

## ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ МИНИМИЗАЦИЯ РИСКОВ ДОГОВОРНОЙ РАБОТЫ

Булгакова Е.В., Булгаков В.В.

В настоящее время, в России закладываются предпосылки перехода от заключения договоров в письменном виде к заключению в форме смарт-контрактов. Примерами достаточно успешного опыта по применению смарт-контрактов являются Банк Barclays и блокчейн компании Waves, аккредитивы Альфа-банк и S7, Райффазен банк, факторинг М. Видео, Сбербанкфакторинг, ценные бумаги Сбербанк и МТС, поставки – Газпромнефть и S7 и др.

Последнее время были приняты Федеральный закон от 31.07.2020 г. № 2 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», регулирующий вопросы оборота цифровых финансовых активов и цифровой валюты<sup>1</sup>, Федеральный закон от 02.08.2019 г. № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации», в котором вводятся понятия утилитарных цифровых прав и инвестиционной платформы<sup>2</sup>, Федеральным законом от 18.03.2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации»<sup>3</sup> в гражданское право введены понятие - цифровые права в качестве объектов гражданских прав, исполнение обязательств при наступлении определенных обстоятельств без

---

<sup>1</sup> Федеральный закон от 31.07.2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Официальный интернет-портал правовой информации [Электронный ресурс]. Режим доступа: <http://publication.pravo.gov.ru> (дата обращения: 12.12.2022).

<sup>2</sup> Федеральный закон от 02.08.2019 г. № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации». Официальный интернет-портал правовой информации [Электронный ресурс]. Режим доступа: <http://publication.pravo.gov.ru> (дата обращения: 12.12.2022).

<sup>3</sup> Федеральный закон «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» от 18.03.2019 г. № 34-ФЗ [Электронный ресурс]. Режим доступа: <http://publication.pravo.gov.ru> (дата обращения: 12.12.2021).

направленного на исполнение обязательства отдельно выраженного дополнительного волеизъявления его сторон. Законодатель, таким образом закрепил исполнение обязательств по договору в автоматическом режиме.

Проблематике заключения и исполнения смарт-контрактов посвящены работы: Ю.С. Харитоновой «Смарт-контракт в сфере интеллектуальной собственности»<sup>4</sup>, М.А. Рожковой «Цифровые права: публично-правовая концепция и понятие в российском гражданском праве»<sup>5</sup>, Л.Г. Ефимовой, О.Б. Сиземовой «Правовая природа смарт-контракта»<sup>6</sup>, А.И. Савельева «Некоторые риски токенизации и блокчейнизации гражданско-правовых отношений»<sup>7</sup>, А.Я. Ахмедова «Правовая природа смарт-контракта»<sup>8</sup>, И.В. Цветкова «Правовые (юридические) риски в договорной работе»<sup>9</sup>.

Тренд по внедрению сквозных цифровых технологий приветствуется многими авторами научных трудов, но работ по оценке эффективности их применения, с точки зрения сокращения юридических рисков в договорной работе практически нет.

Переход от заключения договоров в письменном виде к смарт-контрактам обусловлен рядом преимуществ, заключающихся в сокращении сроков заключения договоров, исключения посредников, прозрачности и безопасностью.

Смарт-контракт («умный контракт») – договор, записанный в виде компьютерного кода и криптографически подписанный сторонами сделки, предусматривающий автоматизированное исполнение обязательств и опосредующий оборот цифровых прав и цифровой валюты.

<sup>4</sup> Харитонова, Ю.С. Смарт-контракт в сфере интеллектуальной собственности / Ю. С. Харитонова // Право будущего: интеллектуальная собственность, инновации, Интернет: Ежегодник / РАН. ИНИОН. Центр. социал. науч.-информ. исслед. Отд. правоведения; Кафедра предпринимательского права МГУ им. М.В. Ломоносова; отв. ред. Афанасьева Е.Г. – Москва : Институт научной информации по общественным наукам РАН, 2019. – С. 32-41.

<sup>5</sup> Рожкова, М.А. Цифровые права: публично-правовая концепция и понятие в российском гражданском праве / М. А. Рожкова // Хозяйство и право. – 2020. – № 10(525). – С. 3-12.

<sup>6</sup> Ефимова, Л.Г. Правовая природа смарт-контракта / Л. Г. Ефимова, О. Б. Сиземова // Банковское право. – 2019. – № 1. – С. 21-28.

