УДК 004.056.53

# ИССЛЕДОВАНИЕ ПОДХОДОВ К РЕАЛИЗАЦИИ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В ДОМЕНЕ FREEIPA НА БАЗЕ ОС ALT

**Солоненко Иван Сергеевич**

*Студент;*
*Российский государственный университет нефти и газа (НИУ) им. И.М. Губкина;*
*119991, г. Москва, проспект Ленинский, дом 65, корпус 1;*
*e-mail: issolonenko@gmail.com.*

*В статье исследуются два подхода к реализации двухфакторной аутентификации пользователей ОС ALT в домене на базе программного обеспечения FreeIPA: с использованием технологии одноразовых паролей и сертификатов цифровой подписи. Исследование направлено на поиск решений, позволяющих обеспечить повышение уровня информационной безопасности информационной инфраструктуры с использованием отечественного и открытого программного обеспечения.*

Ключевые слова: двухфакторная аутентификация, FreeIPA, ОС ALT, домен, LDAP, импортозамещение.

**Для цитирования:**

Солоненко И. С. Исследование подходов к реализации двухфакторной аутентификации пользователей в домене FreeIPA на базе ОС ALT // Системный анализ в науке и образовании: сетевое научное издание. 2025. № 4. С. 1-8. EDN: JOIEYS. URL: https://sanse.ru/index.php/sanse/article/view/675.

# RESEARCH OF APPROACHES TO IMPLEMENTATION OF TWO-FACTOR AUTHENTICATION OF USERS IN THE FREEIPA DOMAIN BASED ON ALT OS

**Solonenko Ivan S.**

*Student;*
*National University of Oil and Gas «Gubkin University»;*
*65 Leninsky Avenye, Moscow, 119991, Russia;*
*e-mail: issolonenko@gmail.com.*

*The article examines two approaches to implementing two-factor authentication of ALT OS users in a domain based on FreeIPA software: using one-time password technology and digital signature certificates. The research is aimed at finding solutions to improve the level of information security of the information infrastructure using domestic and open-source software.*

Keywords: two-factor authentication, FreeIPA, ALT OS, domain, LDAP, import substitution.

**For citation:**

Solonenko I. S. Research of approaches to implementation of two-factor authentication of users in the FreeIPA domain based on ALT OS. *System analysis in science and education*, 2025;(4):1-8(in Russ).EDN: JOIEYS. Available from: https://sanse.ru/index.php/sanse/article/view/675.

## *Введение*

В современной российской информационной инфраструктуре, характеризующейся повышенным ростом числа кибератак, критически важно обеспечивать надежную аутентификацию пользователей и сервисов. Особую значимость вопрос аутентификации приобретает для систем, которые

предоставляют услуги конечному потребителю или обрабатывают данные, компрометация которых ведет к финансовым потерям, репутационным рискам или нарушению законодательства РФ.

Как известно, исторически сложившимся и наиболее известным методом аутентификации является использование пары логин-пароль, что является логичным и интуитивно понятным способом подтвердить, что пользователь является тем, за кого себя выдает. При этом уязвимость метода ввиду склонности людей к созданию «слабых» и легко запоминающихся паролей, их многократного переиспользования на нескольких ресурсах вынуждает компании подстраиваться под современные реалии. Со временем мировой индустрией обеспечения информационной безопасности был выработан подход многофакторной аутентификации, требующий от пользователя двух, а иногда и более доказательств (факторов) своей идентичности в системе, что позволяет допустить компрометацию одного из доказательств (факторов) без риска получения доступа к системе злоумышленником.

Эти факторы можно классифицировать на три основные категории:

1. То, что пользователь знает (пароль).
2. То, чем пользователь владеет (токен, мобильное устройство).
3. Физическое свойство пользователя (лицо, отпечаток пальца).

Так, на российском рынке информационной безопасности представлены отдельные продукты, выполняющие только одну функцию – обеспечение аутентификации пользователей, в том числе многофакторной, примерами чего могут послужить набирающие популярность отечественные вендоры: «*Avanpost*», «Индид», «Мультифактор» и др. Однако применение корпоративных продуктов вышеперечисленных представителей рынка может оказаться финансово нецелесообразным для средних или небольших компаний.

