ІЛЬЄНКО В. Ю.,
магістр права,
секретар с/з
(Господарський суд Дніпропетровської області)

ІЛЬЄНКО Д. Ю.,
аспірант кафедри публічного
та приватного права
(Університет митної справи
та фінансів),
помічник судді
(Господарський суд Дніпропетровської області)

УДК 342
DOI https://doi.org/10.32842/2078-3736/2025.3.1.25

ЗАХИСТ ІНФОРМАЦІЇ ПРИ ЕЛЕКТРОННІЙ ВЗАЄМОДІЇ МІЖ ОРГАНАМИ ДЕРЖАВНОЇ ТА СУДОВОЇ ВЛАДИ

Захист інформації є ключовим аспектом у роботі органів державної та судової влади, оскільки правильність, точність та незмінність інформації є основою для прийняття важливих рішень, що можуть впливати на національну безпеку, охорону прав фізичних та юридичних осіб. У випадку неналежного захисту, дані можуть бути викрадені або змінені, що безпосередньо зашкодить законним правам громадян та організацій. Крім того, втручання в дані або їх зміна може призвести до помилкових рішень у судових справах чи роботі органів державної влади, що матиме серйозні наслідки для правосуддя та правової роботи зазначених органів. Тому забезпечення належного захисту інформації стає питанням не тільки технічного, але й юридичного характеру.

Одним із важливих завдань органів влади є створення та впровадження механізмів безпеки, а також регулярний моніторинг інформаційних систем, що забезпечує оперативне реагування на можливі загрози. Для цього важливим є впровадження систем аудиту та навчання співробітників, а також закріплення правових механізмів для захисту інформації в цифровому просторі. Наявність чіткої нормативно-правової бази, зокрема правове закріплення механізмів захисту, обробки, відновлення та використання інформації є важливою умовою для забезпечення правової визначеності у разі порушення безпеки даних, що дозволить швидко реагувати на інциденти та захищати законні інтереси громадян.

Електронна взаємодія (електронний документообіг) між органами державної та судової влади вимагає надійного доступу до інформації для всіх учасників документообігу. Кіберзлочини, зломи або технічні збої в системі можуть ускладнити доступ до критично важливих даних, що негативно позначиться на виконанні судових рішень і функціонуванні органів влади. Для запобігання таким ситуаціям важливим є дотримання вимог нормативно-правових актів, що регулюють політику захисту електронних документів та інформації, котрі в свою чергу передбачають відповідальність за безпеку обробки інформації.

Використання новітніх технологій, таких як шифрування, біометрична аутентифікація, блокчейн, дає змогу значно підвищити рівень захисту даних

та ефективність електронної взаємодії. Комплексний підхід до цих технологій дозволить забезпечити належне функціонування державних і судових органів, зміцнити довіру громадян до державних установ, а також підвищити ефективність правового процесу. Впровадження персоналізованих електронних кабінетів сприятиме ще більшій безпеці, швидкому обміну інформацією та забезпеченню її збереження протягом тривалого часу.

Ключові слова: *інформаційно-комунікаційна система, електронний кабінет, електронний документ, цифровий носій, захист інформації, цілісність інформації, біометрична аутентифікація, блокчейн, електронний підпис.*

Ilienko V. Yu., Ilienko D. Yu. Protection of information in electronic interaction between state and judicial authorities

Information protection is a key aspect of the work of government and judicial authorities, as the correctness, accuracy and integrity of information is the basis for making important decisions that may affect national security and the protection of the rights of individuals and legal entities. In case of inadequate protection, data can be stolen or altered, which will directly harm the legitimate rights of individuals and organizations. In addition, interference with or alteration of data can lead to erroneous decisions in court cases or the work of public authorities, which will have serious consequences for justice and the legal work of these bodies. Therefore, ensuring proper protection of information becomes not only a technical but also a legal issue.

One of the important tasks of the authorities is to create and implement security mechanisms, as well as regular monitoring of information systems, which ensures prompt response to possible threats. To this end, it is important to introduce audit systems and employee training, as well as to establish legal mechanisms to protect information in the digital space. A clear regulatory framework, including legal frameworks for the protection, processing, recovery and use of information, is an important condition for ensuring legal certainty in the event of a data security breach, which will allow for a quick response to incidents and protect the legitimate interests of citizens.

Electronic interaction (e-document flow) between government and judicial authorities requires reliable access to information for all participants in the document flow. Cybercrime, hacking, or technical failures in the system may make it difficult to access critical data, which will negatively affect the enforcement of court decisions and the functioning of the authorities. In order to prevent such situations, it is important to comply with the requirements of the regulations governing the policy of protecting electronic documents and information, which in turn provide for responsibility for the security of information processing.

The use of the latest technologies, such as encryption, biometric authentication, and blockchain, can significantly increase the level of data protection and the efficiency of electronic interaction. An integrated approach to these technologies will ensure the proper functioning of government and judicial authorities, strengthen public confidence in government institutions, and improve the efficiency of the legal process. The introduction of personalized electronic cabinets will contribute to even greater security, rapid exchange of information and ensuring its preservation for a long time.

