ІНФОРМАЦІЙНА БЕЗПЕКА В ДІЯЛЬНОСТІ СУДІВ: ВИКЛИКИ ТА ШЛЯХИ ВИРІШЕННЯ

КРУПНОВА Любов Василівна - доктор юридичних наук, професор, професор кафедри кримінального права і правосуддя, Міжнародний економіко-гуманітарний університет ім. академіка Степана Дем'янчука

ORCID ID: https://orcid.org/0000-0003-1789-0647

КРУПНОВА Анастасія Олександрівна - адвокат Адвокатського об'єднання «Крупнова і партнери»

ORCID ID: https://orcid.org/0009-0007-7819-9813

ГОРКАВА Вікторія Юріївна - суддя Печерського районного суду міста Києва, доктор філософії за спеціальністю «Право»

DOI: https://doi.org/10.71404/LAW.UA.2025.1.11

У статті розглянуто актуальні проблеми забезпечення інформаційної безпеки в діяльності судів України. Особливу увагу приділено значенню інформаційної безпеки судової системи, яка відіграє ключову роль у забезпеченні правосуддя та захисті прав громадян. Суди є одними з основних державних інституцій, що нерідко зазнають кібератак, спрямованих на підрив їхньої діяльності, витік конфіденційних даних або дестабілізацію правового порядку. В умовах зростання кіберзагроз ефективний моніторинг викликів є невід'ємною складовою захисту інформаційних систем судів, збереження цілісності судових рішень і зміцнення довіри громадян до судової влади.

Для вирішення зазначених викликів доцільно розвивати інфраструктуру кібербезпеки судів, забезпечувати конфіденційність та цілісність судових даних, використовувати національні й міжнародні стандарти у сфері інформаційної безпеки, впроваджувати заходи запобігання та протидії внутрішнім загрозам, а також залучати експертів і партнерів для посилення рівня безпеки. Зроблено висновок, що реалізація цих заходів сприятиме значному підвищенню рівня захищеності судових інформаційних систем, посиленню довіри до судової влади та мінімізації ризиків неправомірного втручання в процеси судочинства.

Ключові слова: інформаційна безпека, судова система, кіберзагрози, захист даних, конфіденційність, кібератаки, правосуддя, цифрова безпека, моніторинг загроз, кіберзахист, судові інформаційні системи, витік інформації, довіра до судової влади, державні інституції.

Постановка проблеми

На сьогодні інформація виступає одним із головних елементів у багатьох сферах державного управління і є важливим фактором суспільних відносин. Зміни, що відбуваються на сучасному етапі в Україні, у першу чергу, пов'язані зі зростанням великих обсягів інформації та її швидкою зміною. Тому саме на державу покладається завдання щодо забезпечення доступу громадян України до об'єктивної інформації, пов'язаної з усіма сферами життєдіяльності громадянина, у тому числі інформації, що використовується в національних судах України. Відтак, інформаційна безпека є невід'ємною складовою національної безпеки України, тому вона викликає підвищений інтерес у суспільства, особливо в умовах сьогодення, коли проти України застосовуються новітні засоби по веденню інформаційної війни [1, с. 301-302].

У сучасному світі інформаційна безпека є ключовим елементом функціонування будь-якої системи, особливо у сферах, які мають значний вплив на права та свободи громадян. Судова система, як одна з основних гі-

лок влади, не є винятком. У судовій діяльності обробляється величезний обсяг даних, що включають персональні дані учасників процесу, конфіденційну інформацію, а також відомості, які мають вирішальне значення для забезпечення справедливості та законності. Втрата або несанкціонований доступ до таких даних може призвести до серйозних наслідків, включаючи порушення прав громадян, дискредитацію судової влади та створення передумов для корупції.

