УДК 004.056.5

Д.А. Саяков, daniyar.sayakov@yandex.ru
Национальный исследовательский ядерный университет «МИФИ», г. Москва
А.Н.Акматова,akmatovaaishoola@gmail.com
Национальный исследовательский ядерный университет «МИФИ», г. Москва

ПРИМЕНЕНИЕ BIG DATA В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ НАЦИОНАЛЬНОЙ ЦИФРОВОЙ ВАЛЮТЫ

В работе исследуется применение методологии Big Data в обеспечении безопасности национальной цифровой валюты. С увеличением числа транзакций и пользователей в секторе цифровых валют возникает необходимость в разработке и применении новых методов и технологий для обеспечения безопасности и защиты от киберугроз. Большие данные (Big Data) позволяют собирать и анализировать большие объемы информации для выявления необычных и аномальных паттернов, поведения и событий. В контексте национальной цифровой валюты это позволяет обнаруживать подозрительные операции, мошенническую активность и другие потенциальные угрозы для безопасности.

Ключевые слова: BIG DATA cbdc, большие данные, анализ транзакций цифровых валют, мошенничество в операциях с цифровыми валютами, угроза безопасности цифровых валют, обработка персональных данных, защита персональных данных.

Введение

Большие данные или огромные объемы данных относятся к объему задействованных данных, который настолько велик, что его невозможно собрать, управлять, обработать и организовать в разумные сроки с помощью обычных программных инструментов, помогающих принимать бизнес-решения.

Gartner, исследовательская организация по «большим данным», дает такое определение. «Большие данные» требуют, чтобы новые модели обработки имели более сильные возможности принятия решений, открытия и оптимизации процессов, чтобы адаптироваться к огромным, высоким темпам роста и диверсифицированным информационным активам.

Определение, данное Глобальным институтом McKinsey, таково: коллекция данных настолько велика, что ее сбор, хранение, управление и анализ значительно превосходят возможности традиционных программных инструментов баз данных. Она имеет огромный масштаб данных, быстрый поток данных и разнообразные характеристики: низкий тип данных и плотность значений.

Стратегическое значение технологии больших данных заключается не в освоении огромных объемов данных, а в профессиональной обработке этих значимых данных. Другими словами, если сравнивать большие данные с отраслью, то ключом к тому, чтобы сделать эту отрасль прибыльной, является улучшение «возможностей обработки» данных и достижение «добавленной стоимости» данных посредством «обработки».

С технической точки зрения связь между большими данными и облачными вычислениями неразделима, это как две стороны одной медали. Большие данные не могут обрабатываться одним компьютером и должны использовать распределенную архитектуру. Его особенность заключается в распределенном интеллектуальном анализе больших объемов данных. Но он должен опираться на распределенную обработку, распределенные базы данных и облачное хранилище, а также технологию виртуализации облачных вычислений.

Большие данные требуют специальных методов для эффективной обработки больших объемов данных в течение приемлемого периода времени. Технологии, применимые к большим данным, включают базы данных массово-параллельной обработки (MPP), интеллектуальный анализ данных, распределенные файловые системы, распределенные базы данных, платформы облачных вычислений, интернет и масштабируемые системы хранения.[1]

Развитие технологий обработки данных сопровождается эволюцией требований к приложениям данных, что влияет на способ и масштаб ввода данных в производство. Данные

постепенно стали ключевым элементом содействия производству в развитии соответствующих технологий и промышленного фона. Таким образом, термин «элемент данных» ориентирован на цифровую экономику и относится к «данным» в контексте обсуждения производительности и производственных отношений, подчеркивая ценность данных для содействия производству. Другими словами, элементы данных относятся к компьютерным данным и их производным формам, которые собираются, организуются и обрабатываются в соответствии с конкретными производственными потребностями, а также к исходным наборам данных, стандартизированным наборам данных, различным продуктам данных и системам на основе данных, которые инвестируются в производство. Как информация, так и знания могут быть включены в обсуждение элементов данных.

