АНАЛИЗ УЯЗВИМОСТЕЙ СИСТЕМ УПРАВЛЕНИЯ КЛЮЧАМИ В РАСПРЕДЕЛЕННЫХ РЕЕСТРАХ НА ПРИМЕРЕ БЛОКЧЕЙН IBM

Плоткин А.С.[1], Кесель С.А[2]., Репин М.М.[3], Федоров Н.В.[4]

Аннотация.

На сегодняшний день одной из самых обсуждаемых тем в сфере информационных технологий являются системы распределенных реестров. Они привлекают инвесторов и разработчиков своей функциональностью. Системы распределенных реестров внедряются в бизнес-процессы во многих областях деятельности человека, что делает их вклад в развитии незаменимым. Одной из наиболее уязвимых частей таких систем является процесс управления криптографическими ключами, атака на который может быть критичной для системы распределенных реестров.

***Целью исследования** является выявление потенциальных угроз информационной безопасности процесса управления криптографическими ключами, на основе которых будут разработаны рекомендации и стандарты управления криптографическими ключами в системах распределенных реестров.*

***Методы исследования:** для достижения поставленной цели была рассмотрена структура жизненного цикла криптографических ключей, проведён анализ возможных уязвимостей процесса управления криптографическими ключами на каждом из этапов жизненного цикла криптографического ключа. Помимо этого, была проанализирована система распределенных реестров в разрезе выделенных уязвимостей процесса управления ключами на примере блокчейн IBM и рассмотрена возможность аутсорсинга систем управления криптографическими ключами.*

***Полученный результат:** предложен набор потенциальных угроз информационной безопасности процесса управления криптографическими ключами, обоснована необходимость оценки безопасности системы управления ключами перед решением о внедрении данных систем в распределенные реестры, сделаны выводы о необходимости разработки рекомендаций и стандартов по процессу управления криптографическими ключами для подобных систем, а также возможности применимости рекомендаций для оценки безопасности внедрения аутсорсинга систем управления криптографическими ключами в распределенные реестры.*

***Ключевые слова:** информационные технологии, угрозы безопасности информации, информационная безопасность, жизненный цикл криптографических ключей, аутсорсинг криптографических ключей, компенсирующие меры, защита криптографических ключей, семантика, метрики, онтология, кибератака, информационная система, интеллектуальный анализ данных.*

DOI: 10.21681/2311-3456-2021-2-61-70

Введение

На сегодняшний день одной из самых обсуждаемых тем в сфере информационных технологий являются системы распределенных реестров. Подобные системы внедряются в по всему миру во многих областях деятельности человека, в том числе образовании, медицине, финансовой сфере и иных областях.

Информационная безопасность подобных систем в первую очередь построена на криптографии, так как технология распределенных реестров основана на применении механизмов электронной подписи, безопасность которых, в основном, определяется именно безопасностью криптографического ключа. Из этого следует, что в технологии распределенных реестров значительное влияние на эффективность использования криптографии при комплексной защите информации оказывает подход к управлению криптографическими ключами. [1]

Ненадлежащее управление криптографическими ключами может поставить под угрозу криптостойкость применяемых алгоритмов. В результате безопасность информации, которая обеспечивается с применени-

1 Плоткин Александр Сергеевич, аспирант кафедры Информационной безопасности Московского Политехнического университета, г. Москва, Россия. E-mail: sances.98@mail.ru.

2 Кесель Сергей Александрович, кандидат технических наук, доцент кафедры Информационной безопасности Московского Политехнического университета, г. Москва, Россия. E-mail: sakesel161@gmail.com.

3 Репин Максим Михайлович, руководитель направления Научно-исследовательского института «Восход», г. Москва, Россия. E-mail: bmstu.iu8@gmail.com.

4 Федоров Николай Владимирович, кандидат технических наук, доцент, заведующий кафедрой Информационной безопасности Московского Политехнического университета, г. Москва, Россия. E-mail: fedorovnv31@mail.ru.

ем криптографии, напрямую зависит от силы ключей, а также эффективности механизмов и протоколов, связанных с их работой. [2]

Со всеми вышеописанными проблемами чаще всего сталкиваются молодые развивающиеся компании, либо компании, которые только начали процесс автоматизации и внедрения информационных технологий, и, в частности, систем распределенных реестров. Поэтому многие из них прибегают к услугам аутсорсинга для построения систем управления ключами. [3]

Для разработки необходимых мер безопасности процесса управления криптографическими ключами необходимо рассматривать весь жизненный цикл криптографических ключей.