Сьогодні судова система України, як і судові системи інших країн, стикається з новими викликами, що виникають в умовах глобальної цифровізації. Розширення використання інформаційних технологій у судочинстві, таких як електронний документообіг, онлайн-розгляд справ, відеоконференції та електронні бази даних, відкриває нові можливості для оптимізації роботи судів. Проте водночас ці технології створюють додаткові ризики для інформаційної безпеки. Кібератаки, витоки даних, незаконний доступ до інформаційних систем – усе це лише частина загроз, які постають перед судовими установами. Усе це вимагає комплексного підходу до забезпечення інформаційної безпеки, що включає як технічні, так і організаційні заходи.

Аналіз останніх досліджень і публікацій

Інформаційна безпека у сфері правосуддя привертає дедалі більшу увагу дослідників, що обумовлено стрімкою цифровізацією судових процесів та необхідністю забезпечення конфіденційності й цілісності судової інформації. Наукові роботи в цій галузі зосереджені на вивченні кіберзагроз, аналізі ефективності заходів захисту, а також розробці рекомендацій для мінімізації ризиків.

Значний внесок у дослідження питань інформаційної безпеки зробили міжнародні організації, такі як Європейська комісія, ENISA (Агентство Європейського Союзу з кібербезпеки) та ООН, які розробляють стандарти й рекомендації з безпечного використання цифрових технологій у судових системах. У звітах цих організацій наголошується на важливості забезпечення кібербезпеки як основного елемента судової реформи.

У працях українських дослідників особлива увага приділяється питанням законодавчого регулювання інформаційної безпеки. Наприклад, В. Ліпкан, Н. Литвин, А. Марущак, Т. Субіна та інші аналізують проблеми захисту персональних даних в органах державної влади, звертаючи увагу на необхідність гармонізації українського законодавства із нормами ЄС. У своїх роботах автори підкреслюють, що наявна нормативна база є недостатньо адаптованою до сучасних викликів, що створює прогалини в захисті інформації. Такі науковці, як І. Бачило, Є. Дуліба, А. Калараш, Н. Литвин, О. Плесканка, В. Теремецький та інші, наголошують, що цифровізація судової системи, хоча й відкриває значні можливості для підвищення прозорості та доступності правосуддя, водночас створює нові загрози, пов'язані з витоком конфіденційної інформації, незаконним доступом до електронних реєстрів і недостатньою захищеністю судових інформаційних систем.

Попри значну кількість наукових робіт, аналіз останніх досліджень свідчить, що багато аспектів інформаційної безпеки судів потребують подальшого вивчення. Зокрема, залишаються недостатньо дослідженими питання інтеграції інформаційних систем судів з іншими державними реєстрами, а також вплив цифровізації на захист прав учасників судових процесів.

Таким чином, наукові розвідки в галузі інформаційної безпеки судів забезпечують важливе теоретичне підґрунтя для вдосконалення практичних заходів захисту, але водночас вказують на необхідність подальшого міждисциплінарного підходу до розв'язання існуючих проблем.

Метою цієї статті є аналіз основних викликів, з якими стикається судова система в контексті інформаційної безпеки, а також розробка рекомендацій щодо їх подолання. Особливу увагу приділено питанням модернізації технічного забезпечення судів, підвищення кваліфікації персоналу, вдосконалення законодавчого регулювання та запровадження ефективних механізмів моніторингу та реагування на кіберзагрози.

Виклад основного матеріалу

Перш ніж говорити про інформаційну безпеку судів, необхідно з'ясувати поняття інформаційного забезпечення судів, адже саме воно формує основу для організації та функціонування інформаційних процесів у судовій системі. Інформаційне забезпечення судів охоплює комплекс заходів, засобів і технологій, які забезпечують збирання, обробку, зберігання, передачу та використання інформації, необхідної для здійснення правосуддя [2, 3, 4]. Це включає не лише внутрішні інформаційні системи судів, але й правові, організаційні та технічні аспекти, які регулюють доступ до інформації, її конфіденційність, цілісність та актуальність. Інформаційне забезпечення охоплює широкий спектр даних: від процесуальних документів і судових рішень до персональних даних учасників судових процесів.

