УДК 004.056.5

КРИТЕРИИ ОЦЕНКИ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФРАСТРУКТУРЫ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ ОТ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ В СИСТЕМАХ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ

А.С. Плоткин
Московский Политехнический университет
Россия, 107023, Москва, Большая Семеновская ул., 38
E-mail: sances.98@mail.ru

К.В. Стародубов
РТУ МИРЭА
Россия, 119454, Москва, проспект Вернадского, 78
E-mail: skw@ya.ru

Shamsuldaeen Haidar Abdulwahhab H.
ТГТУ
392000, Тамбов, ул.Советская, 106
E-mail: shamsuldaeenhaidar@mail.ru

Abd Ali Husseinn Najm Abd Ali
ТГТУ
392000, Тамбов, ул.Советская, 106
E-mail: shamsuldaeenhaidar@mail.ru

Ключевые слова: оценка соответствия защиты инфраструктуры ключей, ГОСТ Р 57580.2, защита криптографических ключей от деструктивных воздействий, интеллектуальный анализ данных, информационные технологии, безопасность в финансовой сфере.

Аннотация: с учетом изменений, происходящих в мире, мгновенно возросло количество кибератак, что потребовало внедрение новых механизмов защиты, а также новых информационных технологий, взамен тех, что подверглись секционному давлению. Одной из ключевых внедряемых технологий в современных ИТ-компаниях, организациях финансовой сферы, ведомственных учреждениях и многих других организациях, являются системы, построенные с применением технологии распределенных реестров. При этом активное развитие и внедрение указанной технологии создает новые нерешенные задачи. Одной из таких задач является оценка защищенности инфраструктуры ключей от деструктивных воздействий в таких системах**.**

1. Введение

С учетом изменений, происходящих в мире, мгновенно возросло количество кибератак, что потребовало внедрение новых механизмов защиты, а также новых

информационных технологий, взамен тех, что подверглись секционному давлению. Одной из ключевых внедряемых технологий в современных ИТ-компаниях, организациях финансовой сферы, ведомственных учреждениях и многих других организациях, являются системы, построенные с применением технологии распределенных реестров.

В настоящее время в научных трудах различных авторов рассмотрены меры защиты от деструктивных воздействий для систем распределенных реестров, которые используют различные инструменты и средства, но в которых оценка защищённости инфраструктуры ключей в системах либо не проводится, либо получена субъективно.

Именно поэтому оценка защищённости инфраструктуры ключей в системах распределенных реестрах должна проводиться по стандартизированной методике. Это позволит объективно оценивать защищённость различных систем распределенных реестров и выявлять наиболее уязвимые из подобных систем для дальнейшей доработки.

Одновременно с этим, в рамках статьи «Анализ уязвимостей систем управления ключами в распределенных реестрах на примере блокчейн IBM» уже был сделан вывод относительно необходимости разработки подобной методики [1].

В свою очередь для разработки такой методики необходимо сформулировать критерии оценки эффективности защиты инфраструктуры криптографических ключей от деструктивных воздействий в системах распределённых реестров.

В рамках текущего исследования предложен вариант решения описанной задачи при помощи адаптации критериев из методики оценки соответствия защиты информации ГОСТ Р 57580.2 [2], применяемой в финансовой сфере и предназначенной для оценки выбора и реализации организационных и технических мер защиты информации в соответствии с требованиями ГОСТ Р 57580.1[3] применительно к обеспечению защиты инфраструктуры ключей в системах распределенных реестров.

2. Адаптация критерии оценки эффективности защищенности от деструктивных воздействий

Жизненный цикл инфраструктуры криптографических ключей

Для адаптации критериев из методики оценки соответствия защиты информации ГОСТ Р 57580.2 необходимо рассматривать весь жизненный цикл инфраструктуры криптографических ключей.

Жизненный цикл инфраструктуры криптографических ключей – это набор состояний, в которых пребывают ключи за время своего существования в автоматизированной системе.

Для любого объекта стандартизации определяются четыре стадии жизненного цикла.

