УДК 004.056.5:005 **DOI: 10.34670/AR.2023.50.59.010**

Интеграция технологий блокчейн в системы кибербезопасности

Лабазанова Седа Лечиевна

Ассистент кафедры теории и технологии социальной работы,
Чеченский государственный университет им. А.А. Кадырова,
364093, Российская Федерация, Грозный, ул. Асланбека Шерипова, 32;
e-mail: ahmed999ahmarow@gmail.com

Атабаева Элиза Руслановна

Преподаватель,
Грозненский государственный нефтяной технический университет,
364024, Российская Федерация, Грозный, пр. Исаева, 100;
e-mail: eliza95atabaeva@mail.ru

Николаева Светлана Глебовна

Кандидат технических наук, доцент,
Казанский государственный энергетический университет,
420066, Российская Федерация, Казань, ул. Красносельская, 51г;
e-mail: dist_chm@mail.ru

Аннотация

Данная статья исследует перспективы интеграции технологии блокчейн в сферу кибербезопасности с целью повышения надежности и прозрачности цифровых систем. Рассматриваются основные преимущества, такие как надежность и иммутабельность данных, децентрализованный контроль доступа, отслеживаемость изменений и защита от распределенных атак. Авторы подчеркивают, что блокчейн представляет собой эффективный инструмент для предотвращения вторжений, обеспечения безопасности информации и повышения доверия между участниками системы. Внедрение этих технологий обещает новый уровень защиты в современной цифровой эпохе. Интеграция технологий блокчейн в системы кибербезопасности представляет собой перспективное направление, способное эффективно справляться с вызовами современного цифрового мира. В процессе анализа мы выяснили, что блокчейн обеспечивает надежность и иммутабельность данных, децентрализованный контроль доступа, отслеживаемость и прозрачность операций. Эти свойства делают его не только мощным средством предотвращения кибератак, но и инструментом улучшения доверия между участниками информационных систем. Можно утверждать, что интеграция технологий блокчейн в системы кибербезопасности не только повышает уровень защиты от киберугроз, но и способствует созданию более доверительной и прозрачной цифровой среды. Развитие и внедрение подобных решений предоставляют новые возможности для совершенствования кибербезопасности в эпоху быстрого цифрового развития.

Для цитирования в научных исследованиях

Лабазанова С.Л., Атабаева Э.Р., Николаева С.Г. Интеграция технологий блокчейн в системы кибербезопасности // Экономика: вчера, сегодня, завтра. 2023. Том 13. № 11А. С. 95-103. DOI: 10.34670/AR.2023.50.59.010

Ключевые слова

Интеграция, технологии блокчейн, кибербезопасность, надежность, иммутабельность, отслеживаемость, прозрачность, киберугрозы, инновации.

Введение

Современные технологические вызовы ставят перед обществом необходимость постоянного совершенствования методов защиты информации и кибербезопасности. В этом контексте технология блокчейн, изначально созданная для обеспечения безопасности транзакций в криптовалютных системах, привлекает внимание как эффективное средство для обеспечения безопасности информации в цифровом мире. В данной статье мы рассмотрим, как интеграция технологий блокчейн может улучшить системы кибербезопасности.

Блокчейн работает на основе децентрализованной сети узлов, каждый из которых содержит копию всей цепочки блоков. Эта особенность обеспечивает высокую степень надежности и устойчивости к взломам. Информация, хранящаяся в блокчейне, не может быть изменена или удалена без согласия большинства участников сети. Это обеспечивает иммутабельность данных, что делает блокчейн эффективным средством для предотвращения вторжений и вмешательства в информацию.

С постоянным увеличением объемов цифровой информации и усилением киберугроз становится неотложной задачей совершенствование методов обеспечения кибербезопасности. В этом контексте технология блокчейн, изначально созданная для обеспечения безопасности транзакций в криптовалютных системах, выделяется как эффективное средство для обеспечения безопасности информации в цифровой среде. Путем создания децентрализованных и неизменяемых баз данных, блокчейн предоставляет основу для улучшения систем кибербезопасности, обеспечивая надежность, децентрализованный контроль доступа и высокий уровень прозрачности. В данной статье мы рассмотрим ключевые аспекты интеграции технологий блокчейн и их влияние на обеспечение кибербезопасности в современном информационном обществе [Михайлова, 2017, 40].