Жизненный цикл криптографических ключей

Жизненный цикл криптографических ключей – это набор состояний, в которых пребывает ключ за время своего существования в автоматизированной системе.

Для любого объекта стандартизации определяются четыре стадии жизненного цикла:

- Предоперационная стадия – криптографический ключ не доступен для эксплуатации в криптосистеме;
- Операционная стадия – криптографический ключ доступен пользователям криптосистемы и эксплуатируется;
- Постоперационная стадия – криптографический ключ выходит из эксплуатации, но остается доступен в особом режиме для специальных целей;
- Стадия выхода из эксплуатации – криптографический ключ становится недоступен, а все записи, содержащие значение криптографического ключа, удаляются из криптосистемы.

Можно также разделить этапы жизненного цикла криптографических ключей на:

- **Генерацию криптографических ключей** – этап включает в себя принятие мер по обеспечению необходимых криптографических качеств ключа;
- **Регистрацию криптографических ключей** – этап включает в себя регистрацию криптографического ключа в базе и выдачу ему сертификата;
- **Распределение криптографических ключей** – этап включает в себя распределение ключей их владельцам по защищенному каналу;
- **Инициализацию пользователя** – этап включает в себя аутентификацию пользователя перед передачей ему криптографического ключа;
- **Эксплуатацию криптографических ключей** – этап, включающий использование ключей для защиты информации в обычном режиме;
- **Обновление криптографических ключей** – этап, на котором происходит замена криптографического ключа с истекшим криптопериодом на новый;
- **Восстановление криптографических ключей** – этап, включающий восстановление криптографического ключа, который был утерян без вероятности его компрометации;
- **Аннулирование криптографических ключей** – этап, включающий отзыв криптографических ключей из эксплуатации в результате истечения криптопериода либо компрометации;
- **Хранение и архивация криптографических ключей** – этап включает процедуры, необходимые для хранения ключа в надлежащих условиях, обеспечивающих его безопасность до момента его замены, а также архивацию и хранение криптографических ключей, вышедших из оборота до момента их удаления;
- **Уничтожение криптографических ключей** – этап, включающий уничтожение ключа и его копий после окончания срока их действия, а также при компрометации.

Полный жизненный цикл криптографических ключей представлен ниже. (рис.1)

Для полноценной защиты процесса управления криптографическими ключами необходимо учитывать все вышеописанные этапы жизненного цикла криптографических ключей. Для этого проведем исследование потенциальных угроз информационной безопасности процесса управления криптографическими ключами.

Исследование потенциальных угроз информационной безопасности процесса управления криптографическими ключами

Рассмотрим потенциальные угрозы к процессу управления криптографическими ключами по каждому из выделенных этапов на основе публичных отчётов из сети интернет о реализованных атаках или попытках атаки. (рис. 2) [4]

Структуру описания угроз предлагаем построить следующим образом:

- Название угрозы;
- Описание угрозы;
- Мера смягчения – меры, предлагаемые для снижения вероятности возникновения угрозы.

Опишем основные угрозы на этапе генерации криптографических ключей:

– Угроза генерации слабого криптографического ключа. Угроза заключается в том, что в результате неудачного выбора генератора случайных чисел может быть выбрано число, которое приведёт к получению слабого криптографического ключа.

В качестве компенсирующих мер можно предложить следующие: надежность криптографических ключей должна соответствовать значению данных, которые он защищает, и периоду времени, в течение которого он должен быть защищен. Криптографический ключ должен быть достаточно длинным для его предназначения и генерироваться с использованием высококачественного генератора случайных чисел, в идеале собирающего энтропию от подходящего аппаратного источника.

Опишем основные угрозы на этапе распределения и эксплуатации криптографических ключей:

– Угроза небезопасного распределение криптографических ключей. Угроза заключается в том, что одно из самых уязвимых мест, это процесс передачи криптографических ключей. В случае если этот процесс недостаточно защищен, ключи могут быть скомпрометированы [5].

