УДК 004.056

Л.В. Астахова, Н.В. Калязин

Невзаимозаменяемые токены (NFT) как средство и объект обеспечения информационной безопасности

Показано использование невзаимозаменяемых токенов как криптографических активов с поддержкой блокчейна, которые представляют собой доказательства владения цифровыми объектами. Обоснован их большой потенциал как средства защиты разных видов информации, способного гарантировать ее конфиденциальность, целостность и доступность. Выделены проблемы обеспечения безопасности невзаимозаменяемых токенов и предложены пути их решения.

Ключевые слова: *блокчейн, кибербезопасность, криптобезопасность, криптовалюта, невзаимозаменяемые токены (NFT), информационная безопасность, защита информации, конфиденциальность, целостность, доступность, персональные данные, врачебная тайна*

DOI: 10.36535/0548-0027-2022-06-3

ВВЕДЕНИЕ

В последнее время невзаимозаменяемые токены (*Non-FungibleTokens – NFT*) приобрели широкое распространение как уникальные токены, работающие на блокчейне [1] и представляющие собой доказательства владения цифровыми объектами [2]. Каждый из них содержит определенное количество данных, которые уникальны для данного токена. *NFT* были созданы в 2010 г., а первые проекты с их использованием вышли в 2017 г. на платформе *Ethereum*. Основную же популярность эта технология получила в 2021 г., когда в форме *NFT* начали массово продавать цифровые файлы [3]. Блокчейн – это разновидность распределенного реестра (*Distributed Ledger Technology – DLT*), технология которого позволяет вести учет на нескольких узлах [4]. Благодаря данной технологии и получили свое развитие невзаимозаменяемые токены.

Согласно аналитическим данным центра *DappRadar*, сегодня популярность *NFT* резко возросла, что сопровождалось повышением объемов торговли ими, достигшей $22 млрд в 2021 г. по сравнению с $100 млн в 2020 г. [5]. По данным аналитической группы *Chainalysis*, на конец 2021 г. объем мирового *NFT*-рынка составлял $40,9 млрд. Несколько крупных исследователей рынка, в их числе *Morgan Stanley*, прогнозируют к 2030 г. рост *NFT*-рынка до $240 млрд и более. В этом случае российская доля может составить около $10 млрд [6].

Стремительное развитие *NFT*, их внедрение в разные сферы деятельности актуализируют их рассмотрение в контексте информационной безопасности. Цель настоящей статьи – показать перспективы *NFT* как средства обеспечения безопасности защищаемой информации и обосновать пути защиты этой технологии.

НЕВЗАИМОЗАМЕНЯЕМЫЕ ТОКЕНЫ КАК СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ

Защита информации представляет собой ряд правовых, организационных и технических мер, направленных на: 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий; 2) соблюдение конфиденциальности информации ограниченного доступа; 3) реализацию права на доступ к информации[1]. Технология *NFT* открывает возможности для реализации всех названных целей: целостности, конфиденциальности и доступности информации.

В обеспечении целостности информации. На данный момент технология *NFT* нашла применение преимущественно в сфере искусства. Сегодня уже реализуются возможности галерей, музеев, вернисажей,

[1] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 30.12.2021) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2022). – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 30.04.2022).

создающих *NF*-объекты. Так, Государственный Эрмитаж уже продал *NFT* картин в виде цифровых копий на общую сумму свыше 32 млн рублей [7]. Однако потенциал этих технологий значительно шире. *NFT* порождают новые способы организации, потребления, перемещения, программирования и хранения цифровой информации, определяют быстрый рост различных адаптаций в сфере искусства, спорта, вещания, создания контента и технологического криптобизнеса, а также они способны разрушить определенные сложившиеся системные элементы на существующих рынках, таких как недвижимость, юридическая отрасль и др. Эксперты ожидают, что *NFT* будут продолжать расширяться как инновационная сила во многих технологических и бизнес-предприятиях и пользоваться большой популярностью у создателей и потребителей [8].

