УДК 347.961.1:004.75(477)
DOI https://doi.org/10.32782/pdu.2024.3.52

А. В. Боксгорн
доктор філософії,
старший викладач кафедри адміністративного
права та адміністративного процесу
Одеського державного університету внутрішніх справ

В. С. Мащенко
викладач кафедри адміністративного
права та адміністративного процесу
Одеського державного університету внутрішніх справ

М. Ю. Клейман
кандидат юридичних наук,
завідувач відділення організаційно-аналітичного
забезпечення інституту права та безпеки
Одеського державного університету внутрішніх справ

Д. С. Пастух
спеціаліст з інформаційної безпеки
ТОВ «ФС Груп-Девелопмент»

БЛОКЧЕЙН-ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У СФЕРІ НОТАРІАЛЬНОЇ ДІЯЛЬНОСТІ УКРАЇНИ

Авторами зазначено, що використання децентралізованої архітектури блокчейну усуває централізовані точки вразливості, що значно підвищує стійкість до кібератак та несанкціонованих змін у правових документах. У сфері нотаріату блокчейн сприяє підвищенню прозорості, достовірності нотаріальних дій та довготривалій збереженості реєстраційних записів, що є важливим фактором у правовій практиці. Проведене дослідження спрямоване на розкриття ролі блокчейн-технологій у зміцненні кібербезпеки нотаріальної діяльності, а також надання практичних рекомендацій щодо захисту цифрових реєстрів та правочинів від несанкціонованих змін або втрати інформації. У процесі дослідження застосовано загальнонаукові методи, зокрема методи систематизації, опису, узагальнення та порівняння. Також авторами було проаналізовано правові аспекти інтеграції блокчейну у нотаріальну практику з урахуванням чинного законодавства України та міжнародних стандартів кібербезпеки. Встановлено, що кількість кібератак і кіберзлочинів в Україні постійно зростає, зачіпаючи різні сфери діяльності, включаючи юридичний сектор. Це зумовлює активне впровадження блокчейн-рішень для забезпечення безпеки нотаріальних записів і правочинів. блокчейн-технології можуть стати ключовим елементом у трансформації нотаріальної діяльності в Україні, забезпечуючи її безпечність, прозорість та стійкість до сучасних кіберзагроз. Подальші дослідження у цій сфері мають бути спрямовані на розробку адаптованих алгоритмів аутентифікації, вдосконалення нормативної бази та створення інфраструктури для повноцінного використання блокчейну в юридичній практиці.

Ключові слова: *кіберзагрози, кібератаки, нотаріат, нотаріальна діяльність, криптографічний захист, SSL Stripping, ARP Poisoning, PKI, смарт-контракти.*

Постановка проблеми. У 2008 році анонімна особа або група осіб під псевдонімом Сатоші Накамото представила концепцію розподіленого реєстру, яка згодом отримала назву «блокчейн». У своїй роботі Накамото описав принципи функціонування децентралізованої однорангової (P2P) мережі для здійснення електронних транзакцій без посередництва централізованих установ. Цей протокол, заснований на криптографічних алгоритмах та механізмах консенсусу, забезпечує безпечний, незмінний і конфіденційний обмін цифровими активами. Головною інновацією блокчейну є усунення необхідності довіри між учасниками шляхом математично обґрунтованої верифікації транзакцій. Це дозволяє системі функціонувати без єдиного центру контролю, що мінімізує ризики шахрайства, несанкціонованого доступу та маніпуляцій із даними. Первісно розроблена для криптовалют (зокрема, біткоїна), блокчейн-технологія з часом знайшла широке застосування в різних сферах, зокрема у фінансах, логістиці, охороні здоров'я, державному управлінні та кібербезпеці. В рамках цього дослідження нас цікавить потенціал блокчейн-рішень у сфері нотаріальної діяльності. Використання розподіленого реєстру може суттєво підвищити рівень безпеки нотаріальних дій, мінімізувати ризики підробки документів, забезпечити їхню незмінність та створити прозорий механізм верифікації даних. Завдяки децентралізованій природі блокчейну та застосуванню смарт-контрактів можна автоматизувати процеси реєстрації угод, посвідчення документів і перевірки прав власності, що сприятиме підвищенню ефективності та доступності нотаріальних послуг. Відтак, блокчейн-технологія, що початково була орієнтована на фінансову сферу, поступово інтегрується в юридичний сектор, відкриваючи нові можливості для нотаріальної практики та правового регулювання цифрових активів. Блокчейн-технологія, що спочатку використовувалася у криптовалютах, набуває значення у сфері кібербезпеки, зокрема в нотаріальній діяльності [15]. Зростання кількості складних кібератак, таких як SSL Stripping, ARP Poisoning та APT (Розширена постійна загроза) загрожує конфіденційності та цілісності нотаріальних записів, що потребує надійних механізмів захисту. З урахуванням зростання обсягу електронного документообігу та цифрових підписів, питання безпеки цифрової нотаріальної діяльності стає критично важливим.