Цифровая валюта, создаваемая центральными банками своих стран, является полноценной национальной валютой, ценность которой подкреплена производимыми технологиями, ресурсами, золотым запасом страны. Все страны мира желают разработать централизованную цифровую валюту. На 2022 год только несколько стран разработали или находятся на стадии тестирования цифровой валюты в своей стране. Коренное отличие цифровой валюты от криптовалюты в том, что все физические и юридические участники экономической среды страны должны воспринимать ее как законное платежное средство.[2]В зависимости от взаимосвязи между криптовалютой и реальной экономикой вместе с реальной валютой ее можно разделить на три категории:

1. Она полностью закрыта, не имеет ничего общего с реальной экономикой и может использоваться только в конкретных виртуальных сообществах.

2. Вы можете купить ее в реальной валюте, но не выкупать обратно. Вы можете использовать ее для покупки виртуальных товаров и услуг.

3. Ее можно обменять и использовать в реальной валюте в определенном соотношении. Вы можете купить виртуальные товары и услуги, а также реальные товары и услуги, такие, как биткойн.

Но есть определенные проблемы и риски, связанные с информационной безопасностью. В связи с этим важно исследовать и разработать механизмы по снижению рисков реализации угроз, связанные с цифровыми транзакциями и финансовыми операциями.

Одним из главных вопросов является защита от несанкционированных транзакций или/и несанкционированный доступ к данным пользователей. Но также с развитием области квантовых компьютеров требуется разработать меры по криптографической защите, которые обеспечат безопасность цифровых подписей, шифрования данных и аутентификации пользователей.

Если защита цифровой валюты и аккаунтов пользователей является задачей криптографических средств защиты, то остается уязвимое место, это атаки человека посередине DoS и DDoS, атаки, против которых важно установить механизмы контроля и мониторинга для обнаружения и предотвращения финансовых мошенничеств и отмывания денег. Это может включать в себя разработку аналитических инструментов и внедрение искусственного интеллекта для анализа и сравнения финансовых операций, а также выявления подозрительных транзакций.

Необходимо разработать механизмы безопасного хранения и передачи цифровых активов, а также защиту от утери или кражи средств пользователей.

Одной из лучших практик, которые многие страны применяют, является использование технологии блокчейн. Блокчейн представляет собой децентрализованную систему хранения данных, которая обеспечивает непрерывность, безопасность и прозрачность транзакций. Модели блокчейн-технологии могут быть использованы для создания и обслуживания цифровой валюты [3].

Однако существуют и неудачные примеры реализации национальной цифровой валюты, в основном такая проблема связана с недоверием со стороны жителей к новой форме денег, вместе с этим коррупция и экономический кризис.

Успехом зарубежного опыта является китайский электронный юань или же e-CNY. Она уже успешно внедрена в торговлю и платежи в различных секторах экономики страны, так как Китай уделяет большое внимание безопасности, чтобы предотвратить мошенничество и взломы. Например, голландский банк разработал специальные физические устройства, которые требуют аутентификации для осуществления транзакций. Это значительно повышает безопасность и предотвращает несанкционированный доступ к цифровой валюте.

Проблемы безопасности национальной цифровой валюты

В зависимости от технического решения, принятого для CBDC, могут возникнуть различные проблемы с конфиденциальностью и защитой данных:

A. Угрозы кибербезопасности

1. Взломы и кибератаки.
2. Фишинг и мошенничество.

B. Угрозы конфиденциальности данных

C. Угрозы финансовых операций

1. Фальсификация транзакций.
2. Нелегальные операции и отмывание денег.

При внедрении без надлежащих протоколов безопасности и адекватной архитектуры вопросы конфиденциальности и безопасности CBDC могут оказать серьезное влияние из-за масштаба таких проектов. Многое также будет зависеть от целей политики и вариантов использования CBDC. Итак, ключевым моментом является подключение требования к защите данных и конфиденциальности в рамках основной концепции CBDC и для проведения оценки воздействия на защиту данных с течением времени, чтобы иметь возможность принимать необходимые меры.