Невзаимозаменяемые токены способны защитить URL-адреса пользователей сайтов. URL-адрес может существенно повлиять на маркетинг сайта и его товаров. В связи с ограниченным количеством доступных расширений адресов определенные доменные имена стали очень дорогими. Поэтому некоторые пользователи занимаются «перехватом доменов»: ждут, пока истечет срок регистрации популярных доменных имен, затем торопятся перекупить адрес, прежде чем владелец узнает, что произошло. По словам генерального директора компании *UnstoppableDomains*, теперь можно купить или зарегистрировать доменное имя в качестве *NFT* на блокчейне и хранить его в своем криптокошельке вместо того, чтобы получать его у регистратора, такого как *NetworkSolutions* или *GoDaddy* [9].

В обеспечении конфиденциальности информации. Несмотря на то, что в мире накоплен большой опыт защиты персональных данных, именно они по-прежнему являются доминирующим типом утекшей информации. Если в 2018 г. утечки персональных данных составляли 70,9% от общего числа утечек, то в 2021 г. эта цифра выросла до 83,1% [10]. В России этот процесс регулируется Федеральным законом "О персональных данных" от 27.07.2006 N 152-ФЗ[2]. Однако утечек персональных данных не становится меньше – их доля составляет более 86% [11]. Поэтому неслучайно на рассмотрении в Госдуме сегодня находится законопроект № 101234-8 «О внесении изменений в Федеральный закон "О персональных данных" и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных»[3]. Эксперты обращают внимание на то, что это будет крупнейшая реформа законодательства о персональных данных за последние 10 лет, согласно которой все операторы персональных данных обязаны будут подключиться к Государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и сообщать в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) в течение 24-х часов о каждой утечке информации [12], поэтому и техническая защита персональных данных также должна будет усиливаться.

В последние годы в тройку «лидеров» по утечкам информации в мире стабильно входят организации сфер здравоохранения [11], традиционно связанные с проблемами защиты персональных данных и врачебной тайны [13]. Поэтому и ученые, и специалисты-практики все больше внимания обращают на использование в этой отрасли технологий *NFT* и высоко оценивают перспективы использования невзаимозаменяемых токенов (*NFT*) в качестве актива безопасности для пациента [14]. По их мнению, если не принять участие в цифровой революции, то практика скоро устареет. В этом процессе крайне важно огромным объемом цифровых данных (сведения о пациентах, хирургические видеоматериалы и т. д.) управлять с максимальным вниманием к безопасности и цифровой конфиденциальности, что Организация Объединенных Наций считает правом человека [15, 16]. В США внедрение технологии невзаимозаменяемых токенов в здравоохранение уже началось с личных электронных медицинских записей, которые будут безопасно храниться, передаваться и проверяться на предмет безопасности. По мнению экспертов, эта технология может оказаться неоценимой для сообщества трансплантантов стволовых клеток. Продвижение продуктов гемопоэтических стволовых клеток, включая костный мозг, стволовые клетки периферической крови, продукты пуповинной крови и продукты клеточной терапии, от вены донора до конечного пункта назначения, представляет собой сложную серию регуляторных, логистических и медицинских процессов. Чтобы обеспечить безопасность этой сложной жизненно важной цепочки трансплантации стволовых клеток, в систему вводятся многочисленные входные данные, начиная от набора доноров и заканчивая постинфузионным мониторингом. Все это происходит в различных медицинских лабораториях, а вся цепочка трансплантации стволовых клеток требует огромного количества разнообразных дискретно разрозненных исходных и выходных данных. Сейчас это не дает возможности специалистам в области здравоохранения оперативно отслеживать и исследовать безопасность и эффективность медицинских операций. Использование *NFT* позволит просматривать данные о донорстве стволовых клеток в режиме реального времени, выявляя неэффективность в цепочке трансплантации [17].

Еще одним вариантом использования *NFT* в здравоохранении является токенизация крови – от идентификации донора, температуры донорской крови в пути, точек местоположения *GPS* из лаборатории в больницу и, наконец, сохранения в медицинской карте пациента, получающего переливание. Кровь токенизируется с помощью штрих-кода, который сканируется в течение всего процесса, создавая обновления в режиме реального времени, доступные для просмотра необходимым сторонам. Путем токенизации крови в блокчейне можно точно отслеживать инвентариза-

[2] КонсультантПлюс – URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 30.04.2022)

[3] О внесении изменений в Федеральный закон "О персональных данных" и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных. – URL: https://sozd.duma.gov.ru/bill/101234-8 (дата обращения: 30.04.2022).