Завдання інформаційного забезпечення діяльності судів обумовлене інформаційними потребами, які визначаються як певний стан суб'єкта предметної діяльності, який виникає у зв'язку з необхідністю отримання відомостей, потрібних для вирішення предметних задач. Призначення інформаційного забезпечення діяльності судів обумовлює необхідність дотримання вимог (принципів), які до нього висуваються [5, с. 112]

Так, О.З. Хотинська-Нор зазначає про такі принципи інформаційного забезпечення:

– забезпечення достовірності інформації, тобто отримання (надходження) її з першоджерел;

– забезпечення об'єктивності інформації, тобто отримання (надходження) її з різних джерел;

– забезпечення оперативності інформації, тобто інформація повинна бути своєчасно надана та оперативно опрацьована;

– забезпечення достатності інформації, тобто формування необхідного масиву релевантної інформації, що дозволить прийняти оптимальні рішення [6, с. 84].

Розуміння сутності та структури інформаційного забезпечення судів є ключовим для визначення потенційних ризиків та загроз, які можуть вплинути на його функціонування, і, відповідно, для формування комплексної системи інформаційної безпеки. Моніторинг загроз у цьому контексті виступає як невід'ємний елемент, що забезпечує своєчасне виявлення, аналіз і оцінку потенційних загроз, спрямованих на порушення конфіденційності, цілісності чи доступності інформації.

Комплексний підхід до інформаційного забезпечення судів дозволяє враховувати всі аспекти взаємодії інформаційних потоків, а моніторинг виступає механізмом, який дозволяє ідентифікувати проблемні зони, запобігати можливим атакам та адаптувати заходи безпеки до мінливих умов. Таким чином, чітке усвідомлення принципів інформаційного забезпечення є не лише основою стабільного функціонування судової системи, а й відправною точкою для побудови ефективної системи моніторингу загроз інформаційній безпеці.

Відтак, в умовах сьогодення моніторинг загроз інформаційній безпеці, що характеризуються тривалою російською агресією проти України, загальною нестабільною геополітичною обстановкою, високим ступенем невизначеності зовнішнього та внутрішньо середовища, обмеженими ресурсами та посиленням кіберзагроз, набуває все більшої актуальності. Негативні обставини, що склалися останніми роками, підкреслюють важливість моніторингу стану інформаційної безпеки в Україні, який функціонує як критичний механізм, що забезпечує шляхом збирання та дослідження відомостей щодо розпізнання можливих атак, попередження, виявлення та оперативне реагування на кризові ситуації у сфері інформаційної безпеки [7, с. 55].

Особливої уваги потребує інформаційна безпека судової системи, яка виконує важливу роль у забезпеченні правосуддя та захисту прав громадян. Суди є одними з ключових державних інституцій, на які спрямовуються кібератаки з метою компрометації їхньої роботи, витоку конфіденційних даних чи дестабілізації правового порядку. У цих умовах ефективний моніторинг загроз є невід'ємним елементом захисту судових інформаційних систем, забезпечення цілісності судових рішень та збереження довіри громадян до системи правосуддя.

Таким чином, моніторинг загроз інформаційній безпеці в умовах сучасних викликів є основою для формування дієвих механізмів захисту судової системи, яка повинна залишатися стійкою до зовнішніх і внутрішніх загроз навіть в умовах обмежених ресурсів.

Моніторинг загроз інформаційній безпеці в Україні – це системний процес оцінки стану безпеки за визначеними критеріями на нормативному, організаційному, процедурному та технічному рівнях. Його результати сприяють створенню ефективної та економічної системи інформаційного захисту, що поєднує технічні засоби, процедури, організаційні та правові заходи в єдиній моделі управління [8]. Моніторинг інформаційної безпеки дає змогу ухвалювати своєчасні та обґрунтовані рішення для забезпечення захисту суверенітету, територіальної цілісності та конституційного ладу, а також конституційних прав громадян на доступ до достовірної інформації. Він сприяє створенню ефективної системи протидії загрозам, зокрема поширенню недостовірної інформації, деструктивної пропаганди та несанкціонованому використанню даних [9]. Отже, моніторинг є ключовим елементом забезпечення інформаційної безпеки, спрямованим на збереження життєво важливих інтересів держави, суспільства та громадян через своєчасне виявлення загроз і впровадження заходів для їхньої нейтралізації.