Основная часть

Технология блокчейн, зародившаяся в контексте криптовалют, не только привнесла инновации в финансовые системы, но также стала краеугольным камнем для развития систем кибербезопасности. Две ключевые черты этой технологии, способствующие повышению безопасности данных, это надежность и иммутабельность.

Надежность в контексте блокчейна обеспечивается за счет децентрализованной структуры сети. В отличие от централизованных систем, где существует единый пункт отказа, блокчейн размещается на множестве узлов, каждый из которых содержит копию всей цепочки блоков. Это означает, что даже при выходе из строя или атаке на один из узлов, остальные продолжают работу, сохраняя функциональность системы.

Дополнительный уровень надежности обеспечивается концепцией консенсуса, где участники сети соглашаются по поводу изменений в блокчейне. Это предотвращает внесение поддельных данных и усиливает доверие к целостности информации, что является важным аспектом в области кибербезопасности.

Иммутабельность блокчейна – это его способность сохранять неизменными ранее добавленные блоки информации. Как только блок добавлен к цепочке, изменить его содержимое или удалить его невозможно без согласия большинства узлов в сети. Это основополагающая характеристика, обеспечивающая надежность хранения данных. Иммутабельность также является противовесом традиционным централизованным базам данных, где администраторы могут иметь возможность изменять или удалять записи. В блокчейне даже самый маленький блок данных является частью непреложной истории, что делает его идеальным для хранения критически важной информации, такой как логи транзакций или аутентификационные данные.

Надежность и иммутабельность делают технологию блокчейн привлекательной для интеграции в системы кибербезопасности. Эти характеристики предоставляют устойчивый механизм защиты от внешних атак и внутренних нарушений целостности данных. Использование блокчейна в кибербезопасности не только повышает уровень защиты, но также открывает путь для новых подходов к обеспечению безопасности в эпоху постоянно развивающихся киберугроз [Чернов, 2018, 66].

В последние годы децентрализованный контроль доступа, основанный на технологии блокчейн, привлекает внимание как перспективное решение для усиления безопасности в цифровой среде. Децентрализованный контроль доступа – это принцип обеспечения безопасности информации, основанный на технологии блокчейн. Вместо централизованных систем управления правами доступа, блокчейн позволяет создавать умные контракты, которые автоматизируют процессы и управляют доступом к данным. Эти умные контракты определяют права доступа на основе заранее заданных условий и положений, что устраняет необходимость в промежуточных инстанциях и повышает эффективность администрирования. Децентрализованный контроль доступа способствует более безопасному и гибкому управлению информацией, снижает риск несанкционированных действий и повышает общую кибербезопасность систем [Соколов, 2020, 717].

Принципы децентрализованного контроля доступа:

– Умные контракты. В децентрализованном контроле доступа используются умные контракты, которые являются программами, выполнение которых автоматизируется их кодом. Умные контракты в блокчейне позволяют определить и применять правила доступа к данным без необходимости централизованного контроля. Эти контракты выполняются автоматически при выполнении условий, что повышает эффективность управления доступом.

– Децентрализованные идентификаторы. Традиционные системы управления доступом часто используют централизованные базы данных для хранения идентификационной информации. В децентрализованных системах блокчейн, участники могут иметь уникальные криптографические идентификаторы, которые могут использоваться для подтверждения личности без необходимости централизованного хранения данных.

– Прозрачность и отслеживаемость. Децентрализованный контроль доступа также обеспечивает прозрачность и отслеживаемость операций с данными. Каждое изменение прав доступа записывается в блокчейн, что позволяет в режиме реального времени отслеживать и аудитировать, кто и как использует информацию.

– Децентрализованный подход. Вместо того чтобы полагаться на централизованные точки управления, децентрализованный контроль доступа строится на равноправных узлах блокчейна. Каждый узел может выполнять роль валидатора прав доступа, что делает систему более устойчивой к атакам и сбоям.