цию донорской крови, выявлять нехватку конкретных групп крови в регионах, а также предотвращать человеческие ошибки [18]. Зарубежные эксперты весьма оптимистично оценивают перспективы технологии невзаимозаменяемых токенов для трансплантации стволовых клеток и переливания крови. Это подтверждают и прогнозы развития рынка блокчейнов для здравоохранения: к 2025 г. он составит 3,4 млрд долл. [19].

В обеспечении реализации права на доступ к информации. Технологии невзаимозаменяемых токенов применяют и в защите иных логистических решений, и операций, позволяющих обеспечить реализацию права на доступ к информации. Так, в Италии производят высококачественную обувь элитного бренда с присвоенным ей *NFT*, который производитель предлагает отсканировать на упаковке. Покупатель с помощью этого токена сможет узнать, где и когда была создана данная пара обуви. По мере перемещения посылки до пункта доставки токен сканируется для добавления новой информации о её статусе: местоположении склада, времени отправления и прибытия. Как только посылка будет доставлена в пункт назначения, магазин должен отсканировать ее и отметить доставку [20]. В результате покупатель получает подтверждение подлинности товара, а также подробную информацию о его доставке.

Имеется множество гипотетических возможностей введения технологии *NFT* в процесс доставки товаров, но для любого из них необходимо использовать одну и ту же систему на всех этапах цепочки поставок. Вследствие большого количества участников процесса реализовать эту идею в реальной жизни бывает достаточно сложно. В связи с этим сейчас использование *NFT* в подобных сферах распространяется медленно. Два примера крупных логистических решений с использованием блокчейна – это системы *TradeLens* от *MAERSK* и *FootTrust* от *IBM*. Они уже используют *HyperledgerFabric* – блокчейн *IBM* с поддержкой *NFT* [21].

NFT КАК ОБЪЕКТ ЗАЩИТЫ ИНФОРМАЦИИ

Стремительное развитие технологии невзаимозаменяемых токенов и перспективы ее использования для защиты информации актуализируют вопрос рисков кибербезопасности и криптобезопасности этой технологии. Угрозы безопасности *NFT* во многом идентичны рискам, присущим криптовалюте. *NFT* могут представлять собой объект кражи так же, как и взаимозаменяемые монеты. Новизна данной технологии обусловливает необходимость выявления проблем безопасности *NFT* и выработки предложений по их решению. На это обращают внимание эксперты, высказывая опасения по поводу законного владения активами *NFT* и распространения мошенничества, связанного с торговлей ими [2].

Злоумышленники являются частью любой системы или решения, блокчейн ничем не отличается. Они могут угрожать безопасности *NFT*-платформ и самим пользователям. Ландшафт *NFT*-угроз включает в себя «классические» проблемы, связанные не только с фишингом, но и с безопасностью на стороне посредника — торговой площадки или биржи.

Проанализировав проблемы безопасности, связанные с невзаимозаменяемыми токенами, мы сгруппировали их по причинам угроз: правовой статус (юридическая неопределенность регулирования технологии), человеческий фактор (угрозы, связанные с низкой технической и финансовой грамотностью пользователей) и хакерские угрозы (угрозы, связанные с внешними атаками). Рассмотрим их подробнее.

Неопределенность правового статуса. Осложняет вопрос безопасности невзаимозаменяемых токенов их юридическая неопределенность, что представляет собой угрозу правового характера. В России с точки зрения права они никак не подкреплены, их нельзя отнести к цифровой валюте, которая регламентируется ФЗ № 259[4]. В настоящий момент к *NFT* в России предлагается применять положения, касающиеся цифровых прав согласно ст. 128 и 141.1 ГК [22, 23]. Эти положения регламентируют гражданские права, но помимо них необходимо руководствоваться правом на интеллектуальную собственность и правом на оборот вещей. Эксперты [24] обосновывают необходимость использования возможностей *NFT* для токенизации объектов авторского права, для предотвращения мошенничества и плагиата, а также для контроля за исполнением финансовых операций.