<sup>7</sup> Савельев, А.И. Некоторые риски токенизации и блокчейнизации гражданско-правовых отношений / А. И. Савельев // Закон. – 2018. – № 2. – С. 36-51.

<sup>8</sup> Ахмедов, А.Я. Правовая природа смарт-контракта / А. Я. Ахмедов // Вестник Саратовской государственной юридической академии. – 2019. – № 5(130). – С. 103-106.

<sup>9</sup> Цветков, И.В. Правовые (юридические) риски в договорной работе / И. В. Цветков, Е. И. Иванова // Законодательство. – 2022. – № 10. – С. 32-40.

Смарт-контракты позволяют избежать трудностей, связанных с бюрократическими процедурами, без которых не обойтись в случае заключения традиционного договора (обращение к юристу или нотариусу и т.п.), а в случае нарушения условий контракта – судебные процессы, на что приходится тратить время и средства. Также, транзакции, проводимые с участием смарт-контрактов, выделяются высоким уровнем безопасности и возможностью их отслеживания. Для обеспечения безопасности разработчики обычно используют службу аудита, которая проверяет код контракта построчно на наличие потенциальных проблем. Кроме того, шифрование данных может использоваться для хранения транзакций в блокчейне для повышения безопасности.

Смарт-контракты хранятся и выполняются в блокчейне, который по сути является децентрализованной, неизменной и общедоступной базой данных. Использование Блокчейн технологии гарантирует, что все транзакции всегда записываются и видны соответствующим сторонам.

Риски при заключении смарт-контракта:

1) Технические риски. Смарт-контракты реализованы в коде, который может содержать ошибки или уязвимости, приводящие к неожиданным результатам.

2) Юридические риски.

3) Риски безопасности. Смарт-контракты хранятся в децентрализованной сети, что делает их уязвимыми для кибератак и других нарушений безопасности.

4) Риски человеческих ошибок: смарт-контракты исполняются автоматически, а это означает, что после развертывания их нельзя изменить даже в случае ошибки.

5) Риски ошибок при составлении контракта: Участники в смарт-контрактах должны быть уверены, что контракт содержит все необходимые условия, чтобы после момента его реализации не создать конфликтные ситуации между сторонами договора.

Юридические риски, связанных с заключением смарт-контрактов:

1. **Незаключение договора:** Статья 432 Гражданского кодекса РФ устанавливает, что, если стороны не достигли соглашения на все существенные условия договора, договор не считается заключенным и не создает юридических обязательств. При использовании смарт-контрактов, контракт может быть незаключенным, если программа не была запрограммирована правильно или если возникли другие технические проблемы, которые могут привести к ошибкам в контракте.

2. **Недействительность договора:** Статьи с 166 по 181 Гражданского кодекса РФ устанавливают основания недействительности договоров, такие как нарушение договорных условий, мошенничество и так далее. Если смарт-контракт не описывает все необходимые условия сделки, не ясен или содержит ошибки, это может привести к его недействительности.

3. **Неисполнимость договора:** если контракт был заключен, но не может быть выполнен по какой-либо причине, это может привести к ответственности участников контракта. Чтобы избежать неисполнения контракта, все условия контракта должны быть определены таким образом, чтобы они могли быть легко поняты и выполнены без необходимости выяснять неясные моменты.

4. **Ответственность за содержание контракта:** Участники в смарт-контрактах должны быть уверены, что контракт содержит все необходимые условия, чтобы избежать ненужных проблем или ответственности. В случае возникновения конфликтов, любые изменения в контракте должны быть выполнены с согласия всех участников.

Для минимизации юридических рисков в смарт-контрактах, важно проводить внимательную проверку всех условий и обязательств в контракте, привлекать квалифицированных юристов, использовать специализированные программные инструменты, такие как Security Vision SGRC, для проведения оценки рисков. Также важно учитывать юридические аспекты при проектировании и программировании смарт-контрактов.

Security Vision SGRC представляет собой платформу для автоматизации процедуры оценки рисков в информационной безопасности при создании и использовании смарт контрактов. Платформа определяет потенциальные риски, связанные с использованием смарт контрактов, и дает рекомендации по управлению рисками.

Риски меняются в зависимости от типа смарт-контракта и специфик его использования.

