УДК 004

Клыгин В.О.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Салов И.В.
Уфимский университет науки и технологий, Уфа

ДЕЦЕНТРАЛИЗОВАННЫЕ ИДЕНТИФИКАТОРЫ (DIDs) КАК ОСНОВА БЕСПАРОЛЬНОЙ АУТЕНТИФИКАЦИИ И УСТРАНЕНИЕ РИСКОВ ЦЕНТРАЛИЗОВАННОГО ХРАНЕНИЯ ДАННЫХ

Аннотация. В статье рассматриваются децентрализованные идентификаторы (DIDs) как метод беспарольной аутентификации, обеспечивающий безопасный вход и суверенное управление данными без рисков централизованного хранения.

Ключевые слова: аутентификация, идентификаторы, блокчейн, децентрализация, пароль.

Во время различных войн противники активно боролись со шпионами, используя кодовые слова или пароли, служившие способом отличить своих от врагов. Принцип «если я знаю секрет, значит, я тот, за кого себя выдаю» лег в основу современных систем аутентификации. Сегодня пароль остается ключевым элементом для подтверждения личности и защиты цифровых данных.

Но их использование сопровождается рядом проблем, главная из которых – баланс между удобством и безопасностью. Согласно исследованию DLBI, российской службы анализа утечек данных, в 2024 г. среди самых популярных паролей в российских доменных зонах оказались «123456», «1221123456», «12345», «йцукен» и «пароль». Такие простые и легко запоминаемые пароли уязвимы к атаке полным перебором (Brute Force), которая позволяет подобрать их за считанные минуты, особенно если злоумышленники используют словари распространенных паролей или радужные таблицы.

В отличие от простых паролей, сложные, состоящие из случайных символов, значительно увеличивают время, необходимое для их взлома. Однако высокая сложность создает другую проблему: такие пароли трудно запомнить. Это вынуждает пользователей прибегать к помощи менеджеров паролей – централизованных хранилищ, которые, в свою очередь, становятся основной целью злоумышленников. В случае их взлома злоумышленник может получить доступ ко всем паролям пользователя, а сам пользователь рискует потерять доступ к своим данным на различных ресурсах.

Для улучшения методов аутентификации были внедрены электронные инструменты, такие как двухфакторная аутентификация (2FA), которая добавляет дополнительный уровень защиты поверх традиционных паролей. Для обхода этого метода начались атаки с применением социальной инженерии, которая по данным экспертов Positive Technologies, в третьем квартале 2024 г. являлась наиболее популярным методом атаки как на организации (50 %), так и на частных лиц (92 %). Также значительно возросло количество фишинговых атак – в России их число в 2024 г. превысило 350 тысяч.

Из-за необходимости постоянной регистрации и ввода длинных паролей началось активное внедрение методов аутентификации, которые не требуют использования паролей. Одним из наиболее известных решений стала биометрическая аутентификация. Несмотря на свою инновационность, она также оказалась уязвимой для атак. На ранних этапах разработки биометрических систем аутентификацию по лицу можно было обойти с помощью качественных фотографий, 3D-масок или заранее записанных видео. В ответ на эти угрозы были разработаны алгоритмы определения живости (liveness detection), способные выявлять поддельные данные. Однако и эти меры не стали панацеей: с появлением генеративно-состязательных сетей (GAN) злоумышленники получили возможность создавать искусственные биометрические данные (deepfake), которые успешно проходят проверки на живость, создавая новые вызовы для биометрических систем.

Кроме того, как и обычные пароли, биометрические данные часто хранятся в централизованных хранилищах, что делает их приоритетной целью для атакующих. Но главным отличием от паролей, которые можно изменить в случае компрометации, биометрические данные остаются неизменными, что делает их утечку особенно критичной. Самым громким инцидентом стала утечка данных на платформе BioStar 2, разработанной компанией Suprema. В 2019 г. в открытый доступ попали более 27,8 млн записей (23 ГБ данных), затронув более 1 миллиона человек.

Осознавая эти проблемы, специалисты по безопасности еще в 1990-х гг. начали обсуждать новые методы аутентификации, включая принципы децентрализованных данных и контроля над личной информацией. Их цель заключалась в том, чтобы отказаться от необходимости использования длинных и уникальных паролей для разных сервисов и их хранения в централизованных базах.

Одним из пионеров децентрализованной идентификации стал Кристофер Аллен – архитектор блокчейна и соавтор стандартов IETF TLS и W3C DIDs. Вместе с Тимом Бернерсом-Ли, создателем всемирной паутины, он участвовал в разработке версии 1.0 децентрализованных идентификаторов (DIDs).