Key words: *information and communication system, electronic cabinet, electronic document, digital medium, information protection, information integrity, biometric authentication, blockchain, electronic signature.*

Вступ. Захист інформації в системі діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [1]. Він є одним з фундаментальних основ у роботі

органів державної та судової влади. Адже точність і незмінність інформації, що стосується національної безпеки або прав фізичних та юридичних осіб, є основою їх ефективної діяльності. Недостатній захист інформації може призвести до серйозних наслідків, таких як блокування інформації, виток конфіденційних даних, порушення цілісності або зміни даних, що можуть призвести до неправомірних судових рішень.

Неналежний захист даних в роботі державних і судових органах може мати негативні наслідки. Атаки або збої в інформаційних системах можуть блокувати доступ до критично важливих даних, що унеможливить виконання судових рішень та інших функцій органів державної влади. Для запобігання таких ситуацій важливою складовою є надійна і безперебійна робота систем захисту, що гарантують цілісність та конфіденційність інформації.

Зазвичай інформація, що поширюється в електронному вигляді формується за допомогою електронних документів, котрі після створення засвідчуються електронним цифровим підписом автора.

Так відповідно до ст. 5 ЗУ «Про електронні документи та електронний документообіг» встановлено, що електронний документ документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством.

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною [2].

Інноваційні технології, такі як шифрування, біометрична аутентифікація, та блокчейн, здатні значно підвищити рівень безпеки інформаційних систем. Вони дозволяють забезпечити більшу захищеність від несанкціонованого використання інформації з обмеженим доступом і кіберзагроз.

Блокчейн (Blockchain або Block Chain) вибудуваний за певними правилами безперервний послідовний ланцюжок блоків, що містять інформацію. Найчастіше копії ланцюжків блоків зберігаються на безлічі різних комп'ютерів незалежно один від одного. Вперше термін з'явився як назва повністю реплікованої розподіленої бази даних, реалізованої в системі «біткоїнів», через що блокчейн часто відносять до транзакцій в різних крипто валютах, проте технологія ланцюжків блоків може бути поширена на будь-які взаємопов'язані інформаційні блоки [3].

Зокрема криптографічний захист інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо [1]. Так шифрування гарантує, що дані не можуть бути прочитані без відповідного ключа, а біометрична аутентифікація забезпечує додатковий рівень захисту, базуючись на унікальних характеристиках користувача (відбитках пальців, розпізнаванні обличчя і т.д.). Технології блокчейн, завдяки своїй дистрибутивній природі, здатні забезпечити непохитну цілісність даних, що стає важливим аспектом в контексті процесуальної діяльності органів судової влади та державного управління.

Для досягнення високого рівня безпеки необхідно застосовувати комплексний підхід захисту інформації, що включає поєднання технічних, правових і організаційних заходів. Зокрема, важливими є електронні кабінети, які дають змогу індивідуалізувати доступ до персональних даних і забезпечити їх зберігання протягом тривалого часу. Такі системи дозволяють знизити ризики витоку інформації, підвищити зручність і швидкість обміну даними між органами судової та державної влади, а також підвищити рівень довіри до державних та судових установ.

Постановка завдання. Метою статті є аналіз проблем та викликів, пов'язаних з захистом інформації в органах державної та судової влади України, а також оцінка ефективності існуючого правового регулювання і технологічних механізмів безпеки даних. Зокрема,

стаття спрямована на вивчення необхідності розробки єдиного нормативно-правового акта для забезпечення інтеграції сучасних технологій захисту інформації, таких як блокчейн і біометрична аутентифікація, в діяльності державних і судових установ, а також необхідності формулювання рекомендацій щодо вдосконалення правових і технічних стандартів для підвищення рівня безпеки інформації.

Результат дослідження. Незважаючи на важливість забезпечення захисту інформації в органах державної та судової влади, на сьогоднішній день в Україні існує ряд проблем, що стосуються недостатності правових механізмів і технологічних рішень у цій сфері.

Однією з основних проблем є відсутність комплексного регулювання питання захисту інформації в державних органах і судових установах.

Сьогодні існують окремі закони, такі як Закон України «Про захист персональних даних», Закон України «Про захист інформації в інформаційно-комунікаційних системах», Закон України «Про інформацію», але ці нормативно-правові акти не охоплюють повністю всі аспекти захисту інформації в умовах сучасних технологічних викликів. Зокрема, вони не визначають механізмів використання новітніх технологій, таких як блокчейн, біометрична аутентифікація чи шифрування, що є надзвичайно важливим для захисту обігу електронних документів та їхнього змісту в умовах кібернетичних атак.

Електронний документообіг (обіг електронних документів) сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів [2].

