Средство двухфакторной аутентификации Aladdin SecurLogon

Руководство системного программиста (Руководство администратора)

RU.АЛДЕ.03.12.010 32 01

Версия	3.0
Статус	Публичный
Дата	06.03.2024
Номер	RU.АЛДЕ.03.12.010 32 01

Авторские права, товарные знаки, ограничения

Ограничение ответственности

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены АО «Аладдин Р.Д.» без предварительного уведомления.
АО «Аладдин Р.Д.» не гарантирует ни отсутствия ошибок в данном документе, ни того, что описанное программное обеспечение (ПО) не содержит дефектов, будет работать в произвольно выбранных условиях и при этом удовлетворять всем требованиям, которые могут быть к нему предъявлены.
АО «Аладдин Р.Д.» не гарантирует работоспособность нелегально полученного программного обеспечения.
Нелегальное использование программного обеспечения и документации на него преследуется по закону.
Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе АО «Аладдин Р.Д.» не предоставляет никаких ни явных, ни подразумеваемых гарантий.
АО «Аладдин Р.Д.» НЕ НЕСЁТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ ИЛИ ПОБОЧНЫЕ УБЫТКИ), ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЁННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОГО КОМПОНЕНТА ОПИСАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ АО «Аладдин Р.Д.» БЫЛО ПИСЬМЕННО УВЕДОМЛЕНО О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

Государственное регулирование и экспортный контроль

Описываемый в данном документе продукт (или продукты) может являться или содержать в себе средство криптографической защиты информации (СКЗИ), являющееся предметом экспортного контроля.
Вы соглашаетесь с тем, что продукт не будет поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону образом.
Вы гарантируете, что будете соблюдать накладываемые на экспорт и реэкспорт продукта ограничения.
Сведения, приведённые в данном документе, актуальны на дату его публикации.

Лицензионное соглашение

Пожалуйста, внимательно прочитайте данное лицензионное соглашение прежде, чем использовать содержимое данного комплекта и/или прежде, чем загружать или устанавливать программное обеспечение.
Все указания по использованию программного обеспечения, предоставляемые Закрытым акционерным обществом «Аладдин Р. Д.» (или любым его дочерним предприятием – каждое из них упоминаемое как «компания»), подчиняются и будут подчиняться условиям, оговоренным в данном соглашении. Загружая данное программное обеспечение (как определено далее по тексту) и/или устанавливая данное программное обеспечение на Ваш компьютер и/или используя данное программное обеспечение иным способом, Вы принимаете данное соглашение и соглашаетесь с его условиями.
Если Вы не согласны с данным соглашением, не загружайте и/или не устанавливайте данное программное обеспечение и незамедлительно (не позднее 7 (семи) дней с даты ознакомления с настоящим текстом) верните этот продукт в АО «Аладдин Р.Д.», удалите данное программное обеспечение и все его части со своего компьютера и не используйте его никоим образом.

Настоящее лицензионное соглашение (далее «Соглашение») является договором, заключенным между Вами (физическим или юридическим лицом) — конечным пользователем (далее «Пользователь») — и АО «Аладдин Р.Д.» (далее «Компания») относительно передачи неисключительного права на использование настоящего программного обеспечения, являющегося интеллектуальной собственностью Компании.

Права и собственность

ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ.
Программное обеспечение, включая все переработки, исправления, модификации, дополнения, обновления и/или усовершенствования к нему (далее по всему тексту и любой его части определяемое как Программное обеспечение или ПО), и связанная с ним документация предназначается НЕ ДЛЯ ПРОДАЖИ и является и остаётся исключительной собственностью Компании.

Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), подтверждённые или включённые в приложенные/взаимосвязанные/имеющие отношение к данному руководству, данные, содержащиеся в нём, а также все права на ПО являются и будут являться собственностью исключительно Компании.
подлежит отмене согласно условиям данного Соглашения. Ничто в данном Соглашении не подтверждает отказ Компании от прав на интеллектуальную собственность по какому бы то ни было законодательству.

Лицензия

Компания настоящим предоставляет Вам, а Вы получаете индивидуальное, неисключительное и отзываемое ограниченное право на использование данного ПО только в форме исполняемого кода, как описано в прилагаемой к ПО технической/эксплуатационной документации, и только в соответствии с условиями данного **Соглашения:**

Вы можете установить ПО и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей технической/эксплуатационной документации ПО и в настоящем соглашении.

Вы можете добавить/присоединить Программное обеспечение к программам для мобильных устройств с единственной целью, описанной в данном Соглашении. Принимая условия настоящего соглашения, Вы соглашаетесь:

- не использовать, не модифицировать и не выдавать сублицензии на данное Программное обеспечение и любое другое ПО Компании, за исключением явных разрешений в данном Соглашении;

- не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения;

- не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть;

- не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому-либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

Требования к использованию

Программное обеспечение должно использоваться и обслуживаться строго в соответствии с описаниями и инструкциями Компании, приведёнными в данном и других документах Компании, в том числе на портале онлайн документации для разработчиков Компании (http://developer.aladdin-rd.ru/).