SSL Stripping дозволяє зловмиснику примусово змінювати HTTPS-з'єднання на незахищене HTTP, що уможливлює перехоплення конфіденційних даних, таких як особисті дані клієнтів, нотаріальні документи та цифрові підписи. Втрата захищеного з'єднання може призвести до підміни документів або їх фальсифікації, що ставить під загрозу легітимність нотаріальних записів.

ARP Poisoning змінює маршрутизацію трафіку в локальній мережі, що може спричинити перенаправлення даних на підроблені сервери. Це особливо небезпечно для нотаріусів, які працюють із цифровими реєстрами та базами даних, оскільки маніпуляція з трафіком дозволяє зловмисникам отримати несанкціонований доступ до конфіденційної інформації або змінювати документи без відома нотаріуса.

APT – це складний вид кібератаки, при якому зловмисники отримують несанкціонований доступ до інформаційної системи нотаріуса та залишаються непоміченими протягом тривалого часу. На відміну від швидких атак, APT спрямована на викрадення або компрометацію конфіденційних даних, таких як: особисті дані клієнтів, інформація про транзакції з нерухомістю, дані про спадкові справи, цифрові підписи та печатки нотаріуса. Фішингові розсилки часто використовуються як початковий етап APT-атаки. Зловмисники надсилають електронні листи, що маскуються під офіційні повідомлення від державних органів, банків або інших довірених організацій. Ці листи містять шкідливі посилання або вкладення, які дозволяють зловмисникам: встановити шкідливе програмне забезпечення на комп'ютери нотаріуса, отримати доступ до облікових даних, проникнути у внутрішню мережу нотаріальної контори.

Використання блокчейну зменшує ймовірність подібних атак завдяки децентралізованому зберіганню даних, незмінності записів і криптографічному захисту. Блокчейн гарантує, що всі зміни вносяться про-

зоро, а будь-які несанкціоновані модифікації легко виявити. Крім того, застосування смарт-контрактів дозволяє автоматизувати верифікацію даних без посередників, знижуючи ризики компрометації людського фактора. Інтеграція блокчейну з PKI (Public Key Infrastructure) дозволяє підвищити безпеку цифрових підписів і забезпечити автентифікацію користувачів у нотаріальній системі. Використання захищених комунікаційних протоколів, таких як TLS 1.3, а також End-to-end шифрування може зменшити ризик атак SSL Stripping і ARP Poisoning. З огляду на стрімкий розвиток технологій та зростаючу кількість загроз, нотаріуси мають адаптуватися до нових умов і використовувати передові методи захисту інформації.

Блокчейн-технології забезпечують більш високий рівень безпеки порівняно з традиційними централізованими системами, що робить їх перспективним рішенням у боротьбі з кібератаками. Крім того, швидкий розвиток криптографічних методів та нових кіберзагроз вимагає постійного вдосконалення механізмів захисту, що підтверджує необхідність подальших досліджень у цій сфері. Подальші дослідження можуть бути зосереджені на розробці адаптованих алгоритмів блокчейн-аутентифікації та механізмів управління ключами, що забезпечать вищий рівень захисту нотаріальних записів від сучасних кіберзагроз.