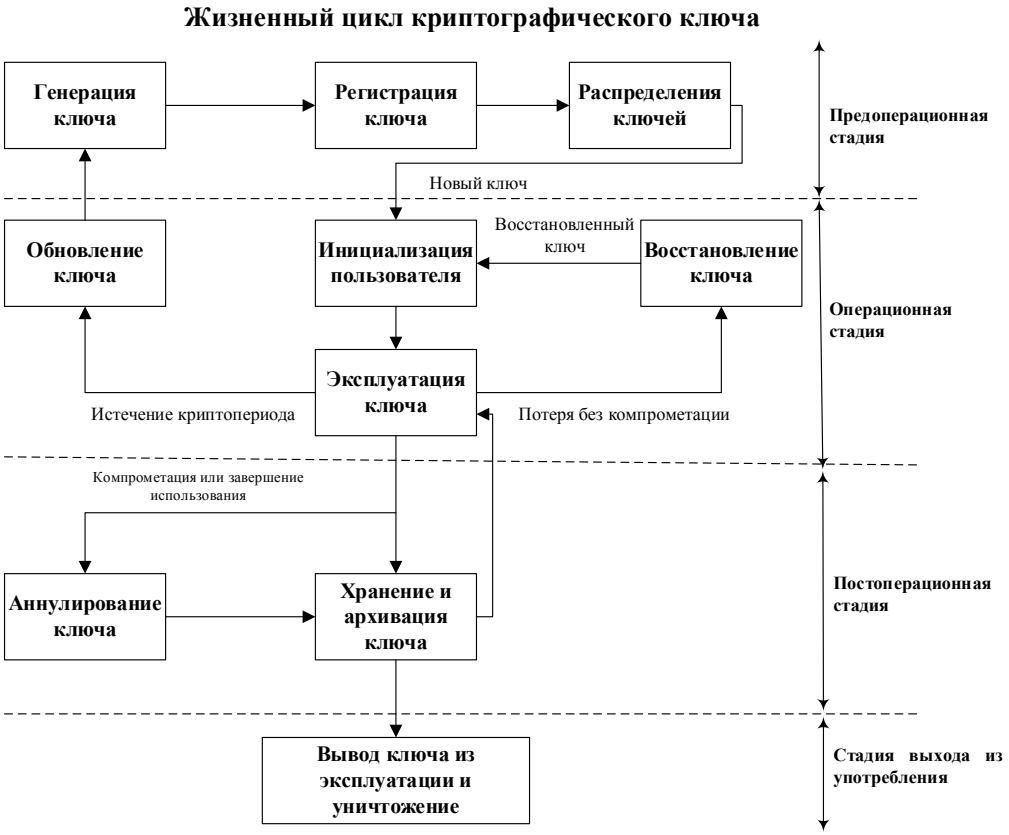

Рис. 1. Жизненный цикл криптографического ключа

В качестве компенсирующих мер можно предложить следующие: для распределения криптографических ключей следует использовать безопасные протоколы распределения криптографических ключей, а также придерживаться определенных правил (не передавать ключи по открытым каналам связи и др.) [6].

– Угроза неправильного использования криптографических ключей. Угроза заключается в том, что использование криптографических ключей для задач, не совпадающих с целью его генерации может привести к проблемам с требуемым уровнем защиты [7].

В качестве компенсирующих мер можно предложить следующие: каждый криптографический ключ должен генерироваться для одной конкретной цели (т. е. предполагаемого приложения и алгоритма).

– Угроза повторного использования криптографических ключей. Угроза заключается в том, что повторное использование криптографических ключей после их вывода из эксплуатации может привести к взлому криптографических ключей.

В качестве компенсирующих мер можно предложить следующие: повторное использование криптографических ключей не допустимо. Для выполнение новых операций должен быть сгенерирован новый криптографический ключ [8].

– Угроза использования криптографических ключей для шифрования больших объемов данных. Угроза заключается в том, что использование криптографических ключей для шифрования больших объемов данных (за раз или частое использование) может сделать его более уязвимым для взлома. [9]

В качестве компенсирующих мер можно предложить следующие: один криптографический ключ не следует использовать для шифрование больших объемов данных (за раз или частое использование). В случае необходимости следует сгенерировать новый криптографический ключ.

– Внутренние угрозы (злоумышленником может быть один из имеющих доступ к криптографическим ключам). Угрозы заключаются в том, что если мошенник может иметь постоянный доступ криптографическим ключам, то он сможет использовать его в злонамеренных целях или передать кому-то другому с той же целью.

В качестве компенсирующих мер можно предложить следующие: аутентификация пользователя, двойной контроль, разделение ролей [10].

Опишем основные угрозы на этапе хранения криптографических ключей:

– Угроза неправильного хранения криптографических ключей. Угроза заключается в том, что любая атака с фильтрацией защищенных данных может поставить под угрозу криптографические ключи. [11]

DOI: 10.21681/2311-3456-2021-2-61-70

Рис. 2. Классификация угроз к процессу управления криптографическими ключами

В качестве компенсирующих мер можно предложить следующие: криптографические ключи никогда не должны хранится вместе с данными, которые они защищают (например, на сервере, в базе данных и т.д.). [12]

– Угроза слабой защиты криптографических ключей. Угроза заключается в том, что криптографические ключи, если даже они хранятся только в памяти сервера, могут быть уязвимы для компрометации.