В США и Европе вопрос применения токенов также остается открытым, несмотря на более раннее их появление в этих странах. Законодательство в этой сфере не проработано, единого подхода к решению проблемы нет. Если невзаимозаменяемый токен создаётся и в последующем продаётся с целью извлечения выгоды, т. е. для предпринимательской деятельности, то к таким правоотношениям применим Закон США «О ценных бумагах», а если он продаётся без цели извлечения прибыли, то этот закон не применим [8]. Поэтому если возникнет конфликт и регуляторы сочтут *NFT* незарегистрированной ценной бумагой, то владельцы токенов будут вынуждены платить высокие штрафы.

Человеческий фактор. Анализ форумов и отчетов показал, что одной из наиболее распространенных проблем безопасности токенов является фишинг. Постоянно в соцсетях и иных платформах из-за фишинга теряют свои сбережения тысячи пользователей, а суммы исчисляются миллионами долларов. Например, нью-йоркский поклонник цифрового искусства потерял 15 токенов на общую сумму $2,2 млн [25]. В результате фишинга преступники получают доступ к кошельку жертвы, они могут перевести хранящиеся в нём токены себе. Учитывая односторонний и децентрализованный характер блокчейн-транзакций, вернуть украденное будет весьма тяжело.

Немаловажная проблема – это подделка самого токена, т. е. приобретение его цифровой копии. Многие пользователи с этим столкнулись. Например, некий хакер подделал *NFT* от *Beeple*, проданный за $69,3 млн [26].

[4] Федеральный закон "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации" от 31.07.2020 N 259-ФЗ // КонсультантПлюс – URL: http://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 04.05.2022).

Серьезным вызовом безопасности для платформ и пользователей стало использование идентичных URL-адресов изображений. Некоторые фальшивые *NFT* указывают на существующие активы, т. е. они копируют *mage_url* настоящих *NFT*. Если покупатель посмотрит на внешний вид лотов и не проверит их подлинность, то он может ошибочно принять их за оригиналы.

Фактор, связанный с внешними атаками. Дополнительный риск сопряжен с самим процессом торговли невзаимозаменяемыми токенами. Зачастую маркетплейс требует перевода *NFT* в свой собственный кошелёк для условного депонирования [27]. Подобные операции осуществляются вне цепочки блокчейна и непрозрачны для владельца актива. Нарушение принципа децентрализации создаёт угрозы как для продавца, так и для покупателя, которые должны безусловно доверять торговой платформе, исполняющей посреднические операции. Если программное обеспечение биржи будет скомпрометировано, то злоумышленники получат возможность вмешаться в операции с токенами.

Проблема хакерства включает в себя атаки на блокчейн, используемый в основе *NFT*. Так, в 2021 г. хакер атаковал сайдчейн *Ronin*, который используется в игре *Axie Infinity* и похитил 5 тыс. единиц *Ethereum* [28].

Помимо этого, токены сами по себе могут нести угрозу. По данным *ESET*, взаимозаменяемые токены в 2021 г. стали одним из основных механизмов распространения вредоносных программ для нелегального майнинга или кражи криптовалюты [29]. Немаловажно, что Россия по итогам этого года стала лидером по числу пострадавших от атак, связанных с криптовалютой. На страну пришлось 11,2% мирового количества пострадавших от краж.

В целом невзаимозаменяемые токены имеют такое же количество и разновидности угроз, как и любая информационная инфраструктура, и так же, как и во многих системах, от них самих могут исходить угрозы. Опасность могут таить кошельки и маркетплейсыдля управления своими активами, почты и прочие сайты с вредоносным ПО и ссылками. Однако от разного рода проблем можно себя частично обезопасить.

Базовой рекомендацией безопасности активов невзаимозаменяемых токенов является надежность пароля. Предпочтительнее всего использовать длинный пароль, состоящий из случайных символов, такие генерации могут автоматически составлять Яндекс или *GoogleChrome*. Помимо обычного пароля необходимо применять многофакторную аутентификацию. Как показывает статистика различных платформ, 99,9% взломанных пользователей не используют многофакторную аутентификацию (*MFA*) [30].

Немаловажна и надежность сохранности кодового слова. Его не нужно хранить в облачных хранилищах или на иных электронных устройствах из-за соображений безопасности. Лучше всего для этого использовать бумажный носитель, который предполагает чередование слов.

Необходима установка безопасного подключения к сети. Это связано с тем, что использование общедоступного *Wi-Fi* упрощает злоумышленникам кражу данных. Помимо безопасных сетей желательно, чтобы пользователи в целях безопасности *NFT* использовали проверенные *VPN*-сервисы и прочие приложения для шифрования своего интернет-трафика и скрытия *IP*-адресов для защиты всех действий, связанных с покупкой, продажей и управлением несменяемыми токенами [31].