В этой связи особую актуальность приобретает построение систем управления идентификацией и доступом к инфраструктурным сервисам с использованием свободного программного обеспечения (СПО), направленного на реализацию механизмов многофакторной аутентификации. Одним из наиболее зрелых решений типа СПО в данной области является *FreeIPA* – набор программного обеспечения (ПО), включающий в себя службы аутентификации, авторизации и управления учетными записями *UNIX*-подобных систем. FreeIPA объединяет в себя следующие сервисы: система доменных имён (*DNS*), инфраструктура открытых ключей (PKI) на базе СПО *DogTag*, *Kerberos*, служба каталога 389 *Directory Server*. Широкий перечень базовых инфраструктурных сервисов, управляемых централизованно на основе доменных политик, позволяет организовывать легко управляемую и при этом защищенную информационную инфраструктуру, что позволило *FreeIPA* лечь в основу службы каталога и управления доменом *Linux*-систем – «*Astra Linux Directory*» (*ALD Pro*), входящего в реестр сертифицированных средств защиты информации ФСТЭК [1]. Для российских компаний, стремящихся к полному импортозамещению не только средств защиты информации, но и инфраструктурных сервисов, особо актуально использовать СПО в связке с отечественными операционными системами общего назначения на базе ОС Linux, таких как «*Astra Linux*», «РЕД ОС», «ОС *ALT*» и др. Таким образом, возникает комплексная задача исследования подходов к практической реализации двухфакторной аутентификации и ее интеграции в российскую импортозамещенную инфраструктуру.

В рамках работы рассматриваются два метода двухфакторной аутентификации, основанные на категории «то, чем пользователь владеет»: с использованием OTP-токена, с использованием сертификата электронной подписи.

Целью работы является исследование возможностей практического применения методов двухфакторной аутентификации пользователей в домене *FreeIPA* на базе ОС *ALT*: с использованием OTP-кода, с использованием сертификата электронной подписи.

## *1. Особенности ОС ALT в контексте обеспечения централизованной аутентификации*

В ОС *ALT* интеграция с *FreeIPA* обеспечивается через набор специализированных пакетов, адаптированных для работы конкретно с данной операционной системой. Основные пакеты *FreeIPA*

в рамках ОС *ALT*: *freeipa-server*, *freeipa-client* и *freeipa-server-dns*; доступны в репозиториях ОС *ALT* и поддерживаются в актуальных версиях системы.

Особенностью ОС *ALT* является использование схемы *TCB* (*Trusted Computing Base*) для управления паролями пользователей. Отдельный каталог в системе, расположенный по пути /etc/tcb/имя_пользователя содержит файл со сгенерированными хэшами паролей, тем самым обеспечивая изоляцию данных каждого пользователя [2].

Управление правами пользователей в *ATL Linux* обеспечено за счет системной утилиты *control* из состава ОС, с помощью которой настраивается доступ к файлам и каталогам. Так, с ее помощью можно разрешить или запретить использование команд для определенных групп пользователей. Такой функционал в том числе входит в состав *FreeIPA* – ограничение выполнения команд пользователей, что является прямым аналогом групповых политик доступа *Active Directory*, основанных на разграничении ролей администраторов и пользователей. Такой механизм в ОС *ALT* реализуется за счет встроенного инструмента *control*.

## 2. Обзор и архитектура СПО FreeIPA

*FreeIPA* является интегрированной системой управления идентификацией с открытым исходным кодом, разработанная в первую очередь для сред *Linux/UNIX*. Её можно рассматривать как аналог *Active Directory* [3], ориентированный на *Linux*, предоставляющий централизованное решение для аутентификации, авторизации и управления учётными записями.

Основой решения является прикладной протокол *Lightweight Directory Access Protocol* (*LDAP*), представляющий из себя иерархическую базу данных облегченного доступа (см. рисунок 1).