В качестве компенсирующих мер можно предложить следующие: независимо от места хранения криптографические ключи должны хранится в зашифрованном виде (исключение: защищенная от несанкционированного доступа среда). [13]

– Угроза недоступности криптографических ключей. Угроза заключается в том, что, если криптографические ключей недоступен при необходимости или утерян из-за какой-либо неисправности или аварии, а резервная копия недоступна, данные, которые он защищает, также могут быть недоступны или потеряны.

В качестве компенсирующих мер можно предложить следующие: место хранение криптографических ключей должно быть надежно защищено от отказа доступа, а для самих криптографических ключей должны хранится резервные копии на случай необходимости их восстановления.

– Угроза отсутствия ведения журнала криптографических ключей. Угроза заключается в том, что, если жизненный цикл криптографических ключей не полностью записывается или регистрируется, будет труднее определить, когда произошел инцидент, что повлияет на обеспечение информационной безопасности других криптографических ключей в будущем.

В качестве компенсирующих мер можно предложить следующие: необходимо вести журнал действий, производимых с криптографическими ключами. Журнал должен быть защищен от скороненного доступа и в идеале быть построен на распределенном реестре так, чтобы записи из него невозможно было бы удалить.

Опишем основные угрозы на этапе уничтожения криптографических ключей:

– Угроза не уничтожения криптографических ключей после истечения их срока эксплуатации. Угроза заключается в том, что не уничтоженные криптографических ключей могут быть скомпрометированы и использованы злоумышленниками.

В качестве компенсирующих мер можно предложить следующие: криптографические ключи должны быть уничтожены (т.е. надежно удалены, не оставляя следов) после истечения срока их действия, если это явно не требуется для последующего использования (например, для расшифровки данных).

– Угроза ручных процессов управления криптографическими ключами. Угроза заключается в том, что использование процессов ручного управле-

ния криптографическими ключами с использованием бумаги или неподходящих инструментов, таких как электронные таблицы, и сопровождаемых ручным вводом криптографических ключей приведут к ошибкам, которые могут сделать их крайне уязвимыми.

В качестве компенсирующих мер можно предложить следующие: для уменьшения вероятности возникновение ошибок управления криптографическими ключами следует доверить автоматизированной системе, предназначенной для этого и соответствующей требованиям по информационной безопасности.

После проведения анализа потенциальных угроз информационной безопасности процесса управления криптографическими ключами рассмотрим их на примере IBM Blockchain Platform.

Сеть IBM Blockchain Platform основана на доверенных идентификаторах. Участники блокчейна используют центры сертификации в консоли для создания идентификаторов и связанных сертификатов, которые требуются всем участникам для осуществления операций в сети.

Документация IBM Blockchain Platform содержит следующее утверждение: «управление ключами является критически важным аспектом безопасности. Если закрытый ключ скомпрометирован или утерян, враждебные субъекты могут получить доступ к данным и функциям».

Приведем правила и рекомендации, описанные в документации IBM Blockchain Platform к управления криптографическими ключами.

Этап генерации криптографического ключа:

- Генерация открытого и закрытого ключа происходит по алгоритму ECDSA с кривой P256.
- Если закрытый ключ утерян и не может быть восстановлен, то необходимо будет сгенерировать новый закрытый ключ и зарегистрировать новый идентификатор в центре сертификации.

Этап хранения криптографического ключа:

- Ключи хранятся в браузере, когда они добавляются в кошелек блокчейна участника, чтобы консоль могла использовать их для управления компонентами блокчейна.
- Клиентам рекомендуется экспортировать ключи и импортировать их в свою собственную систему управления криптографическими ключами на случай, если они очистят кэш браузера или переключат браузеры.
- Клиенты несут ответственность за хранение, резервное копирование и аварийное восстановление всех экспортируемых ключей.

Для генерации и хранения криптографического ключа IBM Blockchain Platform также предлагает использовать HSM (Hardware Security Module – аппаратный модуль безопасности). Он должен соответствовать стандарту FIPS 140-2 уровень 4. В случае использования HSM ответственность за правильную настройку и работу HSM несёт участник сети блокчейн. Также в этом случае применяются следующие правила управления криптографическими ключами: [14]

- Закрытый ключ для узла не должен сохранятся в кэше браузера.
- Закрытый ключ должен быть доступен из HSM через прокси.
- При регистрации идентификаторов администратора другого узла или клиентского приложения в центр сертификации с помощью консоли, их закрытые ключи не должны хранится в HSM, поскольку им нужен закрытый ключ для операции в сети.