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

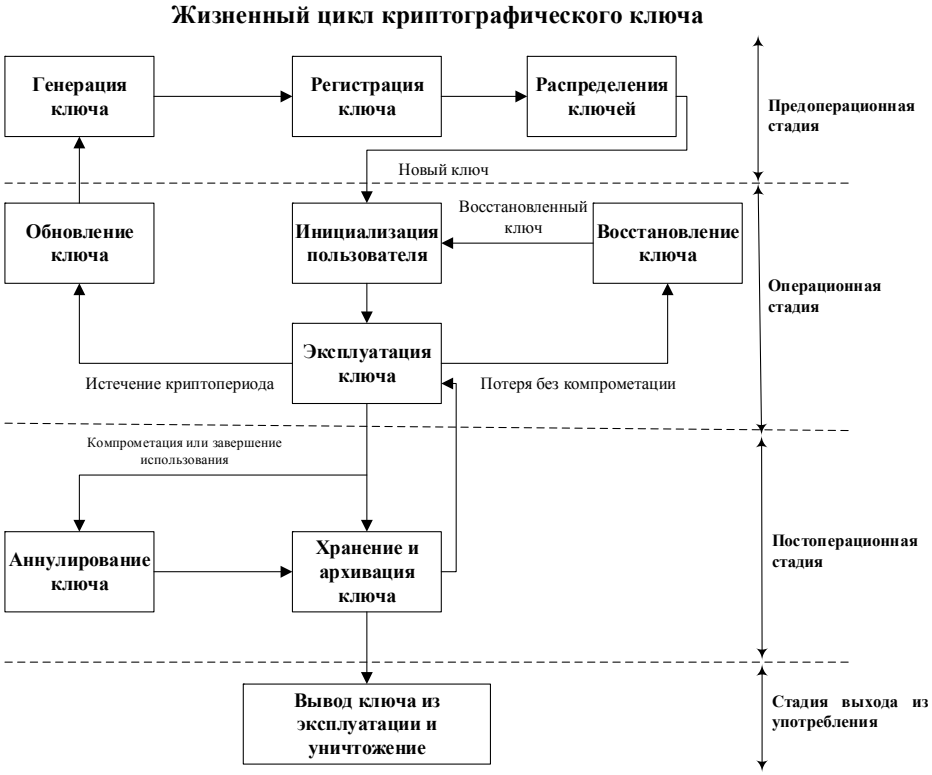

Рис. 1. Жизненный цикл инфраструктуры криптографических ключей.

Для полноценной защиты инфраструктуры ключей необходимо учитывать все вышеописанные этапы жизненного цикла криптографических ключей. В связи с этим одной из важных составляющих оценки при адаптации подхода будет жизненный цикл инфраструктуры ключей.

3. Адаптация критериев ГОСТ Р 57580.2 применительно к системам распределенных реестров

Прежде чем приступать к поставленной задаче, необходимо определить, что под определением деструктивного воздействия, опираясь на устоявшееся определение [4], будем понимать фактор, угрозу, ошибку, предмет или способ реализации того, что ведет к неблагоприятным и разрушительным последствиям для инфраструктуры криптографических ключей в системах распределенных реестров, а под защитой инфраструктуры криптографических ключей будем иметь ввиду меры защиты от таких деструктивных воздействий.

При адаптации критериев из методики оценки соответствия защиты информации ГОСТ Р 57580.2 были сформулированы следующие векторы оценивания:

- (1) выбор организационных и технических мер защиты инфраструктуры криптографических ключей;
- (2) полнота реализации организационных и технических мер защиты инфраструктуры криптографических ключей;
- (3) обеспечение защиты инфраструктуры криптографических ключей на этапах жизненного цикла ключа.

Для адаптации критериев определим ключевые процессы защиты инфраструктуры криптографических ключей в системах распределенных реестров для каждого из которых в соответствии с вектором (1) оценка будет осуществляться отдельно:

- **криптографический алгоритм** (по которому генерируется ключи);
- **протокол конфиденциального вычисления** (с помощью которого узлы вычисляют ключ вместе, сохраняя свою конфиденциальность);
- **протокол консенсуса** (с помощью которого узлы договариваются о легитимности криптографического ключа и запись о нём вносится в распределенный реестр).
- **протокол проверки подлинности** (например, протокол нулевого разглашения секрета с помощью которого возможно провести аутентификацию узла без разглашения секретной информации);

Для оценки полноты реализации процессов системы защиты инфраструктуры криптографических ключей будем использовать следующую качественную модель оценивания:

а) **нулевой уровень соответствия**: организационные и технические меры процесса защиты инфраструктуры криптографических ключей не реализуются или реализуются в единичных случаях. Общие подходы (способы) реализации организационных и технических мер процесса защиты инфраструктуры криптографических ключей не установлены. Контроль и совершенствование реализации организационных и технических мер процесса защиты инфраструктуры криптографических ключей не осуществляются;

б) **первый уровень соответствия**: организационные и технические меры процесса защиты инфраструктуры ключей реализуются в незначительном количестве, бессистемно и/или эпизодически. Общие подходы (способы) реализации организационных и технических мер процесса защиты инфраструктуры криптографических ключей не установлены. Контроль и совершенствование реализации организационных и технических мер процесса защиты инфраструктуры криптографических ключей не осуществляются;

в) **второй уровень соответствия**: организационные и технические меры процесса защиты инфраструктуры ключей реализуются в значительном количестве на постоянной основе. Общие подходы (способы) реализации организационных и технических мер процесса защиты инфраструктуры криптографических ключей установлены в единичных случаях. Реализация организационных и технических мер процесса защиты инфраструктуры ключей осуществляется выборочно. Контроль и совершенствование реализации организационных и технических мер процесса защиты инфраструктуры криптографических ключей практически не осуществляются;

г) **третий уровень соответствия**: организационные и технические меры процесса защиты инфраструктуры криптографических ключей реализуются в значительном количестве на постоянной основе в соответствии с общими подходами (способами), установленными в системе. Контроль и совершенствование реализации организационных и технических мер процесса защиты инфраструктуры криптографических ключей осуществляются бессистемно и/или эпизодически;

д) **четвертый уровень соответствия**: организационные и технические меры процесса защиты инфраструктуры криптографических ключей реализуются в полном объеме на постоянной основе в соответствии с общими подходами (способами), установленными в системе. В системе в основном реализованы контроль и совершенствование реализации организационных и технических мер процесса защиты инфраструктуры криптографических ключей;

Оценку соответствия защиты инфраструктуры криптографических ключей следует основывать на свидетельствах, в качестве основных источников которых рекомендуется использовать:

- документацию по проверяемой системе распределенных реестров и иные материалы в бумажном или электронном виде и, при необходимости, документы третьих лиц, относящиеся к обеспечению защиты инфраструктуры криптографических ключей системы распределенных реестров;
- устные высказывания эксплуатационного персонала проверяемой системы распределенных реестров в процессе проводимых опросов в области оценки соответствия защиты инфраструктуры криптографических ключей;
- результаты наблюдений членов проверяющей группы за процессами системы защиты инфраструктуры криптографических ключей и деятельностью сотрудников в области оценки соответствия защиты инфраструктуры ключей;
- параметры конфигураций и настроек системы и средств защиты инфраструктуры криптографических ключей;
- технические и программные средства сбора свидетельств полноты реализации мер защиты инфраструктуры криптографических ключей (анализ электронных журналов регистрации, анализ фактических настроек, анализ уязвимостей, проведение тестирования на проникновение и т.п.).

На этом формулирование критериев оценки эффективности защиты инфраструктуры криптографических ключей от деструктивных воздействий в системах распределённых реестров завершено и можно приступать к разработке методику и описанию расчет указанных критериев.

4. Заключение

Для достижения поставленной цели исследования была рассмотрена методика оценки соответствия защиты информации ГОСТ Р 57580.2, проведена адаптация её критериев оценки применительно к системам, построенным на основе распределенных реестров с учетом их особенностей.

Указанные критерии позволяют разработать соответствующую методику оценки эффективности защиты инфраструктуры криптографических ключей от деструктивных воздействий в системах распределенных реестров.

Список литературы

1. Плоткин А.С., Кесель С.А., Репин М.М., Федоров Н.В. Анализ уязвимостей систем управления ключами в распределенных реестрах на примере блокчейн IBM // Вопросы кибербезопасности. 2021. № 1 (41). С. 58-68.
2. Национальный стандарт Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия». https://docs.cntd.ru/document/1200158801 (дата обращения: 10.01.2024).
3. Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. защита информации финансовых организаций. Базовая структура организационно-технических мероприятий». https://docs.cntd.ru/document/1200146534 (дата обращения: 10.01.2024).
4. Деструктивное воздействие // Википедия: свобод. энцикл. https://ru.wikipedia.org/wiki/Деструктивное_воздействие (дата обращения: 10.01.2024).