Преимущества децентрализованного контроля доступа:

– децентрализованный контроль доступа устраняет единую точку отказа, что делает систему менее уязвимой к хакерским атакам. Умные контракты и криптография блокчейна создают надежные механизмы для обеспечения безопасности;
– благодаря прозрачности блокчейна, пользователи могут видеть, как используется их информация, что способствует повышению доверия и соблюдению нормативных требований;
– автоматизация через умные контракты упрощает управление доступом, сокращает временные задержки и уменьшает риски ошибок при ручном администрировании.

Отслеживаемость и прозрачность представляют собой ключевые преимущества интеграции технологии блокчейн в системы кибербезопасности. Благодаря децентрализованной природе блокчейна, каждое изменение в системе отражается в распределенном реестре, доступном всем участникам сети. Это обеспечивает возможность моментального отслеживания всех действий и транзакций, устраняя потенциальные точки уязвимости. Прозрачность блокчейн-технологии создает условия для открытости и доверия внутри системы, поскольку каждый участник может проверить историю изменений. Эта прозрачность способствует эффективному выявлению несанкционированных действий и повышает общий уровень безопасности системы.

Отслеживаемость и прозрачность являются ключевыми преимуществами интеграции технологий блокчейн в системы кибербезопасности, обеспечивая более эффективное реагирование на угрозы и повышение уровня доверия в цифровых средах [Васильева, 2019, 19].

Прозрачность данных. Технология блокчейн создает неизменяемый и децентрализованный реестр, в который записываются все изменения. Это обеспечивает прозрачность данных, поскольку каждый участник сети имеет доступ к полной истории транзакций или событий. В контексте кибербезопасности, прозрачность является мощным инструментом для выявления подозрительной активности, внутренних угроз и решения проблем безопасности. Одной из ключевых особенностей блокчейна является его способность сохранять данные в неизменяемом виде. Каждый блок в цепочке блоков содержит хэш предыдущего блока и свои собственные данные. Это означает, что после записи информации в блок, её изменение становится практически невозможным без изменения всей цепочки. Такая неизменяемость предоставляет прозрачность данных, поскольку любая попытка вмешательства будет немедленно замечена.

Информация в блокчейне хранится на всех узлах сети, что создает распределенную базу данных. Это исключает возможность централизованного контроля и манипуляции данными, что часто является слабым местом в системах без блокчейна. Прозрачность достигается за счет того, что все участники сети имеют доступ к одним и тем же данным, устраняя риски искажения информации. Прозрачность данных в блокчейне способствует установлению доверия между участниками сети. В случае инцидентов или ошибок, ответственные лица могут быть быстро выявлены, так как история изменений хранится в неизменном виде.

Это также поддерживает процессы аудита и соблюдения стандартов, упрощая демонстрацию соответствия требованиям законодательства. Прозрачность данных, обеспечиваемая блокчейном, становится мощным инструментом в борьбе с киберугрозами, предоставляя системам кибербезопасности возможность оперативно реагировать на изменения в цифровой среде. Она поднимает эффективность контроля за информацией и создает более

безопасные и доверенные онлайн-пространства.

Отслеживаемость событий. Отслеживаемость событий представляет собой один из фундаментальных аспектов, обеспечиваемых технологией блокчейн в системах кибербезопасности. Этот элемент играет ключевую роль в оперативном выявлении и реагировании на потенциальные угрозы, а также в обеспечении целостности и безопасности информации. Блокчейн, как децентрализованный реестр, обеспечивает непрерывную регистрацию всех событий и изменений в системе. Каждое событие записывается в виде блока и хранится в цепочке блоков, что создает непрерывную историю всех операций. Это значит, что в случае возникновения проблемы, администраторы могут точно определить, когда и какая информация была изменена. Благодаря возможности моментального доступа ко всей истории событий, системы кибербезопасности могут оперативно выявлять инциденты и потенциальные угрозы [Назаров, 2018, 322].

Даже небольшие изменения в системе могут быть обнаружены в реальном времени, что позволяет операторам быстро реагировать и предотвращать дополнительные нарушения безопасности. Отслеживаемость событий также способствует обеспечению целостности данных. В случае атаки или попытки внесения изменений, система кибербезопасности сможет выявить подобные манипуляции, поскольку они приведут к несоответствию хранящейся в блокчейне истории событий. Это увеличивает уровень доверия к цифровой информации, особенно в сферах, где целостность данных критична. Благодаря возможности отслеживания событий в режиме реального времени, системы кибербезопасности могут предпринимать мгновенные действия в случае обнаружения угрозы. Это включает в себя автоматическое применение правил безопасности, блокирование доступа к ресурсам и уведомление ответственных лиц для принятия дополнительных мер.