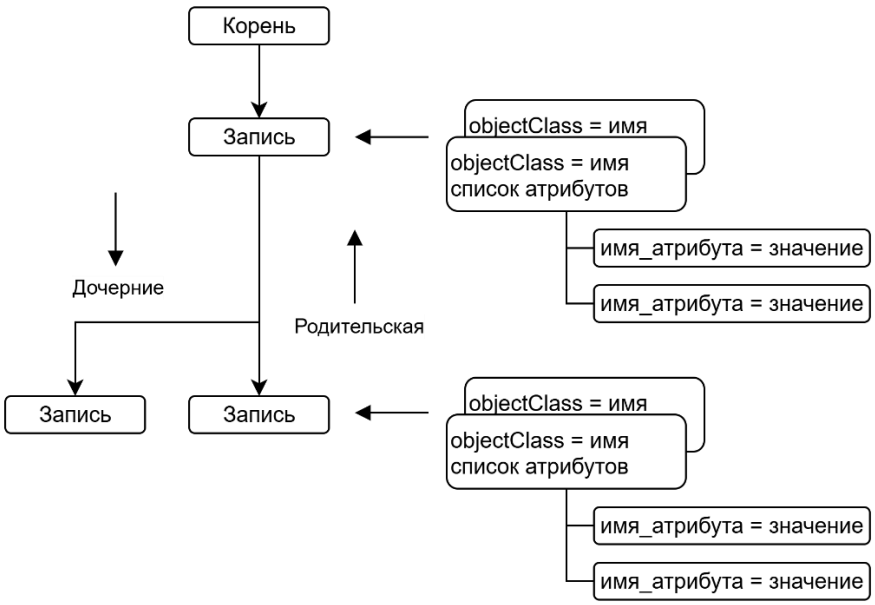


*Рис. 1. Модель данных LDAP*

*LDAP*-каталог организован по древовидной иерархии, называемой *DIT* (*Directory Information Tree*), где каждая запись состоит из одного или нескольких объектных классов, у каждого из которых есть имя. Объектный класс представляет собой контейнер для атрибутов (в его определении идентифицируются атрибуты, которые он может или должен содержать), при этом у каждого атрибута есть имя, и он является членом одного или нескольких объектных классов. При наполнении *DIT* каждая запись уникально идентифицируется в иерархии (относительно своей родительской записи) данными, которые содержатся в этой записи (в атрибутах, которые содержатся в её объектном классе (классах)). Говоря более широко, *LDAP* формирует способ, которым данные внутри службы каталога должны быть представлены пользователям, определяет требования к компонентам, используемым для создания записей данных внутри службы директории, и описывает способ, которым различные примитивные элементы используются для составления записей. Такой подход

позволяет однозначно идентифицировать пользователей в доменной инфраструктуре и определять каким доступом к компонентам системы или сети они должны обладать [4].

Для получения доступа пользователям к сервисам инфраструктуры без повторного ввода пароля используется центр распределения ключей (*KDC*), основанный на протоколе *Kerberos*. *KDC* выдает «билеты», которые используются пользователями для аутентификации вместо пароля и позволяют реализовать технологию единого входа (*SSO*), выходящую за рамки данной статьи [5]. Также подход использования одноразовых паролей (OTP) основан на *Kerberos*, для чего используется отдельный компонент в виде системной службы *ipa-otpd*.

*FreeIPA* позволяет выступать в роли независимого центра сертификации благодаря встроенному СПО *Dogtag Certification Authority* (*Dogtag CA*), обеспечивая полный жизненный цикл сертификатов цифровой подписи, включая их выпуск, отзыв и обновление. Сертификаты цифровой подписи представляют из себя пару закрытого и открытого ключей, сгенерированных на основе криптографического алгоритма, при этом закрытый ключе находится у владельца сертификата, что позволяет ему подтвердить право владения сертификатом. Такой подход позволяет выстроить доверенную сетевую связь между субъектами инфраструктуры [6]. Данная функция находит много применений, но в качестве основных сценариев целесообразно рассматривать выпуск сертификатов для веб-серверов (например, Apache) и для пользователей, которые могут использовать их, например, для аутентификации в корпоративных системах или беспроводных сетях [7].