Выбор дизайна CBDC имеет сильное влияние на конфиденциальность и безопасность данных. Определение учетных записей для каждого владельца требует подтверждения личности, что может создавать проблемы конфиденциальности. Основанный на токенах подход может обеспечить лучшую защиту данных, но существует риск потери денег при утрате ключа. Кроме того, некоторые решения в базовой технологической инфраструктуре могут увеличить проблемы конфиденциальности и защиты данных, такие как незаконное использование транзакционных данных и профилирование пользователей. Проект CBDC может значительно влиять на граждан юрисдикции центрального банка и повлечь за собой операции с высокими рисками для прав и свобод субъектов данных.[4]

Примером решения защиты персональных данных CDBC служит индийский рупий. Законопроект о DP регулирует обработку цифровых персональных данных, полученных как онлайн, так и офлайн. Он также применим к персональным данным, связанным с транзакциями и кошельком в цифровой рупии. Однако могут быть исключения для анонимных транзакций, если они соответствуют стандартам анонимности. Законопроект также распространяется на обработку персональных данных за пределами Индии в отношении товаров и услуг, предлагаемых субъектам данных в Индии. Применимость к трансграничным транзакциям зависит от того, как RBI будет использовать цифровую рупию на международном уровне и будут ли подпадать иностранные центральные банки под действие законопроекта.[5]

В данном анализе основным вопросом является идентификация доверителя данных, полученных в результате использования цифровой рупии. Закон о ДП определяет доверенные лица данных, которыми являются организации, определяющие цель и средства обработки данных. На эти организации распространяются требования, включая получение согласия, реализацию мер безопасности и ответ на запросы на доступ к данным и их удаление. Цифровая рупия, вероятно, будет считаться важной национальной инфраструктурой, а организации, считающиеся доверенными лицами данных, будут подвергаться повышенным требованиям, включая назначение сотрудника по защите данных,

независимого аудитора данных и проведение периодической оценки воздействия на защиту данных.

Архитектура CBDC, принятая RBI, может повлиять на классификацию доверителя данных. В предлагаемой модели RBI будет хранить агрегированные данные о транзакциях на банковском уровне, в то время как банки будут регистрировать только детальные розничные транзакции. В этом случае банки могут быть классифицированы как доверенные лица данных, так как RBI не будет иметь доступа к персональным данным пользователей. Другая модель предполагает регистрацию розничных транзакций как RBI, так и посредниками, для обеспечения безопасности конечных пользователей. В зависимости от выбранной модели цифровая рупия будет выпущена RBI, а банки будут собирать и обрабатывать данные от его имени. RBI определит цели, для которых банки могут обрабатывать эти данные, и в этом случае он будет доверенным лицом данных, а банки — обработчиками данных. Эта классификация имеет серьезные последствия, так как возложение обязательств по хранению данных на RBI потребует значительных финансовых и человеческих ресурсов для соблюдения требований по фидуциарным данным. [5]

Идентифицированному доверителю данных необходимо получить согласие пользователя перед обработкой его персональных данных. Банки уже получают согласие при подключении, поэтому им будет легко сделать это и для цифровой рупии. Однако если RBI является доверенным лицом данных, ему нужно будет помочь банкам получить согласие от имени RBI. RBI также несет ответственность за управление согласием, даже если оно не собирает его напрямую. Согласие может не требоваться, если оно предоставлено посредством предполагаемого согласия в законопроекте о DP. Идентифицированный фидуциарий данных может полагаться на условное согласие, если есть обоснованное ожидание предоставления данных. Предполагаемое согласие также может быть использовано при предоставлении государственных услуг или выгод. Однако использование предполагаемого согласия должно быть обоснованным и хорошо продуманным, чтобы не ослабить защиту конфиденциальности.

BIG DATA может помочь с проблемами безопасности национальной цифровой валюты.

1. Обнаружение мошенничества и кибератак:

BIG DATA предоставляет огромные объемы данных, которые могут быть анализированы для обнаружения мошеннических операций и кибератак. Анализ множества данных позволяет выявить аномалии и необычные паттерны в поведении пользователей, что может указывать на потенциальные угрозы безопасности. Технология BIG DATA может помочь в реальном времени отслеживать и предотвращать подобные атаки.

2. Улучшение идентификации пользователей:

Безопасность цифровой валюты может быть значительно усилена благодаря точной идентификации пользователей. BIG DATA позволяет собирать и анализировать данные о поведении пользователей и на их основе строить уникальные профили. Такая информация помогает выявлять подозрительные действия и контролировать доступ к цифровой валюте только у легитимных пользователей.

