DOI: 10.58168/CISMP2024_217-221
УДК 681.5

ПРИМЕНЕНИЕ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ ИНФРАСТРУКТУРЫ КЛЮЧЕЙ В СИСТЕМАХ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ К НЕКОТОРЫМ ДЕСТРУКТИВНЫМ ВОЗДЕЙСТВИЯМ

А.С. Плоткин[1], Е.Д. Кузнецов[1], К.В. Стародубов[2], Ю.Ю. Громов[3]

[1]ФГАОУ ВО «Московский политехнический университет»
[2] ФГБОУ ВО «МИРЭА - Российский технологический университет»
[3]ФГБОУ ВО «Тамбовский государственный технический университет»

Аннотация. В статье рассматривается решение проблемы обеспечения устойчивости инфраструктуры ключей в системах распределенных реестров к некоторым деструктивным воздействиям с помощью многофакторной аутентификации. Представлены потенциально возможных деструктивные воздействия, зависящие от недостатков в системах аутентификации, в частности на узлах сети. Проведен анализ возможных методов обеспечения устойчивости от таких деструктивных воздействий.

Ключевые слова: технология распределённых реестров, инфраструктура ключей, многофакторная аутентификация, устойчивость к деструктивным воздействиям.

APPLICATION OF MULTI-FACTOR AUTHENTICATION TO ENSURE KEY INFRASTRUCTURE RESILIENCE IN DISTRIBUTED LEDGER TECHNOLOGY SYSTEMS TO SOME DESTRUCTIVE INFLUENCES

A.S. Plotkin[1], E.D. Kuznetsov[1], K.V. Starodubov[2], Yu.Yu. Gromov[3]

[1]Moscow Polytechnic University
[2]MIREA - Russian Technological University
[3]Tambov State Technical University

Abstract. The paper considers the solution of the problem of ensuring the resistance of key infrastructure in distributed registry systems to some destructive influences with the help of multi-factor authentication. Potentially possible destructive influences depending on defects in authentication systems, in particular on network nodes, are presented. Possible methods of providing resistance against such destructive influences are analyzed.

Keywords: distributed ledger technology, key infrastructure, multi-factor authentication, resistance to destructive influences.

Системы с применением технологии распределённых реестров (ТРР), как и любые информационные системы, подвержены множеству информационных рисков и деструктивных воздействий (ДВ). Учитывая растущий интерес к данной технологии, а также постоянное совершенствование методов атак и

повышение квалификации злоумышленников, риск реализации ДВ на такие системы остаётся высоким.

Одним из ключевых классов ДВ на децентрализованные системы, несмотря на их преимущества в виде повышенной прозрачности и устранения единой точки отказа, является слабая защита инфраструктуры ключей, особенно при использовании однофакторной аутентификации пользователей, отличающейся удобством, но простотой поиска паролей [1], в результате которой у злоумышленников появляется возможность компрометации конфиденциальной информации через взлом одного из узлов системы [2].

В этом контексте особую значимость приобретает обеспечение безопасности доступа к управлению инфраструктуры ключей (ИК) на каждом из узлов сети [3]. В таких условиях важнейшую роль играют методы многофакторной аутентификации (МФА), способные существенно повысить уровень устойчивости к ДВ, направленным на получение доступа к ИК. Эти методы обеспечивают создание нескольких независимых каналов аутентификации, что затрудняет злоумышленникам компрометацию системы [4]. В общем плане МФА можно рассматривать как связь репрезентативных данных, представленных паролем и логином пользователя с фактором личного владения, к примеру, токена или карты доступа. [5]

Для эффективного внедрения методов МФА на узлах систем ТРР из общей классификации потенциально возможных ДВ в табл. 1 представлены ДВ, для которых возможно обеспечить устойчивость таким способом [6].

Таблица 1 – Фрагмент классификации потенциально возможных ДВ на ИК в ТРР, связанных с аутентификацией

Деструктивное воздействие	**Описание**	**Применение МФА**
Атаки на узлы сети	Взлом одного из узлов может скомпрометировать ключевую инфраструктуру	Создание независимых каналов аутентификации снижает вероятность компрометации
Атаки на консенсусные механизмы	Манипуляция процессом принятия решений в децентрализованной сети	Усиленная аутентификация участников процессов консенсуса
Компрометация на стадии генерации ключей	Использование недостаточно случайных генераторов ключей	Применение МФА для доступа к подсистеме генерации ключей
Атаки на стадии распределения и эксплуатации ключей	Перехват или подмена ключей при их передаче между узлами	МФА для подтверждения передачи ключей через несколько каналов
Физический доступ к узлам сети	Злоумышленник получает физический доступ к узлу и компрометирует ключи	Физические методы аутентификации в рамках МФА

В качестве основного метода решения задачи обеспечения безопасности доступа к управлению ИК на каждом из узлов сети целесообразно рассмотреть

методы многофакторной аутентификации по трём основным компонентам: безопасность, удобство использования и развёртываемость, опираясь на сравнительный фреймворк «UDS» [7].

Удобство использования (U) отражает степень простоты и интуитивности для пользователя при прохождении процесса аутентификации. Важно минимизировать количество шагов для пользователя, обеспечить лёгкость восстановления доступа и снизить вероятность ошибок. В контексте ТРР, где каждый участник управляет своими ключами, методы аутентификации должны быть удобными, чтобы не перегружать пользователей сложными операциями.

