УДК 004.056.5:342.738:347.9(477)

https://doi.org/10.68134/ah.2026-11-20.038

Назимко Валерія
студент, Дніпровський національний університет внутрішніх справ

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В АРХІТЕКТУРІ ЄСІТС

Анотація. Забезпечення кібербезпеки та захисту персональних даних у межах Єдиної судової інформаційно-комунікаційної системи (ЄСІТС) становить одну з основних правових та організаційно-технічних передумов належного функціонування електронного судочинства в Україні. Специфіка цієї системи полягає в обробленні значних масивів інформації, що охоплюють персональні дані учасників судових проваджень, матеріали кримінальних, цивільних, господарських та адміністративних справ, відомості про майновий стан осіб, медичну інформацію, процесуальні документи й інші дані з обмеженим доступом. Нормативно-правову основу їх захисту становлять закони України «Про захист персональних даних», «Про захист інформації в інформаційно-комунікаційних системах» та «Про основні засади забезпечення кібербезпеки України». Ефективна модель кіберзахисту повинна передбачати багатофакторну автентифікацію, розмежування прав доступу, криптографічний захист інформації, журналювання операцій користувачів та систематичний аудит захищеності програмного забезпечення. Першочерговими напрямами модернізації визначено впровадження централізованого моніторингу кіберінцидентів, регулярного тестування на проникнення та резервного копіювання судових даних. Подальший розвиток ЄСІТС має здійснюватися на основі інтеграції принципів security by design та privacy by design.

Ключові слова: кібербезпека, захист персональних даних, ЄСІТС, електронне судочинство, інформаційна безпека, privacy by design, security by design.

Abstract. Ensuring cybersecurity and personal data protection within the Unified Judicial Information and Communication System (UJICS) constitutes one of the fundamental legal and organisational-technical prerequisites for the proper functioning of electronic justice in Ukraine. The specificity of this system lies in the processing of large volumes of information encompassing personal data of judicial proceedings participants, materials of criminal, civil, commercial and administrative cases, information on property status, medical information, procedural documents and other restricted-access data. The regulatory framework for their protection is established by the Laws of Ukraine «On Personal Data Protection», «On Information Protection in Information and Communication Systems» and «On the Fundamental Principles of Cybersecurity of Ukraine». An effective cyber-protection model must provide for multi-factor authentication, differentiation of access rights, cryptographic protection of information, user activity logging and systematic software security audits. Priority modernisation directions include the introduction of centralised cyber-incident monitoring, regular penetration testing and backup of judicial data. Further development of UJICS should be based on the integration of security by design and privacy by design principles.

Keywords: cybersecurity, personal data protection, UJICS, electronic justice, information security, privacy by design, security by design.

Вступ

Забезпечення кібербезпеки та захисту персональних даних у межах Єдиної судової інформаційно-комунікаційної системи (ЄСІТС) становить одну з основних правових та організаційно-технічних передумов належного функціонування електронного судочинства в Україні. Специфіка цієї системи полягає в обробленні значних масивів інформації, що охоплюють персональні дані учасників судових проваджень, матеріали кримінальних, цивільних, господарських та адміністративних справ, відомості про майновий стан осіб, медичну інформацію, процесуальні документи й інші дані з обмеженим доступом.

Нормативно-правову основу їх захисту становлять закони України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI, «Про захист інформації в

інформаційно-комунікаційних системах» від 5 липня 1994 року № 80/94-ВР та «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [1]. Відповідно до статті 2 Закону України «Про захист інформації в інформаційно-комунікаційних системах» об'єктами захисту визнаються як інформація, що обробляється в системі, так і програмне забезпечення, призначене для її оброблення. Зазначене положення має принципове значення, оскільки встановлює необхідність комплексного захисту не лише електронних документів, але й програмно-технічних компонентів судової інформаційної інфраструктури [2].

Результати та обговорення

Особливу небезпеку становлять атаки з використанням шкідливого програмного забезпечення, фішингові повідомлення та несанкціоноване отримання облікових даних працівників суду. У цьому контексті застосування кваліфікованого електронного підпису необхідно розглядати як важливу, але недостатню самостійну гарантію безпеки. Ефективна модель кіберзахисту повинна передбачати багатофакторну автентифікацію, розмежування прав доступу відповідно до процесуальних повноважень, криптографічний захист інформації, журналювання операцій користувачів та систематичний аудит захищеності програмного забезпечення. Науково обґрунтованим є впровадження принципу мінімально необхідних привілеїв, відповідно до якого кожний користувач отримує доступ виключно до інформації, необхідної для виконання його процесуальних або службових функцій [3, с. 432].

Окремого аналізу потребує питання розподілу юридичної відповідальності за збереження конфіденційності персональних даних між суб'єктами адміністрування ЄСІТС. Відповідно до статті 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах» відповідальність за забезпечення захисту інформації покладається на власника або розпорядника системи. Організаційне та фінансове забезпечення функціонування підсистем ЄСІТС здійснює Державна судова адміністрація України, тоді як функції технічного адміністрування покладено на державне підприємство «Інформаційні судові системи». Важливою проблемою залишається розмежування відповідальності за порушення, що виникають на різних рівнях інформаційної інфраструктури: унаслідок недоліків програмного забезпечення, неправомірних дій працівників суду або компрометації електронного кабінету користувача. Зокрема, витік інформації через помилкове налаштування прав доступу має відрізнятися за правовими наслідками від несанкціонованого поширення персональних даних конкретною посадовою особою. При цьому стаття 8 Закону України «Про захист персональних даних» закріплює права суб'єкта персональних даних, зокрема на отримання інформації про оброблення його даних, доступ до них та захист від незаконного оброблення. Водночас реалізація цих прав у судочинстві має враховувати спеціальні процесуальні правила, вимоги збереження матеріалів справи та законні обмеження доступу [4, с. 71].

Висновки

З огляду на зазначене першочерговими напрямами модернізації доцільно визначити впровадження централізованого моніторингу кіберінцидентів, регулярного тестування на проникнення, резервного копіювання судових даних, територіально розподілених механізмів їх відновлення та незалежного оцінювання інформаційної безпеки. Особливої уваги потребує забезпечення безперервності судового провадження у випадках технічних збоїв або кібератак, оскільки тимчасова недоступність електронного кабінету може фактично перешкоджати своєчасному поданню процесуальних документів. З правової позиції доцільно деталізувати процедури підтвердження технічної несправності системи, порядок фіксації кіберінцидентів та процесуальні гарантії відновлення порушених прав учасників судочинства. Подальший розвиток ЄСІТС повинен здійснюватися на основі інтеграції принципів security by design (безпека на етапі проєктування) та privacy by design (захист персональних даних на етапі

проєктування), що дозволить забезпечити належний баланс між цифровізацією правосуддя, відкритістю судової діяльності та охороною конфіденційної інформації.

Список використаних джерел

1. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України. № № 34. С. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 18.11.2026)
2. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. Відомості Верховної Ради України. № № 31. С. Ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 18.11.2026)
3. Савчук В.С. Цифровізація правосуддя: інформаційно-безпекові аспекти. R30-02144. 2026. С. 432.
4. Колесніков А. П. Підсистема штучного інтелекту як новий модуль ЄСІТС: перспективи застосування. Редакційна колегія. 2024. С.70-72.