С помощью Security Vision SGRC, можно определить все юридические риски при заключении смарт контрактов, а также оценить уровень рисков на каждом этапе процесса заключения контракта. Она может также помочь управлять всеми аспектами риска в смарт-контрактах, и в конечном итоге повысить качество и безопасность сделок.

Security Vision SGRC может помочь оценить и улучшить безопасность смарт-контрактов, применяя следующие методы для оценки его защищенности:

1. Анализ кода. Команда экспертов проводит глубокий анализ кода смарт-контрактов на предмет дефектов и уязвимостей, которые могут привести к эксплойту или хакерской атаке.

2. Аудит смарт-контрактов. Проводится полный аудит смарт-контракта, оценивая его безопасность и производительность, а также выявляя любые потенциальные уязвимости, которые могут быть использованы злоумышленниками.

3. Проверка стандартов безопасности. Проверка соответствие вашего смарт-контракта стандартам безопасности в блокчейне, таким как ERC-20 и ERC-721, и рекомендуем соблюдать эти стандарты, чтобы обеспечить максимальную безопасность.

4. Консультации по безопасности. Команда консультантов по безопасности сможет проанализировать такие аспекты, как доступ к смарт-контракту, управление ключами и т.д. Обратившись к Security Vision SGRC для оценки рисков своих смарт-контрактов, вы сможете получить

всестороннюю оценку и сделать решения на основе рисков и уязвимостей, чтобы обеспечить максимальную безопасность блокчейн-проекта.

Оценка рисков заключения договоров в форме смарт-контрактов включает несколько аспектов, связанных с информационной безопасностью. Вот некоторые из них:

1. Риски, связанные с качеством программного обеспечения (ПО). Если программное обеспечение, используемое для создания и выполнения смарт-контрактов, содержит ошибки или лазейки безопасности, это может привести к непредвиденным последствиям, включая потерю средств и/или разглашение конфиденциальной информации.

2. Риски мошенничества. Если участники в договоренности создают смарт-контракты, которые не соответствуют фактическим условиям сделки, то это может привести к проблемам.

3. Риски нарушения приватности. Смарт-контракты могут содержать чувствительную информацию, такую как даты рождения, имена, номера паспортов и адреса электронной почты. Если эта информация попадает в руки злоумышленников, то это может привести к краже личности или хищению средств.

4. Риски, связанные с регулированием. Некоторые виды договоров и сделок могут подвергаться регулированию. Если смарт-контракты не соответствуют регулируемым требованиям, то это может привести к юридическим проблемам для участников в сделке.

5. Риски, связанные с техническими проблемами. Смарт-контракты используют блокчейн технологию, которая может быть подвержена техническим сбоям. Если в процессе выполнения контракта возникнут проблемы, то это может привести к его неисполнению.

6. Риски, связанные с контрагентами. Смарт-контракты не исключают возможность мошенничества со стороны контрагентов. Прежде чем заключать контракты с другими участниками, необходимо проводить тщательную проверку их репутации и кредитоспособности. Так, оценка

рисков заключения смарт-контрактов включает задачи по анализу и управлению рисками, которые могут возникнуть при разработке, подписании и выполнении сделок с использованием смарт-контрактов. Дополнительные меры, такие как использование аудиторских отчетов, проведение юридического анализа и использование инструментов автоматической верификации, могут помочь уменьшить риски заключения смарт-контрактов.

Для встройки автоматического анализа контрагентов в смарт контракт можно использовать различные подходы, такие как анализ данных, машинное обучение и другие методы искусственного интеллекта. Основная идея заключается в том, чтобы собрать и обработать данные о контрагентах, а затем применить алгоритмы для определения их надежности.

Один из примеров автоматизированной оценки контрагентов - это система FICO (Fair Isaac Corporation), которая используется в банковской сфере. Она использует алгоритмы машинного обучения, чтобы определить кредитоспособность заемщика на основе различных факторов, таких как кредитная история, доходы и расходы, наличие задолженностей и другие факторы.

Еще один пример - это система Dun & Bradstreet, которая собирает и анализирует информацию о компаниях со всего мира, чтобы помочь оценить их финансовую устойчивость и надежность в качестве контрагентов. Она использует алгоритмы машинного обучения для обработки и анализа данных о компаниях, таких как финансовые отчеты, репутация и другие факторы.