IBM Blockchain Platform также предоставляет возможность использовать свои собственные сертификаты из собственного центра сертификации платформы Blockchain, не принадлежащего IBM. В этом случае участник блокчейна должен соблюсти следующие правила:

- При создании однорангового узла необходимо вручную создать файл определения поставщика абонентских услуг одноранговой службы, который включает сертификаты, и импортировать этот файл.
- Поставщик сервисов управления должен определять корневой центр сертификации, который сгенерировал сертификаты для организации, и любые другие роли помимо администратора, связанные с организацией.
- Поставщик сервисов управления должен устанавливать основу для определения привилегий доступа в контекст сети.

На основании проведенного анализа системы IBM Blockchain Platform и составленного описания проанализируем эти угрозы и дадим оценку степени защищенности от них.

Степень защищенности представлена следующими возможными результатами:

- **Полностью защищено** – инструмент безопасности полностью устраняет возможность возникновение угрозы.
- **Частично защищено** – инструмент безопасности частично (не полностью) или не во всех случаях устраняет возможность возникновение угрозы. Вероятность возникновения угрозы присутствует.
- **Не защищено** – инструмент безопасности отсутствует либо не выполняет своих функций. Высока вероятность возникновения угрозы.

Для проведения анализа угроз составим и заполним таблицу. (табл. 1):

В результате проведенного анализа IBM Blockchain Platform удалось оценить степень защищенности процесса управления криптографическими ключами и выявить, что существуют потенциальные угрозы информационной безопасности процесса управления криптографическими ключами.

Часто возникающие вопросы обеспечения информационной безопасности, в частности, вопросы обеспечения надлежащего управления криптографическими ключами, ведут к тенденции развития аутсорсинга процессов и механизмов, обеспечивающих информационную безопасность систем. Подобные механизмы определяются как системы управления криптографическими ключами.

DOI: 10.21681/2311-3456-2021-2-61-70

Таблица 1

Таблица угроз управления ключами в IBM Blockchain Platform

№	Угроза	Элемент безопасности управления криптографическими ключами	Степень защищенности
1	Генерация слабого криптографического ключа	Генерация открытого и закрытого ключа происходит по алгоритму ECDSA с кривой P256	Полностью защищено
2	Неправильное использование криптографических ключей	Возможно отсутствует	Не защищено
3	Повторное использование криптографических ключей	Правила управления криптографическими ключами	Полностью защищено
4	Использование криптографических ключей для шифрования больших объемов данных	Возможно отсутствует	Не защищено
5	Неправильное хранение криптографических ключей	Использование систем управления ключами либо использование сертифицированного HSM	Полностью защищено
6	Слабая защита криптографических ключей	Использование систем управления ключами либо использование сертифицированного HSM	Полностью защищено
7	Небезопасное распределение криптографических ключей	Использование систем управления ключами либо использование сертифицированного HSM	Полностью защищено
8	Не уничтожение криптографических ключей после истечения его срока эксплуатации	Возможно отсутствует	Не защищено
9	Внутренние угрозы (злоумышленником может быть один из имеющих доступ к криптографическому ключу)	Возможно отсутствует. В случае использования сертифицированного HSM - подразумеваться	Частично защищено
10	Недоступность криптографических ключей	Клиенты несут ответственность за хранение, резервное копирование и аварийное восстановление всех экспортируемых ключей	Частично защищено
11	Отсутствие ведения журнала криптографических ключей	Возможно отсутствует. В случае с HSM - встроено	Частично защищено
12	Ручные процессы управления криптографическими ключами	Использование систем управления ключами либо использование сертифицированного HSM	Полностью защищено

Рис. 3. Архитектура системы управления криптографическими ключами

Структура систем управления криптографическими ключами и их применение в системах распределенных реестров

Система управления криптографическими ключами — это централизованная система управления ключами, которая обеспечивает автоматическое обновление и распространение ключей. Она позволяет управлять всем жизненным циклом всех ключей (симметричных и асимметричных) [15].

Подобные системы в основном предоставляют схожий функционал:

- генерация, резервное копирование, восстановление, обновление;
- распределение криптографических ключей;
- обеспечение контроля безопасности;
- ведение журналов аудита и использования;
- шифрование с использованием ключей шифрования ключей (мастер-ключей);
- сертификация (например, с использованием сертификатов X.509).

Примерная архитектура системы управления криптографическими ключами представлена ниже (рис. 2).