3. Анализ и предсказание угроз:

BIG DATA предоставляет возможность для анализа огромных объемов данных, связанных с безопасностью цифровой валюты. Это позволяет выявить скрытые угрозы и предсказать потенциальные уязвимости. Аналитика данных может помочь в реализации мер безопасности, направленных на устранение или предотвращение таких угроз.

4. Улучшение защиты данных и конфиденциальности:

BIG DATA подразумевает сочетание различных технологий и методов для защиты данных и обеспечения конфиденциальности. Защита приватности и регулирование доступа важны для обеспечения безопасности национальной цифровой валюты. Технологии BIG DATA могут помочь в реализации этих мер безопасности, гарантируя, что личные данные пользователей будут надежно защищены.

Преимущества применения BIG DATA для обеспечения безопасности

A. Анализ больших объемов данных

Огромный объем информации, создаваемой человечеством, растет очень быстро. За последние два года количество данных в мире выросло почти вдвое. Только в 2020 году люди сгенерировали 59 зеттабайт данных, что эквивалентно огромному количеству фильмов в разрешении 4K. Обработка и систематизация этих данных с помощью BIG DATA позволяют найти скрытые закономерности и принимать лучшие решения как в масштабных проектах, так и в небольших компаниях.

Эффективность и безопасность работы на современных производственных предприятиях связаны с непрерывным мониторингом параметров через сеть устройств, собирающих информацию на IoT-платформе и обрабатывающих ее в режиме реального времени с помощью алгоритмов BIG DATA. Использование инструментов работы с BIG DATA позволяет отслеживать износ оборудования и проводить своевременное техническое обслуживание, предотвращая аварии.

Внедрение аналитики больших данных совместно с IoT также может быть полезным для жилищно-коммунальных хозяйств, ТЭЦ, ГЭС. Внедрение современных технологий в сфере ЖКХ может привести к значительной экономии. Например, в Москве внедрение автоматизированной системы сбора и обработки данных о потреблении горячей воды в многоквартирных домах может сэкономить до 980 миллионов рублей в год на устранении перегрева при подаче отопления в большем объеме, чем требуется.

В банковской сфере анализ больших данных позволит определить, для каких направлений люди берут кредиты, сумму и срок, а вместе с информацией о доходах позволит подобрать оптимальную программу.

B. Обнаружение аномалий и предупреждение о возможных угрозах

Обнаружение аномалий является важной частью обеспечения безопасности в различных сферах деятельности, от финансовых учреждений до государственных организаций. Аномалии могут возникнуть в различных формах: от несанкционированного доступа к данным до вредоносных атак на информационные системы. Обнаружение таких аномалий является сложной задачей, требующей постоянного мониторинга и анализа больших объемов данных.

С помощью BIG DATA аналитики имеют возможность обрабатывать огромные объемы данных в реальном времени и выявлять нетипичные и аномальные паттерны. За счет использования машинного обучения и алгоритмов, обученных на больших данных, возможны автоматическое обнаружение угроз и предупреждение о них. Например, в банковской сфере BIG DATA может использоваться для обнаружения мошеннических операций. Анализируя огромные объемы данных о транзакциях клиентов, системы могут выделить нетипичные ситуации, такие как необычные суммы переводов или странные местоположения операций. Это позволяет оперативно реагировать на потенциальные мошеннические действия и предупреждать клиентов об угрозах.

BIG DATA также может использоваться для обнаружения аномалий в сетевом трафике и защите от кибератак. Анализируя информацию о трафике в реальном времени, система может обнаружить подозрительные активности, такие как необычные запросы, массовые попытки взлома или распространение вредоносных программ. Такие данные позволяют принимать меры по обеспечению безопасности системы и предупреждать о возможных угрозах.

