса. Фенікс. 2022. С. 62

Зокрема, однією зі стратегій ведення гібридної війни з боку Росії є застосування кібератак, направлених на українські державні реєстри, сервіси та системи, зокрема, і на «Електронний суд», який є підсистемою Єдиної судової інформаційно-телекомунікаційної системи (далі – ЄСІТС). Зокрема, у 2022 році хакерами була заблокована робота Єдиного державного реєстру судових рішень, електронного суду, веб-порталу «Судова влада України» та інш. Певний проміжок часу після цієї кібератаки, спостерігалися проблеми з веб-програмою «Бронювання систем відеоконференцзв'язку» з іншими судами, що позбавляє можливості проведення судових засідань в режимі відеоконференції[1].

19 грудня 2024 року відбулася одна з найбільших зовнішніх кібератак на державні реєстри України. У зв'язку з цим Державне підприємство «Інформаційні судові системи» повідомило про введення певних обмежень в роботі Електронного кабінету підсистеми «Електронного суду». Зокрема, було обмежено можливість реєстрації нового кабінету юридичної особи, надання доступу новому керівнику юридичної особи до кабінету, подання електронного виконавчого документа на виконання до Автоматизованої системи виконавчих проваджень тощо[2].

Неможливість здійснення правосуддя підтверджується судовими рішеннями 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)[3]. З огляду на вказане, в Господарському суді Кіровоградської області

[1] Ковальчук А., Чернявська Б. Забезпечення безпеки електронних даних у господарському судочинстві: правові та організаційні аспекти. *Право та державне управління.* 2023. вип. 2. С. 267

[2] Через атаку на державні реєстри у Електронному суді ввели низку обмежень. *Судово-юридична газета.* 20.12.2024. URL: https://sud.ua/uk/news/sud-info/318692-iz-za-ataki-na-gosudarstvennye-reestry-v-elektronnom-sude-vveli-ryad-ogranicheniy.

[3] Ковальчук А., Чернявська Б. Забезпечення безпеки електронних даних у господарському судочинстві: правові та організаційні аспекти. *Право та державне управління.* 2023. Вип. 2. С. 268.

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 відеоконференції, доступу до державних реєстрів, підписання електронним підписом електронних примірників судових рішень та направлення їх до ЄДРСР тощо»[1].

З урахуванням вищезазначеного, в умовах дії воєнного стану гостро постає питання забезпечення інформаційної безпеки під час здійснення правосуддя, що викликає нові завдання та покладає додаткову відповідальність на суддів під час розгляду та вирішення судових спорів, зокрема, через систему «Електронного суду». З отриманням беззаперечно прогресивних можливостей участі в судовому засіданні в режимі відеоконференції та дистанційного доступу до судових матеріалів виникає безліч викликів, серед яких, питання забезпечення конфіденційності, захисту персональних даних громадян тощо.

Відповідні загрози обумовлюють необхідність дослідження та розроблення пропозицій щодо удосконалення механізму забезпечення інформаційної безпеки під час здійснення судочинства, як під час повномасштабного вторгнення, так і у мирні часи. В контексті даного питання окремої уваги заслуговує робота підсистеми «Електронного суду», функціонування якої надає громадянам можливість отримати повноцінний доступ до захисту своїх прав та інтересів навіть у період дії воєнного стану[2].

Питанню правового забезпечення функціонування електронного судочинства присвячували свої наукові роботи такі вчені, як: А. Барікова, О. Бринцев, М. Гетманцев, Ю. Георгієвський, Н. Голубєва, С. Чванкін, Б. Чернявська, А. Ковальчук, С. Обрусна, І. Ізарова, Є. Петров та інші.

В Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 р. № 537-

[1] Ухвала Верховного Суду у справі No906/908/21. URL: https://reyestr.court.gov.ua/Review/109645641.

[2] Притуляк В. М. Підсистема електронний суд: особливості її функціонування в умовах воєнного стану. *Цивільне судочинство та виконавче провадження в умовах воєнного стану*: матеріали всеукр. наук.-практ. конф. ім. Ю. С. Червоного (Одеса, 16 грудня 2022 р.). Одеса: Фенікс, 2022. С. 62.

V було вперше було зроблено законодавче закріплення терміну «інформаційна безпека». А саме, відповідне поняття розкривається в законі як «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; небажані наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації»[1].

Бакалінська О. зазначає, що інформаційна безпека передбачає захист інформації від випадкових чи навмисних несанкціонованих дій, направлених на порушення конфіденційності, цілісності чи доступності певних даних[2].