Системы управления криптографическими ключами уже нашли применение в системах распределенных реестров. Так, например, некоторые системы управления криптографическими ключами внедряются в системы распределенных реестров на уровне узлов, в результате чего, каждый зарегистрированный узел получает права доступа к положенным для него криптографическим ключам, а также к управлению хранилищем и контролем доступа криптографических ключей.

Несмотря на полезность и удобство подобных аутсорсинговых решений, необходимо четко понимать, что перед внедрением любого нового компонента безопасности в существующую систему следует рассмотреть возможные проблемы, связанные с информационной безопасностью, которые могут возникнуть в связи с его внедрением. Данное правило касается также и системы управления криптографическими ключами, но для проведения подобной оценки нет описанных методов и на текущий момент это происходит по-разному в каждом конкретном случае.

Необходимость создания методики оценки информационной безопасности системы управления криптографическими ключами

В связи с отсутствием описанной методики оценки информационной безопасности системы управления криптографическими ключами, после её внедрения могут возникнуть проблемы с безопасностью, так как специалист, проводивший оценку может упустить какие-то важные составляющие технологии.

Одним из немногих возможных документов, содержащих параметры, применимые для оценки являются сертификаты соответствия требованиям таких документов, как:

- **FIPS 140-2** – стандарт компьютерной безопасности правительства США, используемый для утверждения криптографических модулей;
- **PCI-DSS** – стандарт безопасности данных индустрии платежных карт;
- **PCI-HSM** – набор стандартов соответствия логической и физической безопасности для HSM специально для индустрии платежей.

Это позволяет примерно оценить информационную безопасность систем управления криптографическими ключами. Но для более качественной оценки необходимо выбрать параметры, критически важные для сохранения информационной безопасности систем, в которые будет внедряться система управления криптографическими ключами и разработать методику оценки на основе этих параметров.

В качестве таких параметров могут выступать:

- безопасность криптографического алгоритма;

DOI: 10.21681/2311-3456-2021-2-61-70

- протокол распределения криптографических ключей;
- использования процедур идентификации и аутентификации узлов системы;
- процедуры разграничения прав доступа.

Полный список может включать в себя большое количество подобных параметров. Следует установить наиболее критичные из них, отсутствие или не соответствие которых в системах управления криптографическими ключами может быть причиной отказа от внедрения подобной системы, а также параметры, не являющиеся критическими или относящиеся к специфичным, могут быть использованы при сравнении оценок двух разных систем управления криптографическими ключами.

Выводы

В результате проведенных исследований и анализа были выявлены угрозы и уязвимости процессов управления криптографическими ключами. На основе этого перечня был проанализирован блокчейн IBM, и на основании описания его структуры и функционала сделаны выводы о существовании потенциальных угроз информационной безопасности процесса управления криптографическими ключами.

Помимо этого, была исследована возможность передачи процесса управления криптографическими ключами на аутсорсинг сторонним организациям, что, в свою очередь, также должно осуществляться после анализа безопасности подобной операции. Из этого следует необходимость разработки метода оценивания подобных аутсорсинговых решений.

Метод оценивания, в первую очередь, должна основываться на параметрах, критически важных для сохранения информационной безопасности систем, в которую будет внедряться система управления криптографическими ключами. Помимо этого, метод должен учитывать и специфичные параметры различных систем управления криптографическими ключами для возможности сравнения их между собой и выбора наиболее подходящей.