Регулярное обновление программного обеспечения способствует повышению безопасности. Актуально своевременно обновлять ПО или поставить автообновление, так как зачастую это включает в себя исправление существующих ошибок безопасности.

Во избежание кражи самого токена при взломе учетной записи рекомендуется использовать улучшенную архитектуру нулевого доверия. Такой способ адекватен решением проблемы до ее возникновения из-за использования структур нулевого доверия, основанных на подтверждении личности. Существует возможность ограничивать количество привилегированных пользователей, имеющих доступ к токенам, тем самым снижая риск потери активов.

Целесообразно также применять инструменты мониторинга сети, которые помогут выявлять возможные проблемы с утечкой до того, как произойдет доступ к блокчейну [32]. Помимо простых инструментов аутентификации к решениям для активного поведенческого мониторинга и анализа пользователь имеет возможность завершать потенциально проблемные сеансы, не давая злоумышленникам добраться до токенов. Введение единых стандартов на *NFT*-токены [33] позволило бы повысить уровень безопасности этой перспективной технологии.

Проверка *NFT* на подлинность различными методами перед покупкой – еще один способ обеспечения безопасности. Это связано с тем, что существует вероятность цифровой подделки. Вернуть потраченные средства будет достаточно сложно из-за блокчейн-технологий и юридической неопределенности невзаимозаменяемых токенов. Отсюда вытекает необходимость ускорения законодательного решения данного вопроса, а также повышения финансовой грамотности и культуры кибербезопасности пользователей в процессе работы с *NFT*.

ВЫВОД

Резкий скачок популярности технологии невзаимозаменяемых токенов, прогнозы экспоненциального роста мирового и российского рынков этой технологии, ее стремительное проникновение во все сферы деятельности человека – все это позволяет констатировать большой потенциал *NFT* для защиты информации: обеспечения конфиденциальности, целостности и доступности персональных данных, а также всех видов профессиональной (врачебной, страховой и др.), служебной и коммерческой тайн. Уже вполне осязаемые черты приобрели технологии использования *NFT* для защиты персональных данных и врачебной тайны в зарубежном здравоохранении, для реализации права на доступ к информации.

С точки зрения информационной безопасности невзаимозаменяемые токены должны рассматриваться не только как средства, но и как объект защиты.

Рынок *NFT* – весьма перспективный и быстро развивающийся, но и достаточно рискованный. Новизна данной технологии в России и за рубежом делает ее более уязвимой для атак. Проблемы безопасности *NFT* целесообразно дифференцировать по признаку источников угроз их информационной безопасности и выделить правовые проблемы, а также проблемы, связанные с человеческим фактором и злоумышленными внешними воздействиями. Обоснованные в настоящей статье рекомендации по решению проблем безопасности *NFT* включают в себя классические средства защиты информации: правовые, организационные и технические. Они направлены на обеспечение всех целей защиты информации: конфиденциальности, целостности и доступности. Только комплексный подход позволит гарантировать сохранность *NFT*, надежность используемых маркетплейсов и кошельков, их недоступность для злоумышленников. При условии реализации этих технологий существует возможность существенно обезопасить активы от ошибок потребителей, внешних нарушителей, а также технических сбоев рабочих программ. Повышение культуры кибербезопасности населения – ключевое условие безопасного использования технологии невзаимозаменяемых токенов как физическими, так и юридическими лицами. Для его реализации требуются активные междисциплинарные научные исследования, а также правовые, организационные и технические мероприятия государственных регуляторов. Особое внимание целесообразно обратить на развитие соответствующих компетенций будущих специалистов по защите информации.