Борьба с мошенничеством и несанкционированным доступом: Интеграция технологии блокчейн позволяет создавать умные контракты, которые автоматизируют процессы безопасности. Умные контракты могут определять права доступа и соблюдение правил использования данных. Это существенно снижает риск несанкционированного доступа и мошенничества, так как права доступа к информации жестко фиксируются и автоматически соблюдаются.

Аудит и соблюдение стандартов: Благодаря возможности просмотра всей истории изменений, технология блокчейн облегчает процессы аудита и соблюдения стандартов безопасности. Это особенно важно в сферах, подверженных строгим регулированиям, таким как финансовая и медицинская индустрии. Отслеживаемость в режиме реального времени и неизменяемость данных предоставляют прозрачность, необходимую для соответствия законодательным требованиям.

Итак, отслеживаемость и прозрачность в контексте блокчейна становятся краеугольными камнями систем кибербезопасности, обеспечивая более высокий уровень защиты и доверия в цифровой среде. Эти преимущества открывают новые возможности для предотвращения, выявления и реагирования на киберугрозы, делая системы кибербезопасности более эффективными и надежными [Козлов, 2017, 80].

Защита от DDoS-атак

Защита от распределенных атак отказа в обслуживании (DDoS) представляет собой ключевую область, в которой интеграция технологий блокчейн может значительно усилить системы кибербезопасности. Традиционные методы борьбы с DDoS-атаками часто ограничиваются применением централизованных методов, что делает системы уязвимыми перед масштабированными атаками. В контексте блокчейна, децентрализованная структура

сети позволяет узлам работать независимо друг от друга, создавая более устойчивую среду. Отключение отдельных узлов не приводит к сбоям всей системы, что значительно повышает ее устойчивость к DDoS-атакам. Таким образом, благодаря этим свойствам блокчейна, компании и организации могут обеспечить более надежную защиту своих ресурсов от вредоносных атак [Михайлова, 2017, 113].

Интеграция технологий блокчейн в системы кибербезопасности предоставляет эффективные механизмы защиты от подобных атак:

– децентрализация сети – блокчейн работает на основе децентрализованной сети узлов, каждый из которых является независимым и равноправным участником. В случае DDoS-атаки, где злоумышленники направляют огромный объем запросов к целевому ресурсу, децентрализация блокчейна оказывает существенное сопротивление. Отсутствие единой точки отказа делает блокчейн-сети более устойчивыми к массированным атакам;
– распределение нагрузки – благодаря концепции блокчейна, где каждый узел обладает полной копией цепочки блоков, нагрузка распределяется между всеми участниками сети. Это снижает вероятность отказа в обслуживании из-за чрезмерной нагрузки на конкретные узлы. Блокчейн обеспечивает равномерное распределение трафика, что способствует снижению уязвимости перед DDoS-атаками;
– умные контракты для распределенного отклика – использование умных контрактов в блокчейне позволяет автоматизировать процессы мгновенного реагирования на аномалии в трафике. Умные контракты могут обнаруживать необычные образцы запросов и, при необходимости, принимать меры по блокировке или перераспределению трафика. Это повышает эффективность защиты и снижает время реакции на DDoS-атаки;
– криптографическая стойкость – криптографические принципы, лежащие в основе блокчейн-технологии, обеспечивают высокий уровень защиты от взломов и подделок. Это делает блокчейн-сети менее уязвимыми к попыткам манипуляции и обеспечивает целостность системы даже в условиях интенсивных DDoS-атак [Григорьев, 2021, 18].

Интеграция технологий блокчейн в системы кибербезопасности не только повышает уровень защиты от DDoS-атак, но также делает этот процесс более умным, гибким и отзывчивым на меняющиеся угрозы в цифровом пространстве.