Литература

1. O. Pal, B. Alam, V. Thakur, S. Singh, Key management for blockchain technology. ICT Express (2019). DOI: 10.1016/j.icte.2019.08.002
2. Храмова Н.А. Исследование криптосистемы RSA для шифрования информации // Современные наукоемкие технологии. 2020. №9. С. 88-93.
3. Lenz, Rainer. Managing Distributed Ledgers: Blockchain and Beyond (March 26, 2019). SSRN Electronic Journal. DOI: 10.2139/ssrn.3360655.
4. W. Licheng, S. Xiaoying, L. Jing, S. Jun, Y. Yixian Cryptographic primitives in blockchains // Journal of Network and Computer Applications. 2019. №127. С. 43-58.
5. M. Mingxin, Y. Xiaotong, S. Guozhen, L. Fenghua Enhanced blockchain based key management scheme against key exposure attack // AIIPCC ‘19: Proceedings of the International Conference on Artificial Intelligence, Information Processing and Cloud Computing. 2019. С. 1-6.
6. Кривоногов А.А., Репин М.М., Федоров Н.В. Методика анализа уязвимостей и определения уровня безопасности смарт-контрактов при размещении в системах распределенных реестров // Вопросы кибербезопасности. 2020. №4 (38). С. 56-65.
7. 10.21681/2311-3456-2020-04-56-65
8. Victor Ribeiro, Raimir Holanda, Alex Ramos, Joel J. P. C. Rodrigues Enhancing Key Management in LoRaWAN with Permissioned Blockchain // Sensors. 2020. С. 1-16. DOI: 10.3390/s20113068
9. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah and Z. Sun, “Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems,” in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1832-1843, Dec. 2017, DOI: 10.1109/JIOT.2017.2740569.
10. W. F. Ehrsam, S. M. Matyas, C. H. Meyer and W. L. Tuchman, “A cryptographic key management scheme for implementing the Data Encryption Standard,” in IBM Systems Journal, vol. 17, no. 2, pp. 106-125, 1978, DOI: 10.1147/sj.172.0106.
11. Кузьменко В.В., Макаров В.Л., Разгуляев К.А., Хан Д.В., Щербаков А.Ю. Новый подход к обеспечению безопасности периметра бизнес-процессов и аутентификации пользователей в корпоративной системе // Вестник современных цифровых технологий. 2020. №3. С. 10-13.
12. Sathya Priya S, Revathy S, Kamnag R, Yogeswar L, Sajal M, Suparna S Distributed Key Management for IT Infrastructure using Block Chain and Hash Graph // International Journal of Recent Technology and Engineering (IJRTE). 2019. С. 533-537.
13. Разгуляев К.А., Рязанова А.А., Хан Д.В., Щербаков А.Ю. Об одном способе хранения и управления ключами в системах квантовых коммуникаций // Вестник современных цифровых технологий. 2020. №2. С. 14-20.
14. Rui Zhang, Rui Xue, Ling Liu Security and Privacy on Blockchain // ACM Computing Surveys. 2019. С. 1-35.
15. Панков К. Н. Использование криптографических средств для сквозных цифровых технологий на примере систем распределенного реестра // Технологии информационного общества. Материалы XII Международной отраслевой научно-технической конференции. 2018. С. 365-366.
16. Pankova V.V., Mironenko A.D. Cryptographic key management systems // Информационно-коммуникативная культура: Наука и Образование Сборник статей Международной научно-практической конференции студентов, аспирантов и молодых ученых. Министерство образования и науки Российской Федерации, Донской государственный технический университет. 2018. С. 191-193.

ANALYSIS OF VULNERABILITIES OF KEY MANAGEMENT SYSTEMS IN DISTRIBUTED LEDGER USING THE EXAMPLE OF THE IBM BLOCKCHAIN

Plotkin A.S.[5], Kesel S.A.[6], Repin M.M.[7], Fedorov N.V.[8]

Abstract.

Today, one of the most discussed topics in the field of information technology is distributed registry systems. They attract investors and developers with their functionality. Distributed ledger systems are being introduced into business processes in many areas of human activity, which makes their contribution to development irreplaceable. One of the most vulnerable parts of such systems is the process of managing cryptographic keys, an attack on which can destroy the entire security of the distributed registry system.

The aim of the research *is to identify possible threats to the process of managing cryptographic keys, on the basis of which recommendations and standards for managing cryptographic keys in distributed ledger systems will be developed.*

Research methods: *to achieve this goal, the structure of the life cycle of cryptographic keys was considered, an analysis of possible vulnerabilities in the process of managing cryptographic keys at each stage of the life cycle of a cryptographic key was carried out. In addition, the distributed ledger system was analyzed in the context of the identified vulnerabilities of the key management process using the example of the IBM blockchain and the possibility of outsourcing cryptographic key management systems was considered.*

Result: *a set of possible threats to the process of managing cryptographic keys was proposed, the necessity of assessing the security of the key management system before deciding on the introduction of these systems into distributed registries was proposed, conclusions were drawn about the need to develop recommendations and standards for the process of managing cryptographic keys for such systems, as well as the possibility applicability of the recommendations for assessing the security of the implementation of outsourcing of cryptographic key management systems in distributed ledgers.*

Keywords: *information technology, information security threats, information security, life cycle of cryptographic keys, outsourcing of cryptographic keys, compensating measures, protection of cryptographic keys.*