Данное соглашение не передаёт Вам права на Программное обеспечение, а лишь предоставляет ограниченное право на использование, которое

Использование ПО

Пользователь вправе:

- воспроизводить ПО путём записи его в память электронно-вычислительных машин Пользователя, ограниченное правом инсталляции, копирования и запуска программ для ЭВМ;

- встраивать ПО любым способом в продукты и решения Пользователя;

- распространять ПО любым способом исключительно в составе продуктов и решений Пользователя.

При использовании и распространении ПО Пользователь обязан руководствоваться действующим законодательством Российской Федерации и международным законодательством, учитывая ограничения и дополнительные требования, которые могут возникать в связи с экспортом шифровальных (криптографических) средств с территории Российской Федерации и импортом таких средств в другие страны. В частности, ограничения и дополнительные требования могут возникать при распространении ПО через магазины приложений, содержащие различные приложения для мобильных устройств.

Условия использования, изложенные в настоящем соглашении, действуют в отношении всего содержимого ПО, в частности в отношении:

- дизайна (графики, расположения элементов оформления и т.п.);

- всех иных элементов, в том числе изображений, фонограмм, текстов.

Получаемые Пользователем неисключительные имущественные права не включают права на передачу третьим лицам каких-либо прав на встраивание, воспроизведение, распространение и использование программ для ЭВМ не в составе продуктов и решений Пользователя.

Компания сохраняет за собой все исключительные права на ПО и входящие в него компоненты, включая права на предоставление неисключительных и исключительных прав третьим лицам.

Пользователь вправе осуществлять использование ПО в пределах, предусмотренных настоящим Соглашением, исключительно на территории Российской Федерации.

Обслуживание и поддержка

Компания не несёт обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов ПО.

Ограниченная гарантия

Компания гарантирует, что программное обеспечение с момента приобретения его Вами в течение 12 (двенадцати) месяцев будет функционировать в полном соответствии с его технической/эксплуатационной документацией, при условии, что ПО будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

Отказ от гарантии

Компания не гарантирует, что программное обеспечение будет соответствовать Вашим желаниям и требованиям, или что его работа будет бесперебойной или безошибочной. В объёме, предусмотренном законодательством РФ, компания открыто отказывается от всех гарантий, не оговоренных здесь, от всех иных подразумеваемых гарантий. Ни один из дилеров, дистрибьюторов, продавцов, агентов или сотрудников компании не уполномочен производить модификации, расширения или дополнения к данной гарантии.

Если Вы произвели какие-либо модификации ПО или любой из его частей во время гарантийного периода, ПО подверглось повреждению, неосторожному или неправильному обращению, если Вы нарушили любое из условий настоящего Соглашения, то гарантия, упомянутая выше в разделе 5, будет немедленно прекращена.

Гарантия недействительна, если ПО используется в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в технической/эксплуатационной документации, или используется на компьютере с любым установленным нелицензионным программным обеспечением.

Ограничение возмещения

В случае нарушения гарантии, оговоренной выше, Компания может по собственному усмотрению:

- заменить ПО, если это не противоречит вышеупомянутому ограничению гарантии;

- возместить стоимость, выплаченную Вами за ПО.

Гарантийные требования должны быть выставлены в письменном виде в течение гарантийного периода, но не позднее 7 (семи) дней с момента обнаружения дефекта, и содержать в себе подтверждения, удовлетворяющие Компанию. Всё ПО (все экземпляры, имеющиеся у Вас) должно быть возвращено Компании и отправлено возвращающей стороной с оплаченной стоимостью перевозки и, при необходимости, страховки. Экземпляры ПО должны быть отправлены с копией платёжных документов и накладных. Исключение косвенных убытков

Стороны признают, что Программное обеспечение не может быть полностью лишено ошибок. Компания не несёт ответственности (как в силу договора, гражданского правонарушения, включая халатность, так и в любой иной форме) перед Вами или любой третьей стороной за любые потери или убытки (включая косвенные, фактические, побочные или потенциальные убытки), включая, без ограничений, любые потери или убытки прибыльности бизнеса, потерю доходности или репутации, утраченную или искажённую информацию или документацию вследствие какого-либо использования данного программного обеспечения и/или любой компоненты данного по, даже если компания письменно уведомлена о возможности подобных убытков.

Ограничение ответственности

В случае если, несмотря на условия данного соглашения, компания признана ответственной за убытки на основании каких-либо дефектов или несоответствия программного обеспечения Вашим ожиданиям, полная ответственность за каждый экземпляр дефектного программного обеспечения не будет превышать суммы, выплаченной вами АО «Аладдин Р.Д.» за это ПО.