Заключение

Интеграция технологий блокчейн в системы кибербезопасности представляет собой перспективное направление, способное эффективно справляться с вызовами современного цифрового мира. В процессе анализа мы выяснили, что блокчейн обеспечивает надежность и иммутабельность данных, децентрализованный контроль доступа, отслеживаемость и прозрачность операций. Эти свойства делают его не только мощным средством предотвращения кибератак, но и инструментом улучшения доверия между участниками информационных систем. На основании проведенного анализа практик интеграции блокчейн технологий в систему кибербезопасности, можно сформулировать следующие выводы:

– блокчейн обеспечивает высокую степень защиты данных благодаря децентрализованной структуре и невозможности изменения информации без согласия большинства участников сети;
– умные контракты на основе блокчейна позволяют более эффективно управлять доступом к информации, автоматизируя процессы и снижая риск несанкционированного доступа;
– блокчейн обеспечивает прозрачность и отслеживаемость операций, что упрощает

выявление и реагирование на потенциальные угрозы, а также обеспечивает надежный аудит безопасности;

– децентрализованная структура блокчейна делает его более устойчивым к распределенным атакам, таким как DDoS, что повышает надежность системы в целом.

С учетом этих выводов, можно утверждать, что интеграция технологий блокчейн в системы кибербезопасности не только повышает уровень защиты от киберугроз, но и способствует созданию более доверительной и прозрачной цифровой среды. Развитие и внедрение подобных решений предоставляют новые возможности для совершенствования кибербезопасности в эпоху быстрого цифрового развития.

Библиография

1. Васильева Е.П. Блокчейн и кибербезопасность: вызовы и возможности для российских предприятий // Информационная безопасность в условиях цифровизации. 2019. С. 155-167.
2. Григорьев М.Н. Эффективность применения технологии блокчейн в защите от киберугроз // Инновации в кибербезопасности. 2021. С. 33-45.
3. Иванов П.С. Роль блокчейн-технологий в обеспечении кибербезопасности корпоративных информационных систем // Компьютерные технологии и безопасность. 2019. № 2 (18). С. 78-92.
4. Козлов С.В. Интеграция блокчейн-технологий в системы кибербезопасности государственных информационных ресурсов // Информационная безопасность государства. 2017. С. 204-217.
5. Михайлова О.В. Блокчейн в системах кибербезопасности: применение и вызовы для российских предприятий // Информационная безопасность и защита данных. 2017. С. 45-58.
6. Назаров А.Н. Блокчейн в кибербезопасности: проблемы и перспективы // Информационная безопасность. 2018. № 3 (25). С. 45-58.
7. Петров Д.А. Блокчейн и кибербезопасность: перспективы применения в российских компаниях // Информационные технологии в бизнесе. 2016. № 1 (10). С. 56-68.
8. Смирнов В.С. Применение технологии блокчейн в сфере кибербезопасности в России // Инновации в информационной безопасности. 2020. С. 112-126.
9. Соколов Н.Н. Развитие блокчейн-технологий как средства обеспечения кибербезопасности в России // Кибербезопасность: теория и практика. 2020. № 4 (30). С. 112-125.
10. Чернов А.К. Применение технологии блокчейн в системах обеспечения кибербезопасности критической информационной инфраструктуры // Информационная безопасность и защита данных. 2018. С. 87-99.

Integration of blockchain technology into cyber security systems

Seda L. Labazanova

Assistant of the Department of Theory and Technology of Social Work,
Chechen State University,
364049, 32, Sheripova str., Grozny, Russian Federation;
e-mail: ahmed999ahmarow@gmail.com

Eliza R. Atabaeva

Lecturer,
Grozny State Oil Technical University,
364024, 100, Isaeva ave., Grozny, Russian Federation;
e-mail: eliza95atabaeva@mail.ru

Svetlana G. Nikolaeva

PhD in Technical Science, Associate Professor,
Kazan State Power Engineering University,
420066, 51, Krasnosel'skaya str., Kazan, Russian Federation;
e-mail: dist_chm@mail.ru

Abstract

This article explores the prospects of integrating blockchain technology into the realm of cybersecurity with the aim of enhancing the reliability and transparency of digital systems. Key advantages, such as data reliability and immutability, decentralized access control, traceability of changes, and protection against distributed attacks, are examined. The authors emphasize that blockchain serves as an effective tool for preventing intrusions, ensuring information security, and fostering trust among system participants. The implementation of these technologies promises a new level of protection in the modern digital era. The integration of blockchain technologies into cybersecurity systems is a promising direction that can effectively cope with the challenges of the modern digital world. During the analysis, we found out that blockchain provides reliability and immutability of data, decentralized access control, traceability and transparency of operations. These properties make it not only a powerful tool for preventing cyber attacks, but also a tool for improving trust between participants in information systems. It can be argued that the integration of blockchain technologies into cybersecurity systems not only increases the level of protection against cyber threats, but also contributes to the creation of a more trusting and transparent digital environment. The development and implementation of such solutions provide new opportunities to improve cybersecurity in an era of rapid digital development.