References

1. O. Pal, B. Alam, V. Thakur, S. Singh, Key management for blockchain technology. ICT Express (2019). DOI: 10.1016/j.icte.2019.08.002
2. KHramova N.A. Issledovanie kriptosistemy` RSA dlia shifrovaniia informatcii // Sovremenny`e naukoemkie tekhnologii. 2020. №9. S. 88-93.
3. Lenz, Rainer. Managing Distributed Ledgers: Blockchain and Beyond (March 26, 2019). SSRN Electronic Journal. DOI: 10.2139/ssrn.3360655.
4. W. Licheng, S. Xiaoying, L. Jing, S. Jun, Y. Yixian Cryptographic primitives in blockchains // Journal of Network and Computer Applications. 2019. №127. S. 43-58.
5. M. Mingxin, Y. Xiaotong, S. Guozhen, L. Fenghua Enhanced blockchain based key management scheme against key exposure attack // AIIPCC '19: Proceedings of the International Conference on Artificial Intelligence, Information Processing and Cloud Computing. 2019. S. 1-6.
6. Krivonogov A.A., Repin M.M., Fedorov N.V. Metodika analiza uiazvimostei` i opredeleniia urovnia bezopasnosti smart-kontraktov pri razmeshchenii v sistemakh raspredelenny`kh reestrov // Voprosy` kiberbezopasnosti. 2020. №4 (38). S. 56-65.
7. 10.21681/2311-3456-2020-04-56-65
8. Victor Ribeiro, Raimir Holanda, Alex Ramos, Joel J. P. C. Rodrigues Enhancing Key Management in LoRaWAN with Permissioned Blockchain // Sensors. 2020. S. 1-16. DOI: 10.3390/s20113068

5 Alexander Plotkin, postgraduate student of the Department of Information Security, Moscow Polytechnic University, Moscow, Russia. E-mail: sances.98@mail.ru.

6 Sergey Kesel, Ph.D.(Engineering), Associate Professor Department of Information Security, Moscow Polytechnic University, Moscow, Russia. E-mail: sakesel161@gmail.com.

7 Maxim Repin, Head of the direction of the Research Institute «Voskhod», Moscow, Russia. E-mail: bmstu.iu8@gmail.com.

8 Nikolay Fedorov, Ph.D.(Engineering), Associate Professor, Head of the Department of Information Security, Moscow Polytechnic University, Moscow, Russia. E-mail: fedorovnv31@mail.ru.

9. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah and Z. Sun, “Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems,” in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1832-1843, Dec. 2017, DOI: 10.1109/JIOT.2017.2740569.
10. W. F. Ehrsam, S. M. Matyas, C. H. Meyer and W. L. Tuchman, “A cryptographic key management scheme for implementing the Data Encryption Standard,” in IBM Systems Journal, vol. 17, no. 2, pp. 106-125, 1978, DOI: 10.1147/sj.172.0106.
11. Kuz`menko V.V., Makarov V.L., Razguliaev K.A., Han D.V., Shcherbakov A.Iu. Novy`i` podhod k obespecheniiu bezopasnosti perimetra biznes-protcessov i autentifikatcii pol`zovatelei` v korporativnoi` sisteme // Vestneyk sovremenny`kh tcifrovy`kh tekhnologii`. 2020. №3. S. 10-13.
12. Sathya Priya S, Revathy S, Kamnag R, Yogeswar L, Sajal M, Suparna S Distributed Key Management for IT Infrastructure using Block Chain and Hash Graph // International Journal of Recent Technology and Engineering (IJRTE). 2019. S. 533-537.
13. Razguliaev K.A., Riazanova A.A., Han D.V., Shcherbakov A.Iu. Ob odnom sposobe khraneniia i upravleniia cliuchami v sistemakh kvantovy`kh kommunikatcii` // Vestneyk sovremenny`kh tcifrovy`kh tekhnologii`. 2020. №2. S. 14-20.
14. Rui Zhang, Rui Xue, Ling Liu Security and Privacy on Blockchain // ACM Computing Surveys. 2019. S. 1-35.
15. Pankov K. N. Ispol`zovanie kriptograficheskikh sredstv dlia skvozny`kh tcifrovy`kh tekhnologii` na primere sistem raspredelennogo reestra // Tekhnologii informatcionnogo obshchestva. Materialy` XII Mezhdunarodnoi` otraslevoi` nauchno-tekhnicheskoi` konferentcii. 2018. S. 365-366.
16. Pankova V.V., Mironenko A.D. Cryptographic key management systems // Informatcionno-kommunikativnaia kul`tura: Nauka i Obrazovanie Sbornik statei` Mezhdunarodnoi` nauchno-prakticheskoi` konferentcii studentov, aspirantov i molody`kh ucheny`kh. Ministerstvo obrazovaniia i nauki Rossii`skoi` Federatcii, Donskoi` gosudarstvenny`i` tekhnicheskii` universitet. 2018. S. 191-193.