Як зазначалось вище, в умовах сьогодення інформаційна безпека посідає перше місце в системі національної безпеки кожної держави, що підтверджується ч.1 ст. 17 Конституції України, яка закріплює, що забезпечення інформаційної безпеки України є однією із важливіших функцій держави та справою всього Українського народу.

Правова основа інформаційної безпеки України складається з міжнародних зобов'язань та національного законодавства. На міжнародному рівні слід згадати Будапештську конвенцію та Директиву щодо мережевої й інформаційної безпеки (NIS) (з англ.: «*Network and Information Security Directive*»). На національному рівні основними документами, що регулюють сферу інформаційної безпеки є Закон України № 2163-VIII від 05.10.2017 р. «Про основні засади забезпечення кібербезпеки України» та Національна стратегія кібербезпеки України.

Будапештська конвенція, яка була ратифіковна Україною у 2005 році, являє собою єдиний юридично обов'язковий міжнародний документ з кібербезпеки, який встановлює спільну кримінальну політику щодо захисту від кіберзлочинності шляхом прийняття відповідного внутрішнього законодавства та сприяння міжнародному співробітництву.

У 2016 році Європейський парламент ухвалив «Директиву щодо мережевої й інформаційної безпеки» (NIS), яка встановлює єдині пра-

[1] Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 9.01.2007 р. № 537-V. *ВВР України.* 2007. № 12. Ст. 102.

[2] Бакалінська О. Правове забезпечення кіберзахисту в Україні Координата. 2020. URL: https://coordynata.com.ua/pravove-zabezpecenna-kiberzahistu-v-ukraini

вила та вимоги для всіх країн ЄС у галузі кібербезпеки. Наразі Україна частково виконала відповідні вимоги і продовжує роботу в цьому напрямку.

Стаття 1 Закону України «Про основні засади забезпечення кібербезпеки України» визначає кібербезпеку, як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі.

Вагомим кроком для удосконалення системи кібербезпеки України стало прийняття Постанови Кабінету Міністрів України № 518 від 19.06.2019 р. «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», яким встановлено: визначення загальних вимог щодо кіберзахисту об'єктів критичної інфраструктури; визначення обов'язкових заходів забезпечення захисту від кібератак; запобігання порушенню конфіденційності, цілісності та доступності інформаційних ресурсів тощо.

Відповідно до Концепції побудови ЄСІТС, затвердженої Наказом ДСА України від 07.11.2019 р. № 1096, основним принципом побудови ЄСІТС є гібридна розподілена хмарна технологія, яка передбачає розмежування інформаційних середовищ ЄСІТС на відкрите, підключене до мережі Інтернет, і захищене, де обробляється інформація з обмеженим доступом. В Концепції ЄСІТС зазначається, що такі середовища є фізично розділеними, але побудовані за єдиними стандартами та технологіями, що забезпечують достатній рівень інформаційної безпеки.

Для забезпечення належного рівня інформаційної безпеки у складі ЄСІТС має бути передбачено створення захищеного інформаційного середовища та обмін інформацією з обмеженим доступом між судами, учасниками справи та іншими державними органами й установами системи правосуддя виключно через захищене середовище та захищену телекомунікаційну мережу.

Компоненти ЄСІТС мають функціонувати у складі захищеного та відкритого середовища. У захищеному середовищі, фізично відокремленому від мережі Інтернет та інших незахищених мереж, цир-

кулює інформація з обмеженим доступом (персональні дані, слідча таємниця, медична таємниця, сімейна таємниця, банківська таємниця, службова інформація тощо). Відкрите середовище ЄСІТС містить лише публічно доступні дані, в тому числі знеособлену інформацію. Доступ віддалених користувачів, у тому числі учасників судового процесу, здійснюється у відкрите середовище ЄСІТС. Подання та отримання даних, у тому числі документів судових справ у електронному вигляді, повідомлень про надходження/зміну документів тощо, здійснюється через захищений шлюз інформаційної взаємодії, який забезпечує фізичне розмежування захищеного та відкритого середовищ ЄСІТС і унеможливлює будь-які зовнішні втручання до компонентів ЄСІТС, що функціонують у захищеному середовищі ЄСІТС[1].

За своєю сутністю ЄСІТС, як комплексна уніфікована програма, надала можливість перенести більшість операцій пов'язаних зі здійсненням правосуддя, в електронну форму, автоматизувати деякі аналітичні, моніторингові, статистичні та інші операції[2].