СПИСОКЛИТЕРАТУРЫ

1. Селезнев М. Определение NFT. – URL: https://trends.rbc.ru/trends/industry/604f3f139a794797b44b7a70 (дата обращения: 30.04.2022).
2. Chalmers D., Fisch C., Matthews R., Quinn W., Recker J. Beyond the bubble: Will NFTs and digital proof of ownership empower creative industry entrepreneurs? // Journal of Business Venturing Insights. – 2022. – Vol. 17. – e00309. DOI: https://doi.org/10.1016/j.jbvi.2022.e00309. – URL: https://www.sciencedirect.com/science/article/pii/S2352673422000075 (дата обращения: 04.05.2022).
3. Что такое NFT и как они работают. – URL: https://postium.ru/chto-takoe-nft/ (дата обращения: 30.04.2022).
4. Анисимов М. Определение блокчейна. – URL: https://bytwork.com/articles/ blockchain (дата обращения: 30.04.2022).
5. NFTs market hits $22bn as craze turns digital images into assets. – URL: https://www.theguardian.com/technology/2021/dec/16/nfts-market-hits-22bn-as-craze-turns-digital-images-into-assets
6. Уваров С. Арт-подготовка: рынку NFT в России спрогнозировали рост до $10 млрд. – URL: https://www.comnews.ru/content/218786/2022-02-11/2022-w06/art-podgotovka-rynku-nft-rossii-sprognozirovali-rost-do-10-mlrd (дата обращения: 30.04.2022).
7. Жибуртович Е. NFT: Правовые вопросы современного тренда. – URL: https://vc.ru/crypto/343524-nft-pravovye-voprosy-sovremennogo-trenda. (дата обращения: 30.04.2022).
8. Wilson K.B., Karg A., Ghaderi H. Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity, Business Horizons, 2021. DOI: https://doi.org/10.1016/j.bushor.2021.10.007. – URL: (https://www.sciencedirect.com/science/article/pii/S0007681321002019) (дата обращения: 30.04.2022).
9. Лиханова Е. Не только цифровое искусство: 5 практических способов использовать NFT. – URL: https://rb.ru/story/new-uses-nfts/ (дата обращения: 30.04.2022).
10. Отчёт об исследовании утечек информации ограниченного доступа в 2021 году / Экспертно-аналитический центр InfoWatch. – 2022. – 32 с. – URL: https://www.infowatch.ru/analytics/analitika/v-2021-stalo-bolshe-umyshlennykh-utechek (дата обращения: 12.04.2022).
11. Россия: утечки информации ограниченного доступа, 2020 год / Экспертно-аналитический центр InfoWatch. – 2021. – 30 с. – URL: https://www.infowatch.ru/analytics/analitika/rossiya-utechki-informatsii-ogranichennogo-dostu pa-2020-god (дата обращения: 30.04.2022).
12. Лукацкий А.В. Крупнейшая реформа законодательства о персональных данных за последние 10 лет. – URL: https://lukatsky.ru/legislation/krupneyshaya-reforma-zakonodatelstva-o-personalnyh-dannyh-za-poslednie-10-let.html (дата обращения: 30.04.2022).
13. Эртель Л.А., Хапай С.Х. Персональные данные пациента, персонифицированный учет, врачебная тайна: правовые пробелы // Медицинское право: теория и практика. – 2019. – Т. 5, № 1(9). – С. 51-55.
14. Skalidis I., Muller O., Fournier S. The Metaverse in Cardiovascular Medicine: Applications, Challenges and the role of Non-Fungible Tokens // Canadian Journal of Cardiology. - 2022. DOI: https://doi.org/10.1016/j.cjca.2022.04.006. – URL: https://www.sciencedirect.com/science/article/pii/S0828282X22002227 (дата обращения: 04.05.2022).
15. Carrano F.M., Sileri P., Batt S. et al. Blockchain in surgery: are we ready for the digital revolution? // Updates in Surgery volume. – 2022. –№ 74. – P. 3–6. – URL: https://doi.org/10.1007/s13304-021-01232-y (дата обращения: 04.05.2022).
16. Otto C. What Does an NFT Have to Do With Art, Darknet and Law? // RechtInnovativ. – 2021. –№ 5. – P. 1–17. – URL: https://doi.org/10.1007/s43442-021-0076-y (дата обращения: 04.05.2022).
17. Booth G.S., Gehrie E.A. Non-fungible tokens: Stem cell transplantation in the blockchain // Transfusion and Apheresis Science. – 2021. – Vol. 60, Iss. 5. DOI: https://doi.org/10.1016/j.transci.2021.103196. – URL: https://www.sciencedirect.com/ science/article/pii/S1473050221001701 (дата обращения: 04.05.2022).
18. Blockchain in healthcare: how blockchain can revolutionize the medical industry (2021). – URL:

https://academy.ivanontech.com/blog/blockchain-in-healthcare-how-blockchain-can-revolutionize-the-medical-industry (дата обращения: 04.05.2022).
19. Blockchain market in healthcare – growth, trends, COVID-19 impact, and forecasts (2022-2026). – URL: https://www.mordorintelligence.com/industry-reports/blockchain-market-in-healthcare (дата обращения: 04.05.2022).
20. Топ-7 способов применения NFT. Binance Academy. – URL: https://academy.binance.com/ru/articles/top-7-nft-use-cases (дата обращения: 04.05.2022).
21. TradeLens(блокчейн-платформа). – URL: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:TradeLens_%28%D0%B1%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD-%D0%BF%D0%BB%D0%B0%D1%82%D1%84%D0%BE%D1%80%D0%BC%D0%B0%29 (дата обращения: 05.05.2022).
22. Емельянов Д. С., Емельянов И.С. Невзаимозаменяемые токены (NFT) как самостоятельный объект правового регулирования // Имущественные отношения в Российской Федерации. – 2021. – № 10(241). – С. 71-76. DOI 10.24412/2072-4098-2021-10-71-76. – EDN QERCWG
23. Давыдов-Громадин Д. Как правильно использовать NFT в России и не нарушить закон. – URL: https://www.rbc.ru/crypto/news/60e2f4609a794732c30fc130 (дата обращения: 04.05.2022).
24. Умаров Х.С. Реализация возможностей невзаимозаменяемых токенов (NFT) на современном рынке интеллектуальной собственности // Финансы и кредит. – 2022. – Т. 28, № 3(819). – С. 699-728. DOI 10.24891/fc.28.3.699.
25. Коллекционер потерял NFT на $2,2 млн. – URL: https://letknow.news/news/kollekcioner-poteryal-nft-na-22-mln-42181.html (дата обращения: 04.05.2022).
26. Хакер подделал NFT от Beeple, проданный за $69,3 млн. – URL: https://forklog.com/haker-poddelal-nft-ot-beeple-prodannyj-za-69-3-mln/ (дата обращения: 04.05.2022).
27. Сарычев Д. Безопасность невзаимозаменяемых токенов. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/How-secure-is-NFT#part5 (дата обращения: 04.05.2022).
28. Омолоев А. Хакер атаковал блокчейн, используемый в основе NFT-игры AxieInfinity, и украл криптовалюту на 625 миллионов долларов. – URL:https://dtf.ru/life/1136965-haker-atakoval-blokcheyn-ispolzuemyy-v-osnove-nft-igry-axie-infinity-i-ukral-kriptovalyutu-na-625-millionov-dollarov?ysclid=l1x5m0zspc (дата обращения: 04.05.2022).
29. Токены подключают к майнингу. Мошенники стали использовать NFT для кражи криптокошельков // Коммерсантъ. – URL: https://www.kommersant.ru/doc/5216108 (дата обращения: 14.02.2022).
30. Microsoft: 99.9% of compromised accounts did not use multi-factor authentication. – URL: https://www.zdnet.com/article/microsoft-99-9-of-compromised-accounts-did-not-use-multi-factor-authentication/ (дата обращения: 04.05.2022).
31. NFT cybersecurity: How to Secure NFTs from Hackers and Scammers. – URL: https://hacken.io/researches-and-investigations/are-nfts-safe-how-to-ensure-security-of-your-nfts/ (дата обращения: 04.05.2022).
32. Описание инструментов мониторинга сети. – URL: https://www.securitylab.ru/analytics/520817.php (дата обращения: 04.05.2022).
33. Фомин Д.А. Перспективные направления внедрения блокчейн-технологии NFT в российскую экономику // Экономические науки. – 2021. – № 199. – С. 7-10. DOI: 10.14451/1.199.7.

Материал поступил в редакцию 05.05.22.

Сведения об авторах

АСТАХОВА Людмила Викторовна – доктор педагогических наук, профессор, профессор кафедры защиты информации Южно-Уральского государственного университета, г. Челябинск
e-mail: astakhovalv@susu.ru

КАЛЯЗИН Никита Васильевич – студент кафедры защиты информации Южно-Уральского государственного университета
e-mail: deskanik@yandex.ru