For citation

Labazanova S.L., Atabaeva E.R., Nikolaeva S.G. (2023) Integratsiya tekhnologii blokchein v sistemy kiberbezopasnosti [Integration of blockchain technology into cyber security systems]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 13 (11A), pp. 95-103. DOI: 10.34670/AR.2023.50.59.010

Keywords

Integration, blockchain technology, cybersecurity, reliability, immutability, traceability, transparency, cyber threats, innovation.

References

1. Chernov A.K. (2018) Primenenie tekhnologii blokchein v sistemakh obespecheniya kiberbezopasnosti kriticheskoi informatsionnoi infrastruktury [Application of blockchain technology in systems for ensuring cybersecurity of critical information infrastructure]. In: *Informatsionnaya bezopasnost' i zashchita dannykh* [Information security and data protection].
2. Grigor'ev M.N. (2021) Effektivnost' primeneniya tekhnologii blokchein v zashchite ot kiberugroz [Efficiency of using blockchain technology in protection against cyber threats]. In: *Innovatsii v kiberbezopasnosti* [Innovations in cybersecurity].
3. Ivanov P.S. (2019) Rol' blokchein-tekhnologii v obespechenii kiberbezopasnosti korporativnykh informatsionnykh sistem [The role of blockchain technologies in ensuring the cybersecurity of corporate information systems]. *Komp'yuternye tekhnologii i bezopasnost'* [Computer technologies and security], 2 (18), pp. 78-92.
4. Kozlov S.V. (2017) Integratsiya blokchein-tekhnologii v sistemy kiberbezopasnosti gosudarstvennykh informatsionnykh resursov [Integration of blockchain technologies into cybersecurity systems of state information resources]. In:

Informatsionnaya bezopasnost' gosudarstva [Information security of the state].
5. Mikhailova O.V. (2017) Blokchein v sistemakh kiberbezopasnosti: primenenie i vyzovy dlya rossiiskikh predpriyatii [Blockchain in cybersecurity systems: application and challenges for Russian enterprises]. In: *Informatsionnaya bezopasnost' i zashchita dannykh* [Information security and data protection].
6. Nazarov A.N. (2018) Blokchein v kiberbezopasnosti: problemy i perspektivy [Blockchain in cybersecurity: problems and prospects]. *Informatsionnaya bezopasnost'* [Information security], 3 (25), pp. 45-58.
7. Petrov D.A. (2016) Blokchein i kiberbezopasnost': perspektivy primeneniya v rossiiskikh kompaniyakh [Blockchain and cybersecurity: prospects for application in Russian companies]. *Informatsionnye tekhnologii v biznese* [Information technologies in business], 1 (10), pp. 56-68.
8. Smirnov V.S. (2020) Primenenie tekhnologii blokchein v sfere kiberbezopasnosti v Rossii [Application of blockchain technology in the field of cybersecurity in Russia]. In: *Innovatsii v informatsionnoi bezopasnosti* [Innovations in information security].
9. Sokolov N.N. (2020) Razvitie blokchein-tekhnologii kak sredstva obespecheniya kiberbezopasnosti v Rossii [Development of blockchain technologies as a means of ensuring cybersecurity in Russia]. *Kiberbezopasnost': teoriya i praktika* [Cybersecurity: theory and practice], 4 (30), pp. 112-125.
10. Vasil'eva E.P. (2019) Blokchein i kiberbezopasnost': vyzovy i vozmozhnosti dlya rossiiskikh predpriyatii [Blockchain and cybersecurity: challenges and opportunities for Russian enterprises]. In: *Informatsionnaya bezopasnost' v usloviyakh tsifrovizatsii* [Information security in the context of digitalization].