C. Усиление системы проверки личности

Развитие цифрового банкинга существенно изменило то, как мы управляем своими финансами, и, как следствие, как растет потребность в надежных системах проверки личности. Знай своего клиента (KYC) — это важнейший аспект цифрового банкинга, гарантирующий, что клиенты являются теми, кем они себя называют, и обеспечивающий безопасную основу для финансовых транзакций. С ростом киберугроз потребность в

передовых системах проверки личности для защиты от мошенничества и несанкционированного доступа становится более острой, чем когда-либо.[6]

В современном мире проверка личности в цифровом банкинге все актуальнее. Однако существуют ограничения и проблемы, включая недостаточную безопасность при использовании простых паролей и слабых алгоритмов шифрования, необходимость носить дополнительные устройства, такие как USB-ключи, и возможные ошибки в распознавании биометрии. Развиваются более совершенные технологии, такие как двухфакторная аутентификация и использование искусственного интеллекта и блокчейна для повышения безопасности. Важно, чтобы банки и финансовые учреждения продолжали совершенствовать методы проверки личности, чтобы создавать надежную и безопасную среду для цифрового банкинга.

Эти методы, хотя и широко используются, могут быть следующими:

- подвержены мошенничеству, поскольку мошенники могут получить поддельные личности или использовать украденную личную информацию для создания поддельных учетных записей,
- отнимает много времени и неудобно для клиентов, что приводит к негативному влиянию на качество обслуживания клиентов,
- неточными или недостаточно безопасными, что потенциально может привести к финансовым потерям для клиентов и финансовых учреждений,
- не соответствует новым правилам конфиденциальности данных, таким как GDPR и AML, что приводит к потенциальным юридическим рискам для финансовых учреждений.

Для обхода двухфакторной аутентификации злоумышленнику необходимо знать устройство, с которого выполняет вход пользователь, в какое время совершается вход и браузер в случае, если банк не имеет приложения или пользователь выполняет вход через персональный компьютер или ноутбук, всю эту информацию можно получить через форумы в даркнете. Злоумышленник при помощи социальной инженерии загружает вирусное ПО на телефон жертвы, тем самым получает пароль и прочую информацию.

Сфера цифрового банкинга постоянно развивается, появляются новые технологии проверки личности. Тремя перспективными направлениями развития являются: биометрическая аутентификация, управление идентификацией на основе блокчейна и системы обнаружения мошенничества на основе искусственного интеллекта.

1) Биометрическая аутентификация удобна и точна, но возникают опасения по поводу конфиденциальности данных.
2) Управление идентификацией на основе блокчейна обеспечивает безопасность и прозрачность, но требует значительных инвестиций.
3) Системы обнаружения мошенничества на основе искусственного интеллекта помогают предотвратить мошенничество, но могут быть предвзятыми или содержать ошибки.

Финансовые учреждения должны тщательно рассмотреть преимущества и недостатки каждой технологии перед внедрением.

D. Обеспечение безопасности при финансовых операциях

Применение BIG DATA в финансовых операциях — анализ поведения клиента для определения рисков и предотвращения мошенничества. Обнаружение аномалий и необычных событий на основе массового анализа данных. Важность защиты личных данных клиентов и соблюдение конфиденциальности и законодательства.

E. Прогнозирование вероятных проблем безопасности

В наше время идентификация возможных угроз и уязвимостей в системах безопасности — задача, требующая системного и глубокого подхода. Важно учитывать не только существующие угрозы, но и предвидеть будущие тенденции в области кибербезопасности, чтобы быть впереди потенциальных проблем.

Для прогнозирования вероятных проблем безопасности необходимо применять интеллектуальные методы аналитики данных. Сбор, анализ и интерпретация крупных объемов информации помогут выявить тенденции и паттерны, которые могут привести к возникновению угроз безопасности. Такие методы, как машинное обучение и искусственный интеллект, могут значительно повысить эффективность прогнозирования и помочь вовремя предотвратить возможные проблемы.

Одним из ключевых аспектов прогнозирования вероятных проблем безопасности является анализ предшествующих инцидентов и их последствий. Изучение атак и их последствий поможет определить общие паттерны и уязвимости, которые могут быть использованы хакерами в будущем. Комплексный подход к анализу инцидентов и создание базы знаний о предыдущих угрозах и атаках поможет прогнозировать потенциальные проблемы и разработать соответствующие меры безопасности.

Еще одним важным аспектом прогнозирования проблем безопасности является постоянное обновление и совершенствование систем безопасности. Технологии и методы атак постоянно эволюционируют, и системы защиты должны быть готовы к новым угрозам. Постоянное обновление инфраструктуры и обучение персонала являются неотъемлемыми элементами успешной борьбы с проблемами безопасности.