Аналіз останніх досліджень і публікацій. Терлюк О. І. у своїй дисертації «Використання технології блокчейн у публічному управлінні: вітчизняний та міжнародний досвід правового регулювання» аналізує правові аспекти впровадження блокчейн у публічному секторі, включаючи нотаріат. Він зазначає, що використання блокчейн-технологій може сприяти підвищенню довіри до державних інституцій та забезпечити надійність зберігання даних [14]. Василенко М. Є. у своїй публікації «Використання технології блокчейн у нотаріальній діяльності» аналізує особливості впровадження блокчейн у нотаріальну практику України. Автори наголошують, що ця технологія сприяє підвищенню рівня безпеки та прозорості нотаріальних процесів, знижуючи ризики підробки документів і несанкціонованого доступу до даних, зокрема, з урахуванням зарубіжного досвіду [2]. Спасітєлєва С. О., Бурячок В. Л. у роботі «Перспективи розвитку додатків блокчейн в Україні» аналізують сучасний стан розвитку блокчейн-технологій та їх потенціал у різних сферах, включаючи нотаріальну діяльність. Вони відзначають, що блокчейн може забезпечити безпеку та ефективність нотаріальних послуг, проте для його впровадження необхідно подолати низку технічних та правових викликів [13]. Загалом, дослідження підтверджують, що впровадження блокчейн-технологій у нотаріальну діяльність України має значний потенціал для підвищення кібербезпеки, прозорості та ефективності нотаріальних процесів. Однак, для реалізації цього потенціалу необхідно розробити відповідну нормативно-правову базу та забезпечити технічну готовність інфраструктури.

Метою статті є визначення того, як технологія блокчейн може бути використана для зміцнення кібербезпеки, а також надання практичних рекомендацій для захисту блокчейн-систем від потенційних загроз та мінімізації їх наслідків.

Виклад основного матеріалу. Аналіз поточного стану кіберзлочинності в Україні свідчить про суттєве зростання кількості кіберінцидентів та кібератак у 2023 році. За даними оперативного центру реагування на кіберінциденти Державного центру кіберзахисту (ДЦКЗ), кількість зареєстрованих кіберінцидентів зросла на 62,5% порівняно з попереднім роком. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (далі – ДЦКЗ Держспецзв’язку) Протягом 2023 року за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було:

– опрацьовано 18 мільярдів подій, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки;

– детектовано 133 мільйони підозрілих подій ІБ (при первинному аналізі);

– опрацьовано 148 тисяч критичних подій ІБ (потенційні кіберінциденти, вияв-

лені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу);

– зафіксовано та оброблено безпосередньо аналітиками безпеки 1105 кіберінцидентів. Кількість зареєстрованих кіберінцидентів зросла на 62.5% порівняно з попереднім роком [11]. Див. рис. 1.

– Також протягом 2023 року до Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом звітного періоду було підключено 24 нових об’єктів кіберзахисту, що належать до урядового (22), енергетичного (1) та військового (1) секторів.

Рис. 1. Кількість кіберінцидентів

Також протягом 2023 року до Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом звітного періоду було підключено 24 нових об’єктів кіберзахисту, що належать до урядового (22), енергетичного (1) та військового (1) секторів. Особливої уваги заслуговують кібератаки, пов'язані з розповсюдженням шкідливого програмного забезпечення. ДЦКЗ спільно з Unit 42 Palo Alto Networks провів дослідження щодо поширення шкідливого ПЗ SmokeLoader в Україні у період з травня по листопад 2023 року. Дослідження сфокусовано на відслідковуванні розповсюдження SmokeLoader в Україні у період з травня по листопад 2023 року. За цей період зафіксовано значне зростання атак, пов’язаних із застосуванням цього програмного забезпечення, на державний, оборонний та фінансовий сектори (у звіті проаналізовано 23 хвилі фішингових атак). SmokeLoader, також відомий як Dofoil або Sharik, є завантажувачем для доставки додаткового шкідливого програмного забезпечення на інфікований комп'ютер, який управляється операційною системою Windows. Атаки з його використанням здійснюються щонайменше з 2011 року.

Цей інструмент найчастіше використовують для атак на фінансові установи російські хакери, яких Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA атрибутує за ідентифікатором UAC-0006. Проте кіберзлочинці не обмежуються виключно фінансовим сектором, демонструючи стратегію диверсифікації своїх цілей з метою максимізації потенціалу прибутку [3].

Окрім державної компанії, існує широкий спектр українських та міжнародних компаній, чия діяльність зосереджена на моніторингу та документуванні кіберзагроз, спрямованих як проти України, так і проти її міжнародних партнерів. Цей розгалужений мережевий фронт, що об'єднує зусилля численних організацій, відіграє критично важливу роль у забезпеченні кібербезпеки в умовах ескалації цифрових конфліктів.