Прекращение действия соглашения

В случае невыполнения Вами условий данного Соглашения действие Вашей лицензии и настоящего Соглашения будет прекращено.

После прекращения действия данного Лицензионного соглашения:

- лицензия, предоставленная Вам данным Соглашением, прекращает своё действие, и Вы после её прекращения не сможете продолжать дальнейшее использование данного Программного обеспечения и других лицензионных Продуктов;

- вы незамедлительно вернёте в Компанию все экземпляры ПО и все копии такового и/или сотрёте/удалите любую информацию, содержащуюся в электронном виде.

Применимое законодательство

Данное Соглашение должно быть истолковано и определено в соответствии с законодательством Российской Федерации (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Невозможность для любой из сторон воспользоваться любым из прав, предоставленных ей по данному Соглашению, или принять меры против другой стороны в случае любого нарушения своих обязательств по Соглашению не должно рассматриваться как отказ этой стороны от последующего понуждения к признанию своих прав или совершению последующих действий в случае дальнейших нарушений.

Государственное регулирование и экспортный контроль

Вы соглашаетесь с тем, что ПО не будет Вами поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону и условиям настоящего соглашения образом. ПО является предметом дополнительного экспортного контроля, относящегося к Вам или Вашей юрисдикции. Вы гарантируете, что будете соблюдать накладываемые ограничения на экспорт и реэкспорт ПО.

Разное

Настоящее Соглашение представляет собой полное соглашение, относящееся к данной лицензии, и может быть изменено только посредством письменного соглашения, подписанного обеими сторонами. Если выполнение какого-либо условия настоящего Соглашения представляется невозможным, такое условие будет скорректировано только в пределах, обеспечивающих возможность выполнения данного условия.

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ, И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ. Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ. ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНАВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

Аннотация

Настоящий документ является руководством администратора средства двухфакторной аутентификации Aladdin SecurLogon (далее по тексту – SecurLogon, программное средство, программное средство SecurLogon, программа).

Руководство определяет порядок подготовки, установки, настройки и администрирования программного средства SecurLogon. Перед установкой и эксплуатацией программного средства рекомендуется внимательно ознакомиться с настоящим руководством.

Характер изложения материала данного руководства предполагает, что вы знакомы с операционной системой компьютера, на котором работает SecurLogon (ОС семейства Linux, подробнее перечень поддерживаемых ОС смотри в пункте 2.1 настоящего руководства) и владеете базовыми навыками администрирования для работы в ней.

Настоящий документ ориентирован на администраторов безопасности, ответственных за установку, настройку и сопровождение систем безопасности организации.

Настоящий документ соответствует требованиям к разработке эксплуатационной документации, определённым в методическом документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утверждённого приказам ФСТЭК России от 02 июня 2020 г. №76 по 4 уровню доверия.

Таблица 1 – Соответствие документации требованиям доверия – раздел 16 «Требования к разработке эксплуатационной документации»

Требования доверия (16.1 Руководство пользователя должно содержать описание)	Раздел настоящего документа, в котором представлено свидетельство
действий по приёмке поставленного средства	раздел 3 «Действия по приёмке поставленного средства»
действий по безопасной установке и настройке средства	раздел 1 «Общие сведения о программе», подраздел 1. «Действия по безопасной установке и настройке программы»
действий по реализации функций безопасности среды функционирования средства	раздел 1 «Общие сведения о программе», подраздел 1.5 «Действия по реализации функций безопасности среды функционирования программы»

СОДЕРЖАНИЕ

1. Общие сведения о программе

1.1 Назначение программы

Средство двухфакторной аутентификации SecurLogon предназначено для предотвращения несанкционированного доступа к системе и данным на переносных и настольных ПК. Позволяет повысить сетевую безопасность, упростить управление и защиту паролями.

1.2 Функции, выполняемые программой

Средство двухфакторной аутентификации SecurLogon позволяет настроить следующие виды аутентификации:

- простую локальную аутентификацию;
- строгую локальную аутентификацию (с применением сертификата доступа, записанного на устройство аутентификации (далее по тексту – электронный ключ, токен), защищаемое PIN-кодом);
- усиленную локальную аутентификацию (с применением профиля пользователя, записанного на устройство аутентификации, защищаемое PIN-кодом);
- простую сетевую аутентификацию;
- строгую сетевую аутентификацию (с применением сертификата доступа, записанного на устройство аутентификации, защищаемое PIN-кодом);
- усиленную сетевую аутентификацию (с применением профиля пользователя, записанного на устройство аутентификации, защищаемое PIN-кодом);
- усиленную сетевую аутентификацию (с применением одноразового пароля OTP);
- строгую удалённую по протоколу RDP аутентификацию (с применением сертификата доступа, записанного на устройство аутентификации, защищаемое PIN-кодом);
- строгую удалённую по протоколу RDP аутентификацию (с применением профиля пользователя, записанного на устройство аутентификации, защищаемое PIN-кодом).