З початку повномасштабної війни електронне судочинство деяких важливих змін, які стосуються як технічної, так і законодавної частини щодо його застосування. Так, наприклад, на думку Притуляка В. найбільш корисним нововведенням є інтеграція сервісу «Дія.Підпис» з підсистемою «Електронний суд», що дозволило значно швидше і легше підписувати і направляти документи одразу з підсистеми безпосередньо до суду, не використовуючи електронну пошту або інші додатки, які були раніше необхідні для підписання документів за допомогою КЕП[3].

Окрім того, підсистема «Електронного суду» отримала функціонал відеоконферецзв'язку. Отже, відтепер не потрібно використовувати інші програмні додатки, адже після авторизації в «Електронному суді» учасники справи можуть взяти участь у судовому засі-

[1] Про погодження Концепції побудови Єдиної судової інформаційно-телекомунікаційної системи: рішення Рада суддів України від 22.11.2019 No 97. URL: https://zakon.rada.gov.ua/rada/show/v0097414- 19#Text

[2] Берназюк О. Єдина судова інформаційно-телекомунікаційна система: поняття та структура. *Підприємництво, господарство і право.* 2019. № 6. С. 329. https://doi.org/10.32849/2663- 5313/2019.6.61

[3] Притуляк В. М. Підсистема електронний суд: особливості її функціонування в умовах воєнного стану. *Цивільне судочинство та виконавче провадження в умовах воєнного стану:* матеріали всеукр. наук.-практ. конф. ім. Ю. С. Червоного (Одеса, 16 грудня 2022 р.). Одеса. Фенікс. 2022. С. 63.

данні онлайн, що значного полегшує доступ до правосуддя, зокрема, громадянам, які знаходяться закордоном або не мають можливості брати участь без у судовому процесі безпосередньо в залі судового засідання з інших причин. Використання відеоконференції дозволяє забезпечити присутність сторін, свідків, перекладачів та інших учасників судового процесу, навіть якщо вони не можуть фізично перебувати в судовій залі або в умовах, коли їх участь є неможливою через потенційну загрозу їх життю, зокрема і під час воєнного стану.

Окрім зазначеного під час дії воєнного стану електронне судочинство дозволяє: отримувати повідомлення про надходження до кабінету нових документів та про зміну стану судової справи, у яких користувач є учасником; ознайомлюватись з матеріалами справи в електронному вигляді; переглядати та подавати заяви, клопотання та інші документи, які користувач створив в своєму кабінеті; формувати, переглядати та анульовувати електронні ордери та довіреності у підсистемі для швидкого доступу до матеріалів судової справи; мінімізувати час та кошти на роздруківку та відправку документів; отримувати судові рішення у електронному вигляді. Тобто, наразі наявні всі технічні можливості для забезпечення повноцінного дистанційного судового процесу: від моменту подання позову до моменту набрання рішенням законної сили[1].

Разом з тим, представниками суддівського апарату підкреслюється, що при розробці підсистеми «Електронний суд» та подальшому вдосконаленні дистанційного судочинста основний орієнтир був направлений на зручність та «доступность» цієї підсистеми для учасників справи та їх представників. Водночас, для суддів, їх помічників та секретарів судового засідання в питанні здійснення судочинства, по суті, нічого не змінилось, адже їх робота і далі передбачає особисту присутність в залі судового засідання, друк документів, формування паперових справ та спілкування з учасниками процесів традиційними засобами – поштою, телефоном або особисто[2].

---

[1] Притуляк В. М. Підсистема електронний суд: особливості її функціонування в умовах воєнного стану. *Цивільне судочинство та виконавче провадження в умовах воєнного стану*: матеріали всеукр. наук.-практ. конф. ім. Ю. С. Червоного (Одеса, 16 грудня 2022 р.). Одеса. Фенікс. 2022. С. 63.

[2] Арсірій Р. Електронне судочинство в період воєнного стану: очікування та реальність. *Судово-юридична газета*. 27.06.2024. URL: https://sud.ua/uk/news/blog/242253-elektronne-sudochinstvo-v-period-voyennogo-stanu-ochikuvannya-ta-realnist.

Окрім того, «левова частка» комунікації та документообіг між учасниками електронного судочинства відбувається за допомогою електронної пошти та хмарних сервісів для зберігання файлів, а також враховуючи значення відповідної інформації та небажані наслідки її розкриття, існує потреба в застосуванні дієвих заходів кібербезпеки. Витік інформації або небажане розголошення ходу чи результату судового процесу може спричинити суттєві наслідки, включаючи економічні втрати та репутаційну шкоду. Наприклад, публічне розкриття інформації щодо державних справ може негативно вплинути на державну політику.