На сьогодні в Україні вже ведуться обговорення щодо можливості впровадження блокчейну у нотаріальну діяльність. У 2021 році Міністерство цифрової трансформації України ініціювало розробку законопроєктів щодо цифрової трансформації юридичних процесів, включно з використанням блокчейн-рішень.

Та незважаючи на відсутність окремого законодавчого акту, що прямо регулює використання блокчейн-технологій, кібербезпека в Україні забезпечується комплексом законодавчих та організаційних заходів, серед яких є: «Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV регулює використання електронних документів та документообігу, що є основою для цифровізації нотаріальних процесів [7], Закон України «Про електронні довірчі послуги» від 5 жовтня 2017 року № 2155-VIII встановлює правові засади надання електронних довірчих послуг, включаючи електронний підпис, що є важливим для впровадження блокчейн-технологій у нотаріальній діяльності

[6], Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII визначає правові та організаційні основи державної політики у сфері кібербезпеки, спрямованої на захист життєво важливих інтересів громадян, суспільства та держави в кіберпросторі [8]. Блокчейн-технології також можуть бути впроваджені в електронну комерцію, видавничу справу та страхування. За прогнозами, до 2030 року світовий ринок блокчейн-технологій досягне 1 432 мільярдів доларів, а середньорічний темп зростання становитиме 85,9% у період з 2022 по 2030 рік [12]. Блокчейн-технології мають значний потенціал для впровадження в різні сфери діяльності в Україні. У сфері державного управління блокчейн може забезпечити прозорість та контроль за державними активами. Зокрема, планується переведення державних реєстрів, соціальних служб, органів безпеки, охорони здоров'я та енергетики на блокчейн-платформу, що дозволить уряду контролювати всі зміни, пов'язані з державними активами. [1].

Зростання інтересу до блокчейн-технологій у фінансовій сфері спостерігається по всьому світу, що стимулює розвиток інноваційних рішень. Ця технологія стає ключовим елементом у створенні децентралізованих систем прямих (P2P) платежів, здатних підвищити стабільність фінансових ринків. Блокчейн вирізняється тим, що надає компаніям та організаціям децентралізовану, захищену та прозору платформу. В умовах посилення автоматизації робочих процесів блокчейн виступає каталізатором цифрової трансформації в різних галузях. Технологія вже активно застосовується в таких сферах, як:

– цифрові платежі;
– смарт-контракти;
– управління активами;
– цифрова ідентифікація.

У сфері цифрових платежів блокчейн дозволяє скоротити час обробки та вартість транзакцій. Смарт-контракти, у свою чергу, забезпечують створення безпечних та прозорих умов для укладання угод [4].

У сфері нотаріальної діяльності блокчейн-технології можуть забезпечити підвищення безпеки, прозорості та зменшення ризиків шахрайства. Використання децентралізованого реєстру дозволяє нотаріусам фіксувати юридично значущі дії, що унеможливлює підробку документів і стороннє втручання [9].

Основні можливості блокчейн для нотаріату:

– Цифрова верифікація документів. Блокчейн дозволяє перевіряти справжність та незмінність документів без необхідності звертатися до посередників.

– Автоматизація нотаріальних процесів. Завдяки смарт-контрактам можна автоматично виконувати угоди та зменшити кількість рутинних процедур.

– Захист від підробок та шахрайства. Усі записи, внесені до блокчейн-реєстру, є незмінними, що унеможливлює фальсифікацію правочинів.

– Розширення електронного нотаріату. Блокчейн-технології можуть використовуватися для створення цифрових підписів та електронних архівів.

В деяких країнах блокчейн-технології активно впроваджуються в нотаріальну практику різних країн, забезпечуючи підвищення прозорості, безпеки та ефективності юридичних процесів. Розглянемо досвід Естонії, Швейцарії та Японії Естонія є піонером у впровадженні цифрових технологій у державне управління. У цій країні функціонує єдиний державний реєстр, який об'єднує всі необхідні дані, що дозволяє нотаріусам оперативно отримувати інформацію та здійснювати нотаріальні дії. Це забезпечує швидкість та надійність нотаріальних послуг, мінімізуючи можливості для шахрайства [12]. Швейцарія активно досліджує та впроваджує блокчейн-технології у фінансовому секторі та державному управлінні. Хоча конкретних даних про використання блокчейну в нотаріальній діяльності Швейцарії в наданих джерелах немає, країна відома своїм прогресивним підходом до цифровізації та інновацій. Це створює передумови для потенційного впровадження блокчейн-рішень у різні сфери, включаючи нотаріат. Японія активно досліджує можливості впровадження цифрових валют центрального банку та інших фінтех-інновацій. Спільний проект Банку Японії та Європейського центрального

банку свідчить про зацікавленість країни у використанні блокчейн-технологій. Хоча конкретних даних про застосування блокчейну в нотаріальній сфері Японії немає, загальна тенденція до цифровізації може сприяти впровадженню цієї технології в майбутньому [10].