1.3 Комплект поставки

Комплект поставки включает:

- Программное обеспечение «Средство двухфакторной аутентификации Aladdin SecurLogon« на носителе оптической записи (файлы архивов в формате .tgz). Состав архивов приведён в **Таблица 2**.

Таблица 2 – Состав архивов дистрибутивов SecurLogon

Файл	Описание
`SecurLogon_<версия>_al1.6_x64.tgz`	Дистрибутив установки Aladdin SecurLogon для операционных систем Astra Linux Special Edition 1.6 (Смоленск).
`SecurLogon_<версия>_al1.7_x64.tgz`	Дистрибутив установки Aladdin SecurLogon для операционных систем Astra Linux Special Edition 1.7 (Воронеж).
`SecurLogon_<версия>_al2.12.43_x64.tgz`	Дистрибутив установки Aladdin SecurLogon для операционных систем Astra Linux Special Edition 2.12 (Орёл).
`SecurLogon_<версия>_alt_x64.tgz`	Дистрибутив установки Aladdin SecurLogon для операционной системы Альт 8 СП, Альт 9, Альт 10.

Файл	Описание
`SecurLogon_<версия>_ro7.2_x64.tgz`	Дистрибутив установки Aladdin SecurLogon для операционной системы РЕД ОС 7.2.
`SecurLogon_<версия>_ro7.3_x64.tgz`	Дистрибутив установки Aladdin SecurLogon для операционной системы РЕД ОС 7.3.

- Копия сертификата соответствия системы сертификации средств защиты информации по требованиям безопасности информации (рег. № РОСС RU.0001.01БИ00) в цифровом или бумажном виде;
- Контрольная сумма файла архива программного обеспечения «Средство двухфакторной аутентификации Aladdin SecurLogon« на носителе оптической записи;
- Эксплуатационная документация:
  - «Средство двухфакторной аутентификации Aladdin SecurLogon. Формуляр» RU.АЛДЕ.03.12.010 30 01-1;
  - «Средство двухфакторной аутентификации Aladdin SecurLogon. Формуляр. Приложение. Свидетельства о приёмке, упаковке и маркировке» RU.АЛДЕ.03.12.010 30 01-2;
  - «Средство двухфакторной аутентификации Aladdin SecurLogon. Описание применения» RU.АЛДЕ.03.12.010 31 01;
  - «Средство двухфакторной аутентификации Aladdin SecurLogon. Руководство системного программиста (Руководство администратора)» RU.АЛДЕ.03.12.010 32 01;
  - «Средство двухфакторной аутентификации Aladdin SecurLogon. Руководство оператора (Руководство пользователя)» RU.АЛДЕ.03.12.010 34 01.

1.4 Действия по безопасной установке и настройке программы

Установка программного средства производится только с диска, получаемого от разработчика, после выполнения действий по приёмке поставленного средства.

Установка (изменение) программного обеспечения компьютеров и локальной вычислительной сети должна осуществляться только в присутствии и под контролем администратора информационной безопасности того технологического участка, в котором эксплуатируется данное программное средство.

Настройка программного средства должна проводится привилегированным пользователем с правами администратора, допускаемым к установке и настройке программного средства «Средство двухфакторной аутентификации Aladdin SecurLogon«.

1.5 Действия по реализации функций безопасности среды функционирования программы

Для безопасной работы программного средства в среде операционной системы должно обеспечиваться:

- предотвращение несанкционированного доступа к идентификаторам и паролям привилегированных пользователей (администратора);
- разделение полномочий (ролей) пользователей;
- порядок обработки, хранения и передачи аутентификационной информации пользователей, созданной программным средством;
- срок хранения информации о зарегистрированных событиях безопасности не менее трех месяцев;
- синхронизация внутренних системных часов информационной системы для регистрации всех событий безопасности в журнале событий;

- защита аппаратного обеспечения с функционирующим программным средством от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

1.6 Описание работы программы

Для успешного входа в систему пользователь должен подсоединить своё устройство аутентификации (электронный ключ) к компьютеру и ввести PIN-код устройства.

Операционная система авторизует пользователя в результате успешной аутентификации на основе данных, размещённых в защищённой памяти электронного ключа JaCarta. Это может быть:

- сертификат доступа – как выпущенный центром сертификации, так и самоподписанный;
- профиль учётной записи пользователя, т. е. его логин и пароль. Пароль в профиле SecurLogon может быть задан вручную или сгенерирован автоматически. В последнем случае можно задать периодичность, с которой он будет автоматически изменяться. Возможность входа в систему при этом сохраняется.