Наразі одним з найбільш розповсюджених способів захисту даних є використання хмарних сервісів для їх зберігання, зважаючи доступність і достатню захищеність даних сервісів (наприклад, Google Drive від Google, Dropbox та OneDrive від Microsoft). Втім, на практиці використання хмарних сервісів є лише одним із можливих заходів покращення рівня інформаційної безпеки.

Як зазначалось вище, питання кібербезпеки в умовах воєнного стану є особливо важливим як для учасників процесу, так і для працівників судового апарату. Проте, попри численні кібератаки, які збільшились після початку повномасштабного вторгнення, вітчизняним законодавцем не було передбачено жодних нормативних змін в контексті покращення діловодства та підвищення інформаційної безпеки судочинства. Водночас, дистанційна форма здійснення судочинства залишається недостатньо унормованою в частині технічного забезпечення національних судів. Окрім того, до наявних проблем додались інші, зокрема, брак коштів на цифровий зв'язок чи забезпечення стабільного енергопостачання.

Водночас, ЄСІТС досі має різні вразливості, які можуть потенційно загрожувати інформаційній безпеці, зокрема, через хакерські атаки, фішинг, віруси, зловмисні програми тощо. Це може призвести до несанкціонованого доступу до судових даних, внищення інформації, порушення конфіденційності даних, а також перешкоджати нормальному функціонуванню системи правосуддя. Серед іншого, зловмисники можуть використовувати соціальну інженерію, щоб отримати несанкціонований доступ до судової інформації. Це може включати фальшиві електронні листи чи запити на інформацію тощо, з метою отримання доступу до системи. Такі ризики стають можли-

ві, а іноді навіть сприють атакам на систему, в умовах використання слабких паролів, кодів, недостатні навички працівників суду уникати шахрайство в Інтернеті тощо. Видається, що найбільш небезпечним є хакерські атаки, коли залучаються особи, що мають доступ до судової системи. Недостатня проінформованість персоналу про кіберзагрози може призвести до вразливостейсамої підсистеми «Електронний суд»[1].

З метою запобігання вищеперерахованим ризикам, видається доцільною розробка рекомендацій та протоколів роботи судів, які б могли зменшити загрозу стороннього втручання або маніпулювання в «ручному» режимі програмним забезпеченням підсистеми «Електронний суд». Зокрема, у жовтні 2024 року Національна школа суддів України проводила підготовку та підвищення рівня кваліфікації працівників апаратів судів, відповідальних за інформаційно-технічне забезпечення. Навчання полягало у підготовці працівників інформаційно-технічного забезпечення судів до ефективної та безпечної роботи в цифровому середовищі, забезпеченні надійності електронного документообігу та дотриманні стандартів кібербезпеки. Програма охоплювала як технічні аспекти обміну документами через підсистему "Електронний суд", так і правила інформаційної безпеки під час війни, включаючи інформаційно-психологічну гігієну[2].

При дослідженні вразливостей системи ЄСІТС неможливо оминути систему електронного архівування. А саме, ЄСІТС дозволяють створювати електронні архіви правових документів, судових рішень, законів та інших нормативних актів. В цьому контексті не варто забувати про можливість усвідомленого псування або некоректного внесення інформації працівниками судової системи, що мають доступ до ЄСІТС[3].

Відповідно до ст. 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах», відповідальність за забезпе-

---

[1] Ковальчук А., Чернявська Б. Забезпечення безпеки електронних даних у господарському судочинстві: правові та організаційні аспекти. *Право та державне управління.* 2023. Вип. 2. С. 269.

[2] Інформаційна безпека судів під час війни. *Національна школа суддів України.* 31.10.2024. URL: https://nsj.gov.ua/ua/news/informatsiyna-bezpeka-sudiv-pid-chas-viyni/

[3] Ковальчук А., Чернявська Б. Забезпечення безпеки електронних даних у господарському судочинстві: правові та організаційні аспекти. *Право та державне управління.* 2023. Вип. 2. С. 269.