Окрім того, відсутність єдиного стандарту для забезпечення безпеки інформаційних систем в органах державної та судової влади, є ще одною з ключових проблем на шляху захисту інформації, котру зможе вирішити впровадження єдиного нормативно-правового акта. Який в свою чергу буде регулювати загальні положення інтеграційної політики сучасних елементів захисту інформації та включати основні положення щодо юридичної визначеності методів захисту даних. Хоча кожен орган може використовувати різні технічні рішення для захисту даних, відсутність єдиних норм і стандартів ускладнює інтеграцію та взаємодію інформаційних систем між різними державними установами. Це створює ризик для ефективного обміну інформацією і може призвести до помилок, а також до порушення прав громадян, зокрема в частині захисту персональних даних.

До прикладу, доступ до електронних документів чи інформації може реалізовуватися за допомогою електронного підпису з одноразовим ідентифікатором як альтернативного методу швидкого отримання відповіді на запит до бази даних щодо конкретного виду інформації, яка розміщена в певних каталогах.

Електронний підпис одноразовим ідентифікатором це дані в електронній формі у вигляді алфавітно-цифрової послідовності, що додаються до інших електронних даних особою, яка прийняла пропозицію (оферту) укласти електронний договір, та надсилаються іншій стороні цього договору (пункт 6 частини 1 статті 3 Закону України «Про електронну комерцію») [4].

Таким чином, наявні правові та технічні недоліки створюють прогалини в захисті інформації, що безпосередньо впливає на ефективність роботи органів державної та судової влади, на довіру громадян до державних інституцій і на безпеку суспільства в цілому.

Відсутність комплексного регулювання питання безпеки даних у державному секторі, зокрема невчасна уніфікації нормативно-правових актів, ускладнює ефективне використання новітніх технологій захисту, таких як блокчейн та біометрична аутентифікація. Це, в свою чергу, негативно впливає на ефективність і стабільність систем електронного документообігу та взаємодії між органами влади, а також на рівень довіри громадян до державних інституцій.

Швидкий розвиток технологій зумовлює створення єдиного законодавчого акта, що комплексно регулював би питання захисту інформації в державних органах і судовій системі. Такий акт повинен враховувати як існуючі, так і перспективні технології, забезпечуючи

правову основу для їх впровадження та використання. Законодавче регулювання має чітко визначити, які методи захисту є обов'язковими, зокрема шифрування, біометричну аутентифікацію та технології, подібні до блокчейн.

Також, метою забезпечення ефективного обміну інформацією між різними державними органами та судами необхідно розробити та впровадити єдині стандарти для обміну даними та взаємодії інформаційних систем. Це дозволить забезпечити оперативний доступ до актуальної інформації, знизить ризики помилок і маніпуляцій з даними, а також підвищить загальну ефективність роботи органів влади. Зокрема технологія блокчейн має великий потенціал для забезпечення цілісності та незмінності даних, тому її використання в органах державної та судової влади повинно стати пріоритетом. Впровадження біометричної аутентифікації також є важливим кроком для підвищення безпеки доступу до критичних даних, що дозволить зменшити ризики несанкціонованого доступу.

Важливо також розробити ефективні системи моніторингу для своєчасного виявлення порушень в інформаційних системах та забезпечення оперативного реагування на них. Створення таких механізмів дозволить мінімізувати наслідки можливих кібератак та інших інцидентів, пов'язаних з порушенням цілісності даних.

Отже враховуючи вищевикладене слід зазначити, що забезпечення ефективного захисту інформації в органах державної та судової влади є ключовим для підтримки правопорядку, стабільності та довіри громадян до державних інституцій. Впровадження єдиного нормативно-правового акта, який охоплював би сучасні технології та забезпечував правову основу для їх застосування, а також інтеграція новітніх технологій захисту даних, таких як блокчейн, біометрична аутентифікація та шифрування, дозволить значно підвищити рівень безпеки інформаційних систем. Комплексний підхід до вирішення цих проблем забезпечить надійний і безпечний обмін інформацією між органами державної та судової влади, що стане запорукою стабільної та ефективної роботи цих інституцій.

Висновки. Забезпечення належного захисту інформації в органах державної та судової влади є критично важливим для ефективного функціонування держави, стабільності правової системи та гарантування прав і свобод громадян. В умовах стрімкого розвитку технологій і зростання кіберзагроз необхідність у вдосконаленні правового регулювання захисту інформації стає все більш очевидною.

Аналіз ситуації показує, що в Україні існує низка проблем у цій сфері. Відсутність єдиного нормативно-правового акта, який би комплексно регулював питання захисту даних у державному секторі, створює прогалини в правовій базі. Крім того, обмежене правове регулювання новітніх технологій, таких як блокчейн і біометрична аутентифікація, не дозволяє ефективно використовувати ці технології для забезпечення безпеки даних в судочинстві та в державних органах. Це спричиняє ризики для цілісності та конфіденційності інформації.

Список використаних джерел:

1. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 №80/94-ВР, редакція від 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

2. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV, редакція від 31.12.2023. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

3. IT-Enterprise, 2025. URL: https://www.it.ua/knowledge-base/technology-innovation/blockchain.

4. Про електронну комерцію: Закон України від 03.09.2015 № 675-VIII, редакція від 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text.