Согласно W3C, децентрализованные идентификаторы (DIDs) – это новый тип идентификаторов, которые обеспечивают проверяемую

децентрализованную цифровую идентификацию. DID может быть присвоен любому субъекту: человеку, организации, предмету, модели данных или даже абстрактному объекту. При этом контроль над идентификатором полностью принадлежит его владельцу [1].

Технология DIDs основана на криптографии с использованием приватных и публичных ключей и является одним из трех столпов суверенной идентификации. Ее основные компоненты включают:

Блокчейн – это децентрализованный цифровой реестр, поддерживаемый распределенной сетью компьютеров. Данные хранятся в блоках, связанных в хронологическом порядке, и защищены криптографией [2].

Децентрализованные идентификаторы (DIDs) – это пользовательские идентификаторы, создаваемые и контролируемые самими пользователями без участия централизованных органов.

Проверяемые учетные данные (VC) – это криптографически защищенные цифровые документы, позволяющие подтверждать личность или другие сведения без раскрытия избыточной информации.

Принцип работы технологии заключается в следующем: пользователь подписывает запрос от сервиса своим приватным ключом, а сервис, которому необходимо удостовериться в подлинности, расшифровывает данные с помощью публичного ключа, который хранится децентрализовано.

Технология децентрализованных идентификаторов (DIDs) может усилить безопасность данных, что особенно актуально в условиях роста киберугроз в России. В 2024 г. в сеть попало 710 миллионов записей, включая более 80 млн паролей. Основными целями стали объекты КИИ и базы МФЦ. Основной платформой для хранения персональных данных граждан РФ выступают «Госуслуги», где хранятся данные, позволяющие взаимодействовать с государственными органами и финансовыми организациями, что делает ее привлекательной целью для атак. Одной из главных задач злоумышленников является преодоление этапа аутентификации для доступа к этим данным.

Сегодня для входа в личный кабинет на «Госуслугах» используются логин и пароль с двухфакторной аутентификацией через SMS, сканирование QR-кода только с устройства, на котором уже выполнен вход или электронная подпись, на физическом носителе, как «Рутокен». Помимо проблем, о которых говорилось выше, еще одной проблемой, одинаковой для всех все трех способов, является хранение и обработка необходимых для входа идентификаторов в централизованной системе, что создает высокий риск атак и делает ее уязвимой для краж, уничтожения или изменения данных [3].

С внедрением DIDs можно избавиться от необходимости использовать пароли и дополнительные устройства для входа. Но самое главное – мы откажемся от централизованного хранения данных, перейдя к децентрализованной системе на основе блокчейна, что устранит единую точку отказа и снизит риски потери чувствительной информации.

В качестве эмитента сможет выступать орган исполнительной власти, подтверждающий личность пользователя и выпускающий децентрализованные идентификаторы (DIDs), заверенные государством. Эти идентификаторы будут размещаться в блокчейне вместе с публичными ключами пользователя и эмитента. Узлами блокчейна могут стать министерства, службы и даже частные компании. Для хранения приватного ключа, используемого для подписи запросов, можно задействовать приложение «Госключ», позволяющее пользователю подтверждать личность при аутентификации.

Однако, остаются определенные проблемы. Например, безопасность приложения «Госключ» потребует многофакторной защиты: пароля, биометрии, двухфакторной аутентификации (2FA) или сид-фразы для восстановления доступа. Кроме того, вектор атак сместится на пользователей, увеличивая риски атак с использованием социальной инженерии. Это подчеркивает важность повышения цифровой грамотности пользователей.

Список использованных источников:

1. Decentralized Identifiers (DIDs) v1.1 // W3C. URL: https://www.w3.org/TR/did-1.1/#example-a-simple-did-document.

2. Что такое блокчейн и как он работает? // Binance Academy. URL: https://academy.binance.com/ru/articles/what-is-blockchain-and-how-does-it-work.

3. Кириллов В.С. Проблематика использования электронных подписей / В.С. Кириллов, А.С. Исмагилова, Д.Т. Набиев // Информационные технологии интеллектуальной поддержки принятия решений (памяти проф. Н.И. Юсуповой) ITIDS'2024: труды X Международной научной конференции. В 2 томах. Уфа, 12–14 ноября 2024 г. Уфа: Уфимский университет науки и технологий, 2024. С. 1214.

Klygin V.O.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Salov I.V.
Ufa University of Science and Technology, Ufa

DECENTRALISED IDENTIFICATORS (DIDs) AS A BASIS FOR PASSWORDLESS AUTHENTIFICATION AND REDUCING RISKS OF CENTRALISED DATA STORAGE

Abstract. This paper discusses decentralised identifiers (DIDs) as a passwordless authentication method that provides secure login and sovereign data management without the risks of centralised storage.

Keywords: authentication, identifiers, blockchain, decentralisation, password.