Примеры применения BIG DATA в обеспечении безопасности национальной цифровой валюты

A. Использование алгоритмов машинного обучения для обнаружения мошенничества

Прогнозирование вероятных проблем безопасности — важная часть обеспечения безопасности информации и инфраструктуры организации. Использование анализа исторических данных и мониторинг активности в сети помогает нам выявить общие закономерности и предсказывать будущие атаки. Обучение персонала и обновление систем безопасности также играют роль в борьбе с угрозами. Однако прогнозирование не является стопроцентно точным, поэтому постоянное обновление и модернизация систем безопасности являются необходимыми. Применение современных технологий и методов анализа данных помогает эффективно предвидеть и предотвращать угрозы. Непрерывное улучшение защиты и обучение персонала — ключевые факторы в обеспечении безопасности информации и инфраструктуры.

B. Анализ данных для идентификации подозрительных транзакций

Анализ данных для идентификации подозрительных транзакций — это процесс сбора, обработки и анализа информации, связанной с финансовыми операциями, с целью обнаружения аномалий и подозрительных действий.

Основными инструментами, используемыми в анализе данных, являются статистические методы, модели машинного обучения и алгоритмы. С их помощью производятся множественные проверки, исследуются шаблоны поведения, определяются аномалии и строятся прогнозы по возможным рисковым сценариям.

Одной из ключевых задач анализа является выделение "красных флагов" — признаков потенциально подозрительной транзакции. К таким признакам могут относиться необычные суммы переводов, несоответствие места расположения отправителя и получателя, странные покупки или снятие наличных, несоответствие паттерна клиента и т.д. Эффективность анализа данных для идентификации подозрительных транзакций заключается в своевременном обнаружении мошеннической активности. Благодаря своей автоматизированной и непрерывной природе эта система способна предотвратить финансовые потери, связанные с мошенничеством, и минимизировать возможный репутационный риск для компании.

Однако следует учитывать, что системы анализа данных не являются идеальными и могут давать ложные срабатывания. Поэтому важно создать надежную и непрерывно обновляемую систему, которая будет адаптироваться к постоянно меняющимся моделям

мошеннического поведения и обладать высокой степенью точности в выявлении реальных рисков.

C. Системы мониторинга и обнаружения аномалий

Основные этапы процесса обеспечения безопасности информации, реализация которых требует проведения оценки:

1) оценка рисков нарушения безопасности информации;
2) анализ информационных потоков и архитектуры;
3) анализ модели угроз и нарушителя безопасности информации;
4) разработка политики информационной безопасности;
5) построение системы защиты информации;
6) оценка эффективности системы защиты информации;
7) управление процессами защиты информации и инцидентами;
8) контроль обеспечения безопасности информации.

Для оценки безопасности информационной системы нужно провести классификацию и анализ ее физических и логических элементов. Это включает использование методов моделирования и упрощение модели для разрешения задачи. При увеличении сложности системы точность модели снижается, что недопустимо для критических информационных систем. Для повышения достоверности результатов моделирования можно использовать методы BIG DATA.

Основные принципы обеспечения безопасности персональных данных при использовании технологии Big Data в соответствии с Мавританской резолюцией[7]:

1) Открытость в информации о составе собираемых сведений, их обработке, целях использования и передачи третьим лицам.
2) Определение цели сбора информации непосредственно во время ее сбора и ограничение использования данных исключительно установленной целью.
3) Получение согласия на использование данных.
4) Сбор и хранение только того объема данных, который необходим для реализации намеченных законных целей.
5) Предоставление персонального доступа лицам к тем данным, которые были собраны о них, обеспечение информацией об источниках данных и любых алгоритмах, используемых для дальнейшего развития их профиля.
6) Предоставление лицам возможности исправления и управления своей информацией.
7) Проведение анализа того, как сбор информации влияет на неприкосновенность частной жизни пользователя.
8) Анонимизация (обезличивание) данных.
9) Ограничение и контроль доступа к персональным данным.
10) Проведение регулярного анализа для подтверждения того, что результаты профилирования «надежны, справедливы и этичны, а также отвечают той цели, для достижения которой и используются профили».