В процедуре аутентификации важную роль играет системная служба *SSSD*, хотя она и не является компонентом *FreeIPA* напрямую, а входит в состав операционной системы *Linux*. *SSSD* кэширует учетные данные, обрабатывает автономную аутентификацию и взаимодействует с *LDAP* и *Kerberos*. Когда пользователь входит в систему *Linux*, зарегистрированную в *FreeIPA*, *SSSD* использует *Kerberos* (для проверки учетных данных) и *LDAP* (для извлечения информации о пользователе, такой как *UID*/*GID*, группы, домашний каталог, оболочка) с сервера *FreeIPA*.

Преимуществом СПО *FreeIPA* является то, что вышеперечисленные компоненты интегрированы между собой и управляются централизованно. Так, добавление нового пользователя в домен *FreeIPA* повлечет за собой создание записи в *LDAP* и субъекта *Kerberos*, который в дальнейшем используется службой *SSSD* и при использовании одноразовых OTP-паролей.

## *3. Разработка решения для обеспечения централизованной аутентификации пользователей с использованием двухфакторной аутентификации*

В целях исследования применимости подхода к организации двухфакторной аутентификации с использованием СПО *FreeIPA* в инфраструктуре ОС *ALT* реализуется инфраструктура, состоящая из двух виртуальных машин, описание которых представлено в таблице 1.

*Табл. 1. Описание инфраструктуры*

| Hostname | Роль | ОС | IP-адрес | Основные сервисы |
|---|---|---|---|---|
| ipa.isolonenko.com | Контроллер домена | ALT Linux Workstation 10.1 | 10.0.2.15 | Freeipa-server, DNS, NTP<br>Dogtag |
| alt2.isolonenko.com | Клиент домена | ALT Linux Workstation 10.1 | 10.0.2.6 | Freeipa-client, SSSD |

Развертывание и настройка контроллера домена, а также клиента домена производится в соответствие с руководством вендора [8,9]. Также была настроена *DNS*-зона и сетевая связность виртуальных машин [10]. Серверная часть *FreeIPA* доступна из официального репозитория ОС *ALT*, благодаря чему инсталляция производится средствами операционной системы – с помощью менеджера пакета *apt*. Также клиентская часть доступна в репозитории и устанавливается аналогично. После установки компонентов клиентское устройство необходимо ввести в домен, это можно выполнить как из графического интерфейса сервера управления *FreeIPA*, так и с помощью интерфейса командной строки. Для этого необходимо знать учетные данные от администратора домена, инициализирующегося во время инсталляции. С момента ввода устройства в домен *FreeIPA* на него распространяются доменные политики, в том числе политики, регламентирующие доступные методы аутентификации:

1. Пароль.
2. *RADIUS*.
3. Двухфакторная аутентификация (пароль + OTP).
4. *PKINIT*.
5. Пароль с усиленной защитой (*SPAKE* или *FAST*).
6. *External Identity Provider*.

Таким образом, *FreeIPA* позволяет централизованно управлять идентификацией, аутентификацией и авторизацией пользователей доменной сети.

Схема взаимодействия сервисов решения представлена на рисунке 2.