Моніторинг загроз інформаційній безпеці для судової системи передбачає систематичне виявлення, аналіз та оцінку потенційних ризиків і загроз, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації в судових установах. Його актуальність зумовлена викликами, що постають перед судовою системою в умовах зростання цифровізації, посилення кіберзагроз та необхідності реагувати на складну інформаційну обстановку.

Так, виклики у сфері інформаційної безпеки судів є багатогранними та охоплюють технічні, організаційні та правові аспекти. Одним із ключових викликів є кібератаки, спрямовані на судові інформаційні системи, які можуть призвести до витоку конфіденційної інформації, знищення або пошкодження даних, а також до порушення безперервності роботи судових органів. Загрози також включають несанкціонований доступ до електронних реєстрів, маніпуляції судовими справами чи процесами, що ставить під сумнів цілісність і справедливість правосуддя. Проблеми виникають і внаслідок недостатнього рівня технічного захисту інформаційних систем, зокрема застарілого програмного забезпечення, відсутності оновлень або слабких протоколів автентифікації користувачів.

Не менш важливим викликом є людський фактор: недоліки в навичках працівників судової системи щодо забезпечення інформаційної безпеки, нехтування стандартами захисту даних, неналежна обізнаність про актуальні кіберзагрози. В умовах цифровізації судочинства ризики збільшуються через недосконалість регулювання у сфері захисту інформації, що створює прогалини для можливих зловживань. Додатковим ускладненням є низький рівень фінансування заходів інформаційної безпеки, що обмежує можливості для впровадження сучасних технологій захисту, проведення аудитів безпеки чи навчання персоналу.

Крім того, складність викликів посилюється зовнішніми факторами, такими як геополітична нестабільність, кіберзагрози з боку держав-агресорів та активне використання технологій для гібридної війни, які мають на меті дестабілізувати роботу державних інституцій, включаючи судову систему. Усе це вимагає системного підходу до вирішення проблем інформаційної безпеки судів, зокрема впровадження міжнародних стандартів, удосконалення нормативної бази, розробки нових технологічних рішень та забезпечення належного рівня фінансової підтримки.

Для вирішення вказаних вище викликів, пов'язаних з інформаційною безпекою судів в Україні, доцільно:

- *розвивати інфраструктуру кібербезпеки судів*, що включає створення спеціалізованих систем захисту судових інформаційних ресурсів, які б забезпечували надійний захист від кіберзагроз; оновлювати і модернізувати чинні судові інформаційні системи, зокрема для забезпечення захисту персональних даних осіб, які беруть участь у судових процесах;

- *забезпечувати конфіденційність та цілісність судових даних*, а саме використовувати технології шифрування для забезпечення конфіденційності і цілісності судових даних під час їх обміну, зберігання; впроваджувати електронні підписи і використовувати двофакторну аутентифікацію для доступу до судових документів і систем;

- *використовувати національні і міжнародні стандарти у сфері інформаційної безпеки*, що передбачає адаптацію національного законодавства до міжнародних стандартів у сфері кібербезпеки, зокрема в межах співпраці з ЄС та іншими міжнародними організаціями; запроваджувати стандарти безпеки інформації, які включають чіткі регламенти щодо захисту даних суддів, адвокатів, прокурорів та інших осіб, що беруть участь у судових справах;

- *запроваджувати заходи запобігання і протидії внутрішнім загрозам*, зокрема це створення механізмів для виявлення та запобігання витоку інформації зсередини судової системи, у тому числі через внутрішні розслідування та контроль доступу до чутливих даних; запровадження обмеження на доступ до інформації на основі ролей і потреби в знанні, що дозволяє мінімізувати ризик несанкціонованого доступу;

- *залучати експертів та партнерів для забезпечення безпеки*, що полягає в співпраці з фахівцями з інформаційної безпеки, а також міжнародними партнерами, які можуть допомогти в розробці та впровадженні ефективних заходів захисту судових інформаційних систем; проведенні аудитів та тестів на вразливість для виявлення і усунення потенційних слабких місць.