чення захисту інформації в системі покладається на власника системи. Розпорядником інформації, який відповідає за захист інформаційних систем судової системи є Державна судова адміністрація України. Разом з тим, до сфери управління ДСА належить Державне підприємство «Інформаційні судові системи»[1]. Вказане підприємство створено, серед іншого, з метою організації збереження та захисту даних, що містяться в автоматизованих системах державних реєстрів; надання послуг з інформаційно-технічного забезпечення судів; забезпечення діяльності органів судової влади, у тому числі в умовах особливого періоду[2]. Судячи з опису обов'язків підприємства, що були надані Державною судовою адміністрацією, саме до цієї юридичної особи слід звертатися з питаннями повного або часткового відключення суду від доступу до електронних сервісів.

У межах реалізації Стратегії кібербезпеки України для виконання постанови Кабміну від 04.04.2023 № 299, 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. Серед методичних рекомендації можна виокремити: необхідний перелік заходів із кіберзахисту, яких можуть вживати суб'єкти забезпечення кібербезпеки послідовно за етапами реагування на кібератаки; механізм застосування критеріїв, за якими визначається категорія (рівень) критичності кібератаки; принципи пріоритезації кібератак; типовий перелік заходів із реагування на кібератаки для одночасного відстеження заходів до їх завершення тощо.

Реалізацію відповідних методичних рекомендацій покладено на начальника Відділу інформаційно-технічного забезпечення, захисту інформації та баз даних суду. Отже, начальник Відділу здійснює: забезпечення кібербезпеки та захисту інформації в суді, кіберзахи-

[1] Витяг із Статуту Державного підприємства «Інформаційні судові системи» (затвердженого наказом Державної судо- вої адміністрації України від 26 листопада 2019 року № 1142). URL: https://ics.gov.ua/ics/about/acts/

[2] 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.

сту 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, на начальника Відділу покладається обов'язок з забезпечення формування довідкових матеріалів, презентацій по користуванню програмним забезпеченням та інформаційними системами, які впроваджені у суді. Тобто, вказана особа здійснює інформаційні роз'яснення для працівників суду, зокрема, щодо способів уникнення інтернет-шахрайства та інформаційної гігієни[1].

Висновки

Робота підсистеми «Електронного суду» заслуговує окремої уваги в період воєнного часу, адже саме відповідна підсистема дозволила адаптуватися до складних умов воєнного стану та забезпечити функціонування судової системи в дистанційному режимі, що надало можливість громадянам отримати доступ до правосуддя як законодом, так і в умовах ракетних обстрілів в межах України.

З урахуванням вищезазначеного, можна констатувати, що всі вищеперераховані виклики не зупиняюсь здійснення правосуддя, хоча можуть ускладнювати чи гальмувати роботу суддівського апарату. Одним із ризиків, який можна очікувати через кібератаки під час проведення судового процесу, є ризик погіршення репутації дистанційної форми судочинства, як надійного та прогресивного способу здійснення правосуддя.

Впровадження електронного судочинства в Україні має на меті підвищення ефективності, якості та прозорості правосуддя, зменшення бюрократичних процедур шляхом автоматизації процесів документообігу, розподілу справ, обміну документами між судами та

[1] Ковальчук А., Чернявська Б. Забезпечення безпеки електронних даних у господарському судочинстві: правові та організаційні аспекти. *Право та державне управління.* 2023. Вип. 2. С. 270.

учасниками судового процесу, фіксування судового процесу, участь учасників судового процесу в режимі відеоконференції, забезпечення фінансових, майнових, організаційних, інформаційно-телекомунікаційні та інші потреб органів судової влади.

Інформаційна безпека України забезпечується шляхом проведення державної політики відповідно до прийнятих в установленому порядку нормативно-правових актів, концепцій, стратегій і програм. Основними напрямами державної політики у сфері кібербезпеки України є: створення захищеного національного сегмента кіберпростору, що сприятиме підтриманню відкритого суспільства і забезпечуватиме безпечне використання цього простору суспільством; запобігання втручанню у внутрішні справи України і нейтралізація посягань на її інформаційні ресурси з боку інших держав; посилення обороноздатності держави у кіберпросторі; зниження рівня уразливості об'єктів кіберзахисту; забезпечення повноправної участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки тощо.

Для захисту системи ЄСІТС важливо приділяти увагу інформаційній безпеці, використовувати захисне програмне забезпечення, проводити регулярні тренінги серед працівників суду, аудити безпеки, а також дотримуватися міжнародних стандартів щодо обробки, збереження і передачі судових даних.

З урахуванням вищезазначеного, забезпечення безпечного функціонування ЄСІТС та підсистеми «Електронний суд» постає одним з пріоритетів подальшої державної політики в частині реформування судової системи України.

Ключові слова: електронне судочинство, інформаційна війна, гібридна війна, кіберзагроза, кібербезпека.