Другой пример - это система Creditsafe, которая использует алгоритмы машинного обучения и более чем 200 миллионов источников данных для сбора информации о компаниях и их рейтингах. Эта система также используется для оценки кредитоспособности компаний и рисков при заключении контрактов.

Системы, описанные ранее, просматривают миллионы баз данных, различных сайтов и источников в поиске различной информации о контрагенте. Примеры приведены ниже.

Для начала система распознает ИНН контрагента с помощью системы распознавания ИНН физ. На основе распознанного ИНН система заходит на единый федеральный реестр сведений о банкротстве и указывает, банкрот ли контрагент.

Также, на портале открытых данных Счетной палаты Российской Федерации можно узнать, как распорядился контрагент федеральным бюджетом. Есть и сервис, который позволяет выяснить, заблокированы или нет банковские счета конкретного юридического лица или ИП. Далее система анализирует многие другие платформы в поиске различной информации.

В общем, автоматический анализ контрагентов на предмет надежности может быть полезен для предотвращения рисков и улучшения эффективности бизнеса. Он может быть встроен в смарт контракты и другие системы, чтобы обеспечить быстрый и точный анализ контрагентов и принимать обоснованные решения на основе данных.

Таким образом, оценка рисков информационной безопасности при заключении смарт-контрактов, полученная при проведении исследования на уязвимости с использованием специально программного обеспечения показала высокие риски их незаключенности, недействительности, неисполнимости. Установление уязвимостей смарт-контрактов при массовом их использовании, а также разработка безопасных смарт-контрактов, обеспечит надежное и безопасное взаимодействие участников сделки.

### **Список литературы**

1. Федеральный закон от 31.07.2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Официальный интернет-

портал правовой информации [Электронный ресурс]. Режим доступа: <http://publication.pravo.gov.ru> (дата обращения: 12.12.2022).

2. Федеральный закон от 02.08.2019 г. № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации». Официальный интернет-портал правовой информации [Электронный ресурс]. Режим доступа: <http://publication.pravo.gov.ru> (дата обращения: 12.12.2022).

3. Федеральный закон «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» от 18.03.2019 г. № 34-ФЗ [Электронный ресурс]. Режим доступа: <http://publication.pravo.gov.ru> (дата обращения: 12.12.2021).

4. Харитонова, Ю.С. Смарт-контракт в сфере интеллектуальной собственности / Ю. С. Харитонова // Право будущего: интеллектуальная собственность, инновации, Интернет: Ежегодник / РАН. ИНИОН. Центр. социал. науч.-информ. исслед. Отд. правоведения; Кафедра предпринимательского права МГУ им. М.В. Ломоносова; отв. ред. Афанасьева Е.Г. – Москва : Институт научной информации по общественным наукам РАН, 2019. – С. 32-41.

5. Рожкова, М.А. Цифровые права: публично-правовая концепция и понятие в российском гражданском праве / М. А. Рожкова // Хозяйство и право. – 2020. – № 10(525). – С. 3-12.

6. Ефимова, Л.Г. Правовая природа смарт-контракта / Л. Г. Ефимова, О. Б. Сизимова // Банковское право. – 2019. – № 1. – С. 21-28.

7. Савельев, А.И. Некоторые риски токенизации и блокчейнизации гражданско-правовых отношений / А. И. Савельев // Закон. – 2018. – № 2. – С. 36-51.

8. Ахмедов, А.Я. Правовая природа смарт-контракта / А. Я. Ахмедов // Вестник Саратовской государственной юридической академии. – 2019. – № 5(130). – С. 103-106.

9. Цветков, И.В. Правовые (юридические) риски в договорной работе / И. В. Цветков, Е. И. Иванова // Законодательство. – 2022. – № 10. – С. 32-40.

**Ключевые слова:** смарт-контракт; договорное право; искусственный интеллект; нейросеть; блокчейн технология; юридические риски; договорная работа; информационная безопасность смарт-контрактов; незаключение договора; недействительность договора; неисполнимость договора.

**Аннотация:**

Статья посвящена вопросам минимизации рисков в договорной работе при использовании смарт-контрактов. Авторами были установлены юридические риски, которые сопутствуют заключению договора в простой письменной форме и смарт-контракта, а также установлены преимущества управления юридическими рисками при использовании последних. Приведенные в статье результаты исследования свидетельствуют о том, что риски информационной безопасности порождают юридические риски при заключении договоров, с использованием смарт-контрактов.