Таким чином впровадження технології блокчейн у нотаріальну практику відкриває шлях до суттєвого підвищення ефективності та надійності роботи нотаріусів в Україні, сприяючи розвитку електронного нотаріату. Ця інтеграція дозволить:

– Оптимізувати витрати та скоротити часові затрати на здійснення нотаріальних дій, що підвищить доступність послуг для громадян.

– Зміцнити довіру до цифрових угод, забезпечивши незмінність та прозорість транзакцій.

– Спростити процедуру верифікації автентичності документів та правочинів, мінімізуючи ризики фальсифікації.

Висновки. Блокчейн-технології демонструють значний потенціал у забезпеченні кібербезпеки нотаріальної діяльності в Україні. Аналіз показав, що традиційні централізовані системи, які використовуються для збереження та обробки нотаріальних записів, мають численні вразливості перед сучасними кіберзагрозами, такими як SSL Stripping, ARP Poisoning, фішингові атаки та розширені постійні загрози (APT). Використання блокчейну усуває ці ризики завдяки таким ключовим властивостям, як децентралізація, незмінність даних та криптографічний захист. Запропонований підхід до інтеграції блокчейну в нотаріальну практику передбачає створення захищеної розподіленої бази даних для нотаріальних документів, що мінімізує ризики їх підробки або несанкціонованого доступу. Застосування смарт-контрактів дозволяє автоматизувати юридично значущі процеси, такі як реєстрація правочинів та перевірка автентичності документів. Це сприяє підвищенню ефективності нотаріальної діяльності та зменшенню адміністративного навантаження на нотаріусів. З огляду на правові аспекти, впровадження блокчейну в нотаріальну діяльність потребує відповідного нормативно-правового врегулювання. Аналіз законодавства України свідчить про необхідність адаптації чинних норм для забезпечення юридичної сили блокчейн-записів та їх використання у судовій практиці. Крім того, важливим напрямом подальших досліджень є розробка механізмів ідентифікації та аутентифікації учасників нотаріальних дій на основі інфраструктури відкритих ключів (PKI) у поєднанні з блокчейн-рішеннями. Використання передових методів криптографічного захисту та сучасних технологій, зокрема протоколів TLS 1.3 та шифрування end-to-end, сприятиме захисту цифрових підписів і нотаріальних реєстрів від атак. Це дозволить не лише підвищити рівень безпеки, а й сформувати новий рівень довіри до нотаріальних послуг серед громадян та бізнесу.

Отже, блокчейн-технології можуть стати ключовим елементом у трансформації нотаріальної діяльності в Україні, забезпечуючи її безпечність, прозорість та стійкість до сучасних кіберзагроз. Подальші дослідження у цій сфері мають бути спрямовані на розробку адаптованих алгоритмів аутентифікації, вдосконалення нормативної бази та створення інфраструктури для повноцінного використання блокчейну в юридичній практиці.

Список використаної літератури:

1. Акімова Л. М. Застосування блокчейн технологій у публічному управлінні *Науковий вісник «Демократичне врядування».* 2017. Вип.20
2. Василенко, М. Є. Використання технології «блокчейн» у нотаріальній діяльності. *Правова наука і державотворення в Україні в контексті інтеграційних процесів*: матеріали XIV Міжнар. наук.-практ. конф. (м. Суми, 19-20 трав. 2023 р.). Суми, 2023. С. 80– 82 URL: https://dspace.univd.edu.ua/handle/123456789/17537
3. Державна служба спеціального зв'язку та захисту інформаціїї України. URL: https://cip.gov.ua/ua/news/derzhavnii-centr-kiberzakhistu-spilnoz-unit-42-palo-alto-networks-proviv-doslidzhennya-shkidlivogo-programnogo-zabezpechennya-smokeloader?utm_source=chatgpt.com
4. Електронний журнал «Ефективна економіка» 2023. No 12. URL: https://nayka.com.ua/index.php/ee/issue/view/119