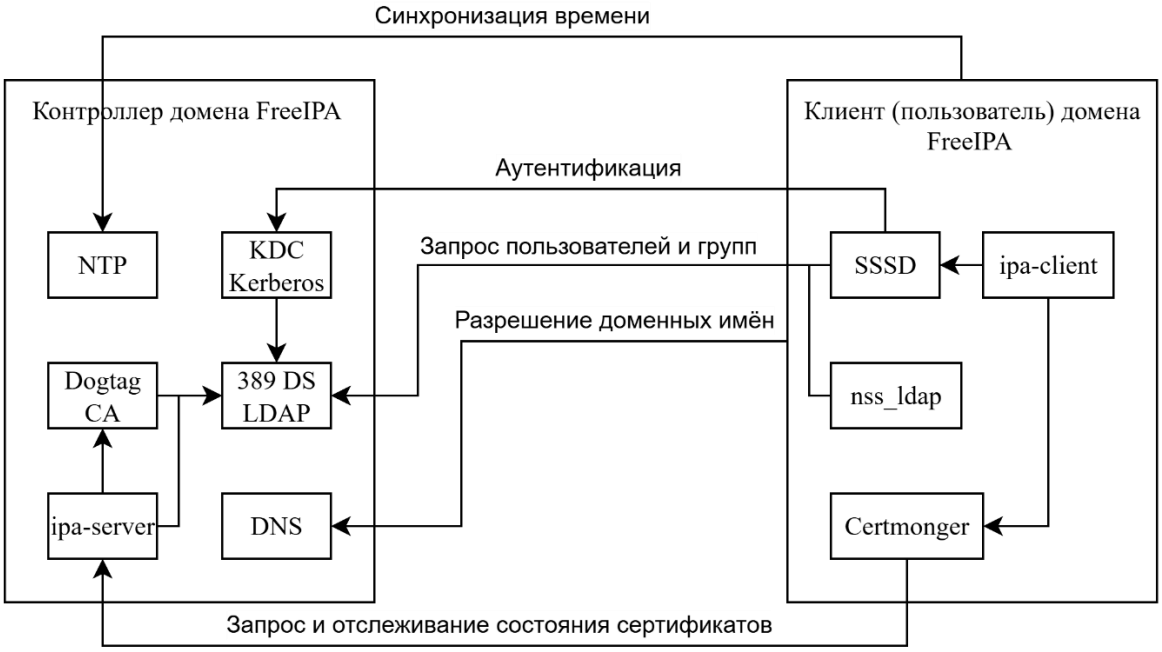


*Рис. 2. Взаимодействие сервисов контроллера домена FreeIPA и клиента в инфраструктуре на базе ОС ALT*

## *4. Реализация двухфакторной аутентификации в ОС ALT в домене FreeIPA типа «пароль + OTP»*

Двухфакторная аутентификация подразумевает использование второго фактора аутентификации. В качестве второго фактора в данном случае выступает OTP-код, который меняется с определенной периодичностью и находится на внешнем устройстве.

OTP – это механизм временных паролей, который обеспечивает дополнительный уровень безопасности при аутентификации. *FreeIPA* поддерживает *TOTP* (*Time-based One-Time Password*) и *HOTP* (*HMAC-based One-Time Password*) согласно стандартам *RFC* 6238 и *RFC* 4226. OTP-код можно выдать как доменному пользователю, так и в качестве временного одноразового кода для ввода нового устройства в домен.

Для настройки OTP-кода необходимо перейти в *Web*-консоли управления *FreeIPA* в раздел управления политиками аутентификации и сгенерировать *QR*-код для доменного пользователя. Для добавления OTP-кода на мобильное устройство можно использовать любое бесплатное приложение, поддерживающее функционал хранения OTP-кодов, в рамках работы используется мобильное приложение *FreeOTP*. При сканировании кода в мобильном приложении *FreeOTP* добавляется новая

вкладка, содержащая уникальный номер OTP-кода. При нажатии на вкладку отображается 6-значный (по умолчанию) код (см. рисунок 3).

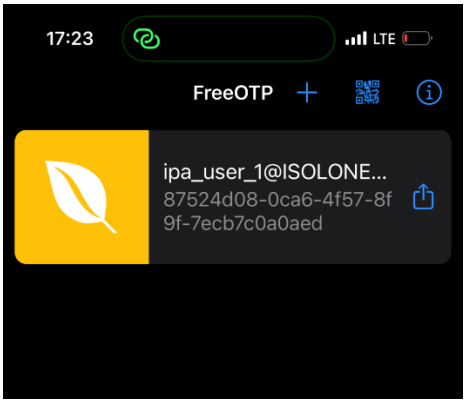


*Рис. 3. OTP-код пользователя ipa_user_1 в мобильном приложении FreeOTP*

На рисунке 4 представлено использование OTP-кода для аутентификации доменного пользователя в ОС.