Рішення цих проблем дозволить значно підвищити рівень безпеки судових інформаційних систем, забезпечити довіру до судової влади та зменшити ризик неправомірного втручання в процеси судочинства.

Висновки

Забезпечення інформаційної безпеки в діяльності судів є необхідною умовою для збереження довіри громадян до правосуддя, а також захисту прав учасників судових процесів. Виклики у цій сфері потребують комплексного підходу, що поєднує технологічні, організаційні та правові заходи. Лише спільними зусиллями держави, судових органів та громадськості можна створити надійну систему захисту судової інформації.

Література

1. Литвин Н. А. Реалізація інформаційної політики органами Державної фіскальної служби України: адміністративно-правовий аспект: монографія. Київ: Гельветика, 2018. 516 с.

2. Ахтирська Н. Інформаційне забезпечення пізнавальних процесів у кримінальному судочинстві України. *Віче*. 2012. № 8. URL: https://veche.kiev.ua/journal/3073/ (дата звернення: 23.01.2025)

3. Єльцов В. О. Сутність інформаційного забезпечення діяльності судів. *Форум права*. 2010. № 4. С. 364-368.

4. Волошина В.А. Науково-консультативне забезпечення діяльності Верховного Суду України : дис. … канд. юрид. наук: 12.00.10. К., 2016. 256 с.

5. Раца В.А. Гносеологічний аспект поняття «інформаційне забезпечення діяльності судів». *Вісник кримінального судочинства*. 2016. № 4. С. 109-115. URL: https://vkslaw.knu.ua/images/verstka/4_2016_Ratsa.pdf (дата звернення: 23.01.2025)

6. Хотинська-Нор О. З. Теорія і практика судової реформи в Україні: монографія. К.: Алерта, 2016. 428 с.

7. Крупнова А. О. Система моніторингу загроз інформаційній безпеці в Україні. *Період трансформаційних процесів в світовій науці: задачі та виклики*: збірник наукових праць з матеріалами III Міжнародної наукової конференції (м. Хмельницький, 12 липня, 2024 р.). Вінниця: ТОВ «УКРЛОГОС Груп, 2024. С. 55 – 61.

8. Про моніторинг безпеки в інформаційній системі. URL: https://duikt.edu.ua/uploads/n_7836_42482763.pdf?file=n_7836_42482763.pdf (дата звернення: 23.01.2025)

9. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 23.01.2025)

SUMMARY

The article considers the current problems of ensuring information security in the activities of the courts of Ukraine. Particular attention is paid to the importance of information security of the judicial system, which plays a key role in ensuring justice and protecting the rights of citizens. Courts are one of the main state institutions that are often subjected to cyberattacks aimed at undermining their activities, leaking confidential data or destabilizing the legal order. In the context of growing cyber threats, effective monitoring of challenges is an integral part of protecting court information systems, preserving the integrity of court decisions and strengthening citizens' trust in the judiciary. To address these challenges, it is advisable to develop the cyber security infrastructure of courts, ensure the confidentiality and integrity of court data, use national and international standards in the field of information security, implement measures to prevent and counter internal threats, and also involve experts and partners to strengthen the level of security. It was concluded that the implementation of these measures will contribute to a significant increase in the level of security of judicial information systems, strengthening trust in the judiciary and minimizing the risks of improper interference in judicial processes.

Keywords: information security, judicial system, cyber threats, data protection, confidentiality, cyber attacks, justice, digital security, threat monitoring, cyber protection, judicial information systems, information leakage, trust in the judiciary, state institutions.