5. Електронний ресурс, компанії в сфері кібербезпеки Onapsis URL: https://onapsis.com/category/resources/case-studies/
6. Закон України «Про електронні довірчі послуги» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.400**)** URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text
7. «Закон України «Про електронні документи та електронний документообіг» (Відомості Верховної Ради України (ВВР), 2003, № 36, ст.275) URL: https://zakon.rada.gov.ua/laws/show/851-15#Text
8. Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
9. Захарко В. А. Застосування технологій блокчейн у фінансових розрахунках: кваліф. магістерська робота: 072 / Львівський національний університет ім. І. Франка. Львів, 2023. 78 с. URL: https://econom.lnu.edu.ua/wp-content/uploads/2024/11/Zakharko-V.pdf?utm_source=chatgpt.com
10. Збірник тез звітної наукової конференції Львівського національного університету імені Івана Франка за 2023 рік (електронне видання) : Секція факультету управління фінансами та бізнесу, (Львів, 1-8 лютого 2024 р.). Львів : ЛНУ ім. І.Франка, 2024. 332 с. URL: https://financial.lnu.edu.ua/wp-content/uploads/2024/10/ZBIRNYK_ZVITNA-KONF._2024.pdf?utm_source=chatgpt.com
11. Звіт про роботу системі виявлення вразливостей і реагування на кіберінциденти та кібератаки. 2023 URL: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a
12. Молодь і наука: сучасний стан, проблеми та перспективи розвитку права в Україні: Матеріали Всеукраїнської науково-практичної конференції аспірантів, студентів, молодих учених. м. Київ, 17 травня 2024 р. / За ред. проф. Івчук Ю.Ю. – Київ: вид-во Східноукраїнського національного університета ім. В. Даля, 2024. 270 с. URL:https://snu.edu.ua/wp-content/uploads/2024/08/m_n_s_2024.pdf?utm_source=chatgpt.com
13. Спасітєлєва С. О., В. Л. Бурячок Перспективи розвиткудодатків блокчейн в Україні. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2018. №1(1) С. 35-48 URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/18?utm_source=chatgpt.com
14. Терлюк О. І. Використання технології блокчейн у публічному управлінні: вітчизняний та міжнародний досвід правового регулювання: дис…доктора філософії: 081 / НУ «Львівська політехніка». Львів, 2023. 248 с. URL: https://lpnu.ua/sites/default/files/2023/radaphd/25126/disertaciyaterlyuk.pdf?utm_source=chatgpt.com
15. W.Mougayar, "The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology," NewYork, USA, JohnWiley& SonsInc., 2016.

Bokshorn A., Mashchenko V., Kleiman M., Pastukh D. Blockchain technologies as a tool for ensuring cybersecurity in the field of notarial activities in Ukraine

The authors note that the use of the decentralized blockchain architecture eliminates centralized points of vulnerability, which significantly increases the resistance to cyberattacks and unauthorized changes to legal documents. In the field of notary, blockchain contributes to increased transparency, reliability of notarial acts and long-term preservation of registration records, which is an important factor in legal practice. This study aims to reveal the role of blockchain technologies in strengthening the cybersecurity of notarial activities, as well as to provide practical recommendations for protecting digital registers and transactions from unauthorized changes or loss of information. The study used general scientific methods, including methods of systematization, description, generalization and comparison. The authors also analyzed the legal aspects of integrating blockchain into notarial practice, taking into account the current legislation of Ukraine and international cybersecurity standards. It has been established that the number of cyberattacks and cybercrimes in Ukraine is constantly growing, affecting various areas of activity, including the legal sector. This leads to the active implementation of blockchain solutions to ensure the security of

notarial records and transactions. blockchain technologies can become a key element in the transformation of notarial activities in Ukraine, ensuring its security, transparency and resilience to modern cyber threats. Further research in this area should be aimed at developing adapted authentication algorithms, improving the regulatory framework, and creating an infrastructure for the full use of blockchain in legal practice.

Key words: *cyber threats, cyber attacks, notary, notarial activity, cryptographic protection, SSL Stripping, ARP Poisoning, PKI, smart contracts.*