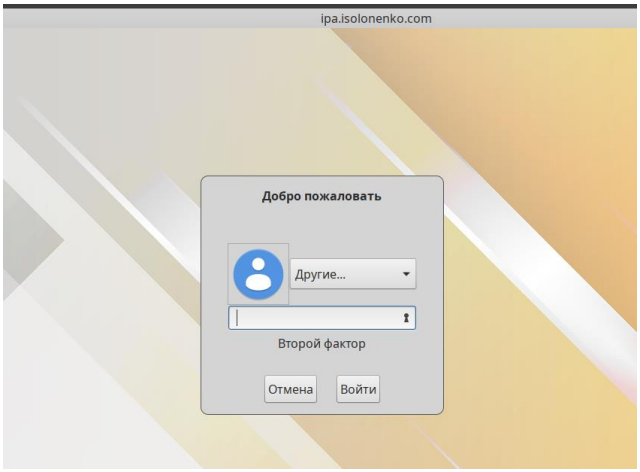


*Рис. 4. Запрос OTP-кода в качестве второго фактора при аутентификации в ОС ALT*

## 5. Реализация двухфакторной аутентификации в ОС ALT в домене FreeIPA с использованием сертификата цифровой подписи

Процедура выпуска сертификата для пользователя начинается с формирования файла запроса с расширением *.csr*. Такой файл можно создать прямо на сервере, предварительно определив, какое поле *CN* (*Common Name*) описано в *LDAP* для целевого пользователя.

Генерация файла запроса может быть выполнена с помощью системной утилиты openssl, входящей в официальный репозиторий ОС *ALT*, что позволяет создать файл запроса и закрытый ключ с использованием необходимого алгоритма шифрования с использованием штатных средств ОС. Также в сертификат добавляется поле *CN*, точно идентифицирующее пользователя в *LDAP*. Таким образом, происходит привязка сертификата к доменному пользователю. При выпуске сертификата на основе файла запроса в Web-интерфейсе *FreeIPA* генерируется открытый ключ, который содержит информацию о пользователе, в данном случае его *CN*.

В рамках работы рассматривается аутентификация с использованием сертификата в *Web*-консоли *FreeIPA*. Для этого формируется файл с расширением *p*12 (далее – контейнер), в котором будет храниться ключевая пара, этот этап необходим для импорта контейнера в *Web*-браузер для использования сертификата. Обязательным условием является назначение пароля на контейнер, который запрашивается при его импорте в браузер.

Теперь, при переходе в *Web*-консоль *FreeIPA* по адресу *https://ipa.isolonenko.com* и нажатии кнопки «войти с помощью сертификата», браузер автоматически предложит выбрать сертификат (см. рисунок 5).