SecurLogon также позволяет настроить поведение операционной системы при извлечении пользователем электронного ключа при активном сеансе входа в систему, возможны следующие варианты:

- бездействие, когда при активном сеансе входа работа системы не прерывается;
- блокировка сеанса входа пользователя – в этом случае для возобновления доступа пользователь должен вновь подсоединить свой электронный ключ к компьютеру и ввести PIN-код;
- выключение компьютера.

1.7 Примеры применения программы

1.7.1 Локальная аутентификация

Прежде всего начнем с локальной аутентификации, когда пользователь хочет войти непосредственно на рабочую станцию, не входящую в домен.

В небольшой сети зачастую используется локальная аутентификация. При локальной аутентификации каждое устройство использует собственную базу данных комбинаций имён пользователей и паролей. Концепция локальной аутентификации показана на Рисунок 1.

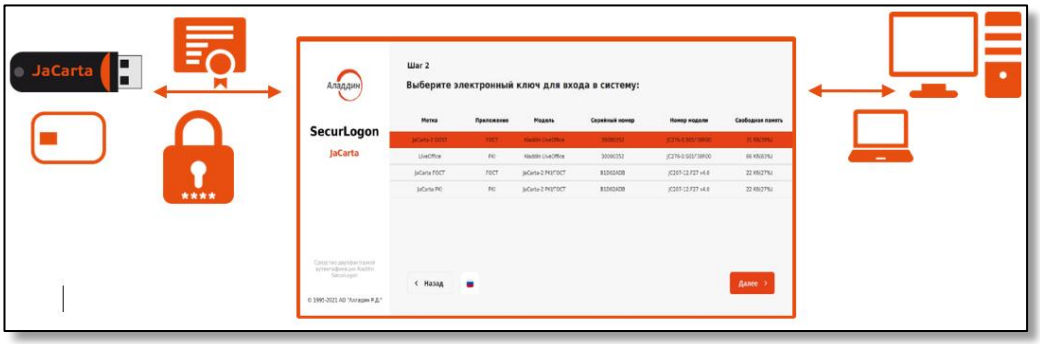

Рисунок 1 – Локальная аутентификация по профилю пользователя

Для обеспечения локальной аутентификации по профилю пользователя необходима:

- Генерация профиля:
  - администратор безопасности на своём компьютере или на компьютере пользователя средствами SecurLogon генерирует сертификат или профиль пользователя. Сгенерированная аутентификационная информация сохраняется в защищённом разделе электронного ключа.
  - при генерации профиля пользователя администратор задаёт периодичность смены пароля. Перегенерация пароля происходит в автоматическом режиме. Пользователь может даже не знать о смене пароля.

- Аутентификация пользователя:
  - пользователю выдаётся электронный ключ;
  - пользователь подсоединяет электронный ключ к своему компьютеру с предустановленным и настроенным SecurLogon;
  - для входа в операционную систему пользователь подключает электронный ключ к рабочему месту и вводит PIN-код;
  - в зависимости от выбранной политики входа и выбранного способа аутентификации происходит сопоставление данных в защищённом разделе электронного ключа и в операционной системе рабочего места пользователя;
  - при успешной аутентификации пользователю предоставляется доступ к рабочему столу.

По мере роста сети и добавления дополнительных устройств в сеть поддержка локальной аутентификации, а также её масштабирование сильно затруднено.

1.7.2 Внешняя аутентификация

Внешняя аутентификация позволяет всем пользователям проходить аутентификацию посредством внешнего сетевого сервера. Концепция внешней аутентификации показана на Рисунок 2.

Внешняя аутентификация позволяет ускорить и обезопасить работу пользователя в информационной среде. Исчезает необходимость заведения паролей для каждого конкретного ресурса, а доступ ко всем разрешенным осуществляется по одному сертификату, хранящемуся в токене. При помощи этого же сертификата пользователь может осуществлять защищенный и достоверный обмен информацией по открытым каналам, а также получать удаленный доступ к корпоративной информационной системе.