Развёртываемость (D) оценивает лёгкость и стоимость внедрения метода аутентификации, его совместимость с различными платформами, а также масштабируемость. В распределённых системах, таких как ТРР, где число узлов и участников может быстро увеличиваться, развёртываемость играет критическую роль. Эффективные методы должны быть легко интегрируемыми и масштабируемыми, особенно в условиях децентрализации.

Безопасность (S) ключевой критерий, определяющий защиту от атак и несанкционированного доступа. Методы аутентификации должны быть устойчивы к угрозам, таким как атаки на пароли, фишинг, перехват данных, а также физический доступ. В ТРР защита ключей, хранящихся на каждом узле, напрямую зависит от выбранного метода аутентификации.

Результаты проведенного исследования методов МФА применительно к рассматриваемым ДВ в системах ТРР приведены в табл. 2.

Таблица 2 – Оценка методов МФА на основе Фреймворка UDS

Метод МФА	**Удобство (U)**	**Развёртываемость (D)**	**Безопасность (S)**
Биометрическая аутентификация	Средняя	Высокая	Высокая
Поведенческая аутентификация	Высокая	Средняя	Высокая
SMS-аутентификация	Высокая	Высокая	Низкая
Аутентификация по устройству	Средняя	Высокая	Средняя

Выводы

На основании проведенного исследования определены деструктивные воздействия на ИК, в отношении которых может быть обеспечена устойчивость ИК с использованием методов МФА, проведена оценка методов МФА с использованием фреймворка UDS, наиболее подходящих для их использования при обеспечении безопасности доступа к управлению ИК в системах ТРР. Указанные результаты будут учитываться в качестве критериев устойчивости при формировании модели оценки устойчивости ИК в системах ТРР.

Список литературы

1. Новиков А. Л. Организация многофакторной аутентификации пользователей в корпоративной сети // Международный научный журнал

“ВЕСТНИК НАУКИ” №6 (63). URL: https://cyberleninka.ru/article/n/organizatsiya-mnogofaktornoy-autentifikatsii-polzovateley-v-korporativnoy-seti/ (дата обращения: 09.09.2024)

2. Шишкин С. Р., Ратушняя Е. С., Басыров И. И., Богач Е. В., Устинова Е. В. Оценка проблем и поиск путей решения при использовании технологии блокчейн в авторизации пользователей // Инновации и инвестиции. 2023. №3. URL: https://cyberleninka.ru/article/n/otsenka-problem-i-poisk-putey-resheniya-pri-ispolzovanii-tehnologii-blokcheyn-v-avtorizatsii-polzovateley (дата обращения: 09.09.2024).

3. 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.

4. Файзулин Р.Ф., Демичев М.С., Маркевич И.В., Оголь А.Р., Бондарев А.С. Двухфакторная аутентификация – современные реалии // Актуальные проблемы авиации и космонавтики. 2022. URL: https://cyberleninka.ru/article/n/dvuhfaktornaya-autentifikatsiya-sovremennye-realii (дата обращения: 09.09.2024).

5. Голуб В. А. Системы контроля доступа: Учебно-методическое пособие к курсу “Методы и средства защиты информации”. – Воронеж: Изд-во ВГУ, 2004. – 15 с.

6. 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.

7. Bonneau, J., Herley, C., Oorschot, P. C. van, & Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. 2012 IEEE Symposium on Security and Privacy.

References

1. Novikov A. L. Organization of multi-factor authentication of users in a corporate network // International scientific journal “VESTNIK NAUKI” No. 6 (63). URL: https://cyberleninka.ru/article/n/organizatsiya-mnogofaktornoy-autentifikatsii-polzovateley-v-korporativnoy-seti/ (date of reference: 09/09/2024).

2. Shishkin Sergey Ruslanovich, Ratushnyaya Ekaterina Sergeevna, Basyrov Ildar Ilshatovich, Bogach Egor Vladimirovich, Ustinova Evgeniya Vadimovna Assessment of problems and search for solutions when using blockchain technology in user authorization // Innovations and Investments. 2023. No. 3. URL: https://cyberleninka.ru/article/n/otsenka-problem-i-poisk-putey-resheniya-pri-ispolzovanii-tehnologii-blokcheyn-v-avtorizatsii-polzovateley (date of reference: 09/09/2024).

3. Pankov K. N. The use of cryptographic tools for end-to-end digital technologies on the example of distributed registry systems // Technologies of the

Information Society. Materials of the XII International Industrial Scientific and Technical Conference. 2018. pp. 365-366.

4. Fayzulin R.F., Demichev M.S., Markevich I.V., Ogol A.R., Bondarev A.S. Two-factor authentication – modern realities // Actual problems of aviation and cosmonautics. 2022. URL: https://cyberleninka.ru/article/n/dvuhfaktornaya-autentifikatsiya-sovremennye-realii (date of reference: 09/09/2024).

5. Golub V. A. Access control systems: A teaching aid for the course "Methods and means of information security". – Voronezh: VSU Publishing, 2004. – 15 p.

6. Plotkin A.S., Kesel S.A., Repin M.M., Fedorov N.V. Vulnerability analysis of key management systems in distributed registries on the example of IBM blockchain // Voprosy cybersecurity. - 2021. - №1(41). - C. 58-68.

7. Bonneau, J., Herley, C., Oorschot, P. C. van, & Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. 2012 IEEE Symposium on Security and Privacy.