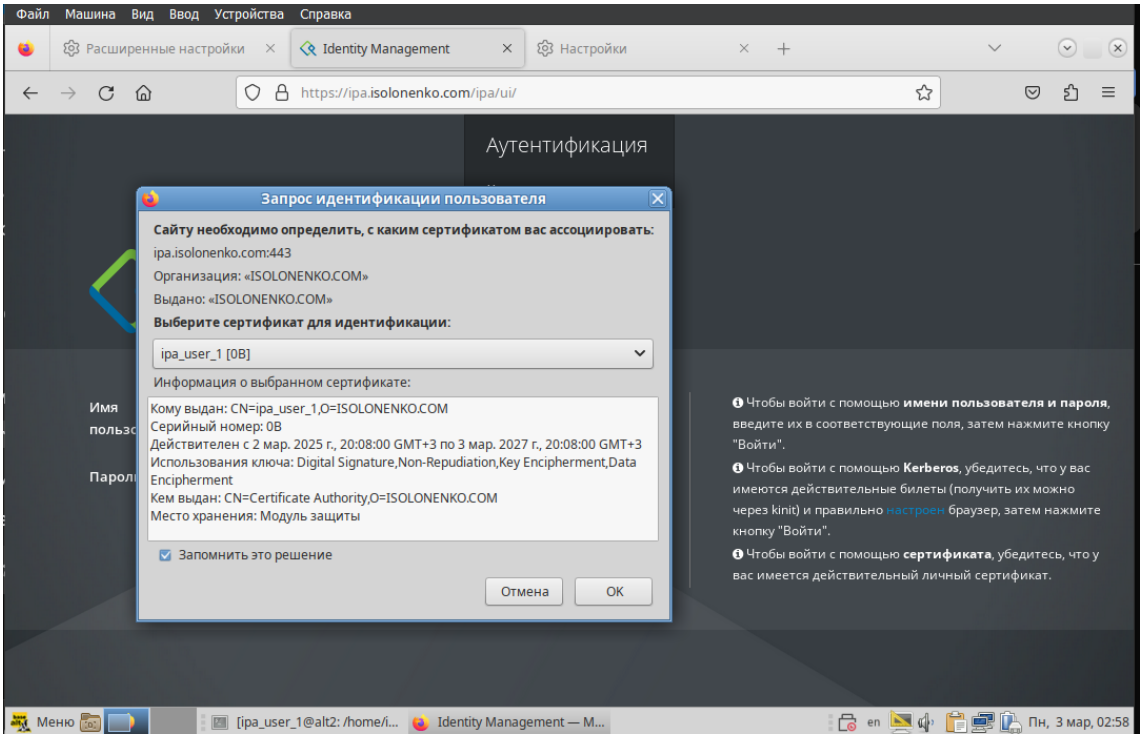


*Рис. 5. Выбор сертификата пользователя в браузере для аутентификации в Web-консоль FreeIPA*

Таким образом, пользователю необходимо обладать двумя факторами: пароль от контейнера и действующий сертификат, право владения которым он подтверждает наличием закрытого ключа.

## *Заключение*

С целью исследования реализации подхода к двухфакторной аутентификации представлена концепция аутентификации пользователей в домене *FreeIPA* в инфраструктуре ОС *ALT* с использованием OTP-кода и сертификата цифровой подписи в качестве второго фактора. Концепция подвергается масштабированию за счет использования доменных политик, управляемых централизованно. Практическая значимость исследования обусловлена использованием отечественной ОС *ALT* и ПО исключительно открытого доступа. Такой подход позволяет реализовать механизм двухфакторной аутентификации пользователей в ОС и инфраструктурных сервисах в импортозамещенном исполнении и без использования проприетарных продуктов, что является преимуществом для малых и средних организаций.

## *Список источников*

1. Государственный реестр сертифицированных средств защиты информации // Реестры ФСТЭК России. Федеральная служба по техническому и экспортному контролю. – ФСТЭК России, 2025. – URL: https://reestr.fstec.ru/reg3 (дата обращения: 10.09.2025).
2. tcb – ALT Linux Wiki // ALT Linux Wiki : [база знаний]. – URL: https://www.altlinux.org/Tcb (дата обращения: 10.09.2025).
3. Боцман С. А., Карасева Е. А. Замена Active Directory на отечественные аналоги: анализ, выбор и внедрение // Universum: технические науки. – 2025. – №8. – С. 11-15.
4. Компьютерные сети : учебник и практикум для вузов / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. – Москва : Издательство Юрайт, 2025. – 515 с.

5. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. – Москва : Издательство Юрайт, 2025. – 310 с.
6. Внуков, А. А. Защита информации в банковских системах : учебник для вузов / А. А. Внуков. – 2-е изд., испр. и доп. – Москва : Издательство Юрайт, 2025. – 246 с.
7. Редикульцев Р. Н. О проблеме надежной идентификации пользователей в сетях общего пользования // Решетневские чтения. - 2017. - №8. - С. 424-225.
8. FreeIPA/Установка сервера FreeIPA – ALT Linux Wiki // ALT Linux Wiki : [база знаний]. – URL: https://www.altlinux.org/FreeIPA/Установка_сервера_FreeIPA (дата обращения: 10.09.2025).
9. FreeIPA/Клиент – ALT Linux Wiki // ALT Linux Wiki: [база знаний]. – URL: https://www.altlinux.org/FreeIPA/Клиент (дата обращения: 10.09.2025).
10. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование : Практикум. Учебное пособие для вузов / А. Г. Уймин. – Санкт-Петербург : Издательство «Лань», 2024. – 116 с.