Заключение

В заключение: применение BIG DATA в обеспечении безопасности национальной цифровой валюты имеет многочисленные преимущества, которые помогают предотвращать мошенничество, обнаруживать потенциальные уязвимости и повышать надежность системы. Однако необходимо учитывать и риски, связанные с конфиденциальностью данных. В целом применение BIG DATA является важным шагом в обеспечении безопасности и надежности национальной цифровой валюты, и его эффективное использование помогает обеспечить стабильность и успех этой инновационной системы.

Прежде всего использование BIG DATA позволяет собирать и анализировать огромные объемы данных, связанных с транзакциями и активностью пользователей. Это позволяет выявлять паттерны и необычное поведение, что может указывать на потенциальные

кибератаки или мошенничество. Большой объем данных позволяет эффективно фильтровать информацию, и о нарушении безопасности могут быть извлечены данные, которые помогут в реагировании на угрозы.

Кроме того, BIG DATA позволяет проводить анализ рисков и прогнозирование потенциальных уязвимостей системы. Алгоритмы, работающие на больших объемах данных, могут выявить узкие места или слабые места в безопасности национальной цифровой валюты и предложить меры по их усилению. Это существенно снижает вероятность успешного вторжения или атаки на систему. Значительное преимущество применения BIG DATA в области безопасности национальной цифровой валюты заключается в обнаружении и предотвращении финансовых мошенничеств. Анализ огромного количества данных позволяет выявить аномалии, связанные с незаконными финансовыми транзакциями. Это позволяет оперативно реагировать на потенциальные угрозы, предотвращать финансовые потери и защищать интересы пользователей национальной криптовалюты.

Однако, несмотря на все преимущества применения BIG DATA в безопасности национальной цифровой валюты, существуют и риски. Например, возникает потенциальная опасность нарушения конфиденциальности данных пользователей при сборе и анализе их личной информации. Этот аспект должен быть тщательно учтен, и меры должны быть приняты для защиты приватности пользователей и соответствия законодательству о защите персональных данных.

Список использованных источников

1. 大数据(Большие данные) - .- URL: https://baike.baidu.com/item/%E5%A4%A7%E6%95%B0%E6%8D%AE/1356941#reference-3 (дата обращения: 02.02.2024). Текст: электронный
2. Саяков, Д. (2023). ОСОБЕННОСТИ РАЗВИТИЯ ЦИФРОВОЙ ВАЛЮТЫ И ПЕРСПЕКТИВНЫЕ ПРИМЕНЕНИЯ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ. Проблемы автоматики и управления, (1), 96–105. извлечено от https://pau.imash.kg/index.php/pau/article/view/404
3. Саяков, Д. А. Исследование и разработка механизмов защиты национальной цифровой валюты в контексте информационной безопасности / Д. А. Саяков, Г. О. Крылов, В. А. Рычков // Кибернетика и информационная безопасность «КИБ-2023» : Сборник научных трудов Всероссийской научно-технической конференции, Москва, 18–19 октября 2023 года. – М.: Национальный исследовательский ядерный университет "МИФИ", 2023. – С. 142–143. – EDN FQGDEY. https://www.elibrary.ru/item.asp?id=54719670&selid=54719752
4. Central Band Digital Currency – European Data Protection Supervisor - .- URL: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://edps.europa.eu/system/files/2023-03/23-03-29_techdispatch_cbdc_en.pdf&ved=2ahUKEwjV0umtuYyEAxXBHhAIHclpCykQFnoECDYQAQ&usg=AOvVaw0bKMmYH-Eolw7PGwRpbRsU (дата обращения: 02.02.2024). Текст: электронный.
5. Towards a CBDC-Friendly Data Protection Regulation - .- URL: https://www.ijlt.in/post/towards-a-cbdc-friendly-data-protection-regulation (дата обращения: 02.02.2024). Текст: электронный.
6. The Future of Identity Verification in Digital Banking: Trends, Technologies, and Opportunities - .- URL: https://fully-verified.com/identity-verification-in-digital-banking/ (дата обращения: 05.02.2024). Текст: электронный.
7. Перспективы применения Big Data для обеспечения безопасности критических информационных систем - .- URL: https://digital.report/big-data/ (дата обращения: 06.02.2024). Текст: электронный