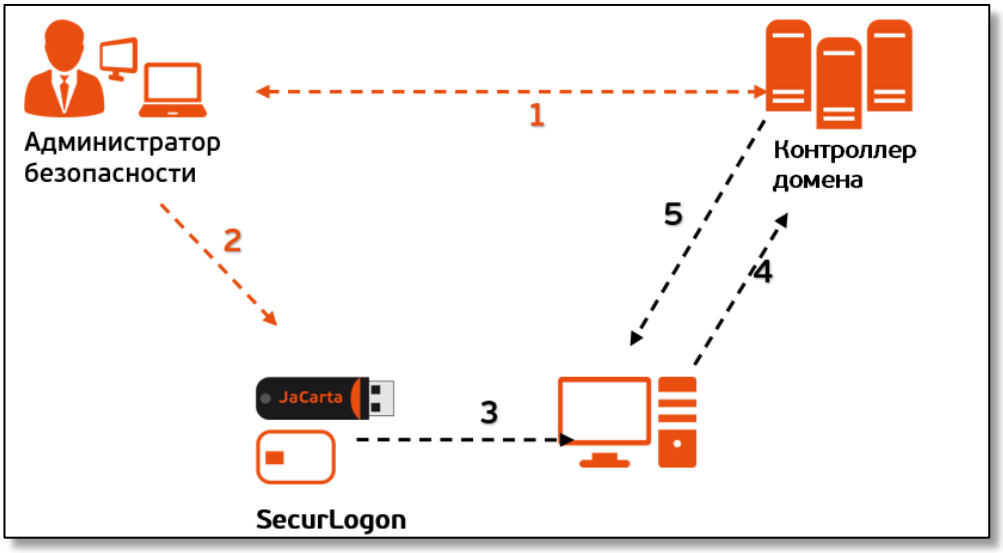

Рисунок 2 – Внешняя аутентификация

Для обеспечения внешней аутентификации необходима:

- Генерация профиля:
  - администратор безопасности посредством SecurLogon записывает доменный профиль пользователя (логин и сложный пароль) в защищённую область электронного ключа JaCarta;
  - электронный ключ с записанным на неё профилем передаётся пользователю.
- Аутентификация пользователя (см. Рисунок 2):
  - пользователю выдаётся электронный ключ (1);
  - пользователь подсоединяет электронный ключ к своему компьютеру с предустановленным и настроенным SecurLogon и вводит PIN-код, тем самым предоставляя доступ системе к закрытой области с записанным на устройстве профиле. При этом пользователь не знает свой сложный пароль, а знает только PIN-код (2).
  - профиль передаётся на сервер для проверки (3);

– сервер проверяет соответствие логина и пароля, записанного на устройство, со своей базой данных (4);
– в случае успешной аутентификации авторизует пользователя (5).

1.7.3 Аутентификация в инфраструктуре открытых ключей (PKI)

В системах аутентификации на основе PKI пользователь владеет и распоряжается электронным ключом (токеном), который обеспечивает фактор владения.

Средства аутентификации, основанные на технологии открытых ключей, обладают большей надежностью криптографических методов. Метод аутентификации основан на применении сертификата открытого ключа, выпущенного удостоверяющим центром. Концепция аутентификации в среде PKI показана на Рисунок 3.

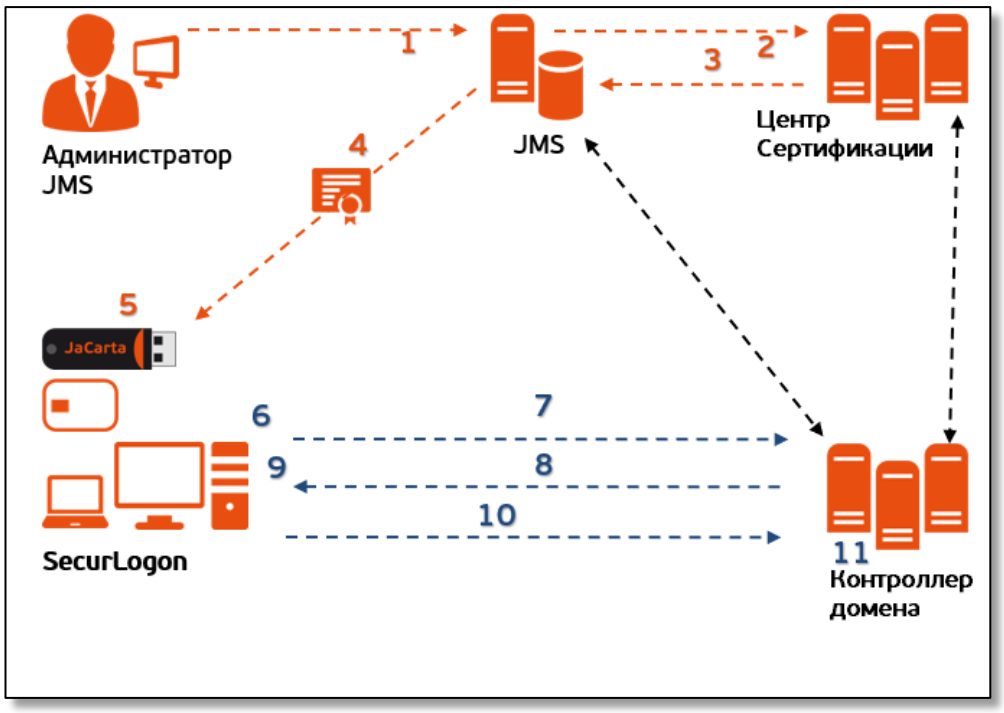

Рисунок 3 – Аутентификация в среде PKI

Для обеспечения аутентификации в среде необходима:

- Генерация сертификата:
  – администратор безопасности через консоль управления JaCarta Management System создаёт на электронном ключе закрытый ключ и формирует CSR-запрос (1);
  – JMS передаёт CSR-запрос в центр сертификации (2);
  – центр сертификации возвращает в JMS сертификат пользователя (3);
  – JMS записывает полученный сертификат пользователя в защищённую память электронного ключа JaCarta (4);
  – электронный ключ передаётся пользователю (5).
- Аутентификация пользователя:
  – пользователь полученный электронный ключ подсоединяет его к своему компьютеру с предустановленным и настроенным SecurLogon (6);
  – для входа в домен пользователь инициирует запрос на аутентификацию (7);
  – сервер отправляет пользователю набор данных с запросом их подписать (8);
  – пользователь вводит PIN-код для доступа к закрытому ключу, которым подписывается запрос (9);
  – подписанный запрос передаётся на сервер (10);
  – сервер проверяет подпись и в случае успешной аутентификации авторизует пользователя (11).

2. Условия применения программы

2.1 Требования к программному обеспечению

Требования к конфигурации программного обеспечения рабочих мест, при которых гарантируется обеспечение корректной работы SecurLogon, приведены в **Таблица 3**.

Таблица 3 – Требования к программному обеспечению

Компонент	Минимальная конфигурация
Операционная система	- Astra Linux Special Edition 1.6 (Смоленск) [1] - Astra Linux Special Edition 1.7 (Воронеж) [2] - Альт 8 СП [3] - РЕД ОС 7.2 [4] - РЕД ОС 7.3 [4]
Дополнительное ПО	Единый Клиент JaCarta

Примечания:

[1] – должно быть установлено кумулятивное обновление безопасности Astra Linux 1.6 SE, бюллетень № 20200722SE16 или новее и дополнительные пакеты:

ca-certificates; libengine-pkcs11-openssl; libnss3-tools;
freerdp2-x11; libfreerdp-client2-2; libp11-2;
krb5-pkinit; libfreerdp2-2; libpcsclite1;
libavcodec57; libgost-astra; libswresample2;
libavutil55; libnss3; libwinpr2-2;
libccid; qml-module-qt-labs-settings; opensc;
libcurl3; qml-module-qtquick-controls; qml-module- opensc-pkcs11;
pcscd; qt-labs-folderlistmodel; qml-module-qtquick-controls2.

[2] – на ОС должны быть установлены дополнительные пакеты в приведённом порядке:

ad_package qml-module-qtquick-controls2;
sssd; pcscd; libfreerdp-client2-2;
sssd-tools; opensc-pkcs11; libfreerdp2-2;
dnsutils; opensc; libwinpr2-2;
adcli; libnss3; libavcodec58;
freeipa_packages libnss3-tools; libavutil56;
dnsutils; ca-certificates; libswresample3;
freeipa-client; libengine-pkcs11-openssl; freerdp2-x11;
freeipa-admintools; qml-module-qt-labs-settings; libgost-astra;
libccid; qml-module-qt-labs-folderlistmodel; krb5-pkinit;
libp11-3; qml-module-qtquick-controls; libcurl4;
libpcsclite1; libjsoncpp1.

[3] – на ОС должны быть установлены дополнительные пакеты:

cracklib; libqt5-eglfskmssupport; libxcbutil-keysyms;
cracklib-utils; libqt5-gui; libxkbcommon-x11;
cracklib-words; libqt5-network; opensc;
freerdp; libqt5-opengl; pcsc-lite;
libcrypto1.1; libqt5-printsupport; pcsc-lite-ccid;
libcurl; libqt5-widgets; qt5-base-common;
libopensc; libqt5-xcbqpa; qt5-graphicaleffects;
libp11; libts0; qt5-qtbase-gui;
libpwquality; libxcb-render-util; qt5-quickcontrols;
libqt5-core; libxcbutil-icccm; qt5-quickcontrols2;
libqt5-dbus; libxcbutil-image; rsyslog.

[4] – на ОС должны быть установлены дополнительные пакеты:

brotli; pcre2-utf16; qt5-qtgraphicaleffects;
engine_pkcs11; pcsc-lite; qt5-qtquickcontrols;
freerdp; pcsc-lite-ccid; qt5-qtquickcontrols2;
freerdp-libs; pcsc-lite-libs; qt5-qtxmlpatterns;
krb5-pkinit; qt-settings; xcb-util-image;
libcurl; qt5-qtbase; xcb-util-keysyms;
libp11; qt5-qtbase-common; xcb-util-renderutil;
libwinpr; qt5-qtbase-gui; xcb-util-wm.
openh264-libs; qt5-qtdeclarative;

opensc;

2.2 Требование к вводу ПК в домен Active Directory

Для успешного применения настройки сетевой аутентификации ввод компьютера в домен должен быть выполнен строго с использованием инструментария sssd.

2.2.1 Ввод в домен ПК под управлением Astra Linux

Для ввода компьютера под управлением Astra Linux в домен Windows Active Directory или в домен Samba должен быть выполнен с использованием инструментария sssd:

- графический инструмент fly-admin-ad-sssd-client;
- инструмент командной строки astra-ad-sssd-client.

2.2.1.1 Установка пакета realmd

- Скачайте пакет realmd (соответствующей версии в соответствии с установленным обновлением ОС).
- Установите скачанный пакет сервиса D-Bus, позволяющий проводить настройку аутентификации и членства в домене, выполнив команду:

```
sudo apt install Загрузки/realmd_xxx_xx.deb
```

2.2.1.2 Установка инструмента

- Установите графический инструмент fly-admin-ad-sssd-client, выполнив команду:

```
sudo apt install fly-admin-ad-sssd-client
```

При установке графического инструмента будет автоматически установлен инструмент командной строки astra-ad-sssd-client.

2.2.1.3 Ввод в домен с помощью графического инструмента fly-admin-ad-sssd-client

- После установки пакет доступен в графическом меню: «Пуск» - «Панель управления» - «Сеть» - «Настройка клиента SSSD Fly».
- Для ввода компьютера Astra Linux в домен Active Directory нужно запустить инструмент, после запуска инструмента указать имя домена, имя и пароль администратора и нажать кнопку «Подключиться» (см. Рисунок 4).

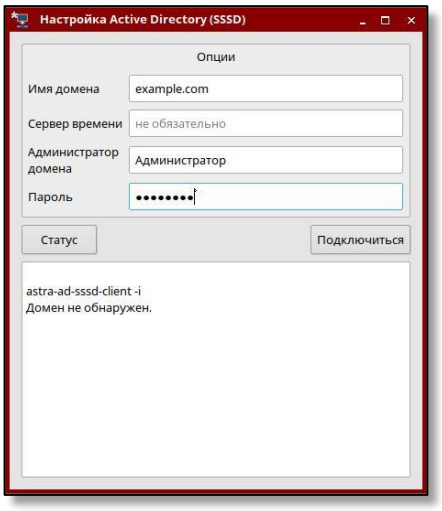

Рисунок 4 – Окно настройки клиента SSSD Fly

2.2.1.4 Ввод в домен с помощью командной строки astra-ad-sssd-client

- Ввод компьютера в домен может быть выполнен командой:

```
sudo astra-ad-sssd-client -d dc01.example.com -u Администратор
```

где:

- d dc01.example.com - указание контроллера домена;
- u Администратор - указание имени администратора домена;

Примерный диалог при выполнении команды:

```
compname = astra01

domain = dc01.example.com

username = admin

введите пароль администратора домена:

ok

продолжать? (y\N)

y

настройка сервисов...

Завершено.

Компьютер подключен к домену.

Для продолжения работы, необходимо перезагрузить компьютер!
```

- Для завершения подключения требуется перезагрузить компьютер:

```
sudo reboot
```

- Подсказка по команде astra-ad-sssd-client:

```
sudo astra-ad-sssd-client -h

Usage: astra-ad-sssd-client <ключи>

ключи:

-h,--help   этот текст

-d   домен. если отсутствует, берется из hostname.resolv.conf

-y   отключает запрос подтверждения

-i   информация по текущему подключению

-u   логин администратора домена

-n   сервер времени.

-px  получает пароль администратора домена от внешнего сценария

     через перенаправление стандартного ввода (stdin)

-p   пароль администратора домена

-U   удаление

--par     указать параметры вручную
```

- После перезагрузки проверить статус подключения можно следующими способами:
  - Получить билет Kerberos от имени администратора домена:

```
kinit admin@dc01.example.com
```

  - Проверить статус подключения:

```
sudo astra-ad-sssd-client -i
```

Подробная инструкция по вводу в домен компьютера под управлением Astra Linux приведена на официальном сайте https://wiki.astralinux.ru/.

2.2.2 Ввод в домен ПК под управлением РЕД ОС

2.2.2.1 Проверка настройки сети

- Перед вводом ПК под управлением РЕД ОС в домен проверьте настройки сети, выполнив команду:

```
ping -c 3 dc.win.redos

PING dc.win.redos (10.81.1.196) 56(84) bytes of data.

64 bytes from dc.win.redos (10.81.1.196): icmp_seq=1 ttl=128 time=0.320 ms

64 bytes from dc.win.redos (10.81.1.196): icmp_seq=2 ttl=128 time=0.601 ms

64 bytes from dc.win.redos (10.81.1.196): icmp_seq=3 ttl=128 time=0.701 ms
```

где `dc.win.redos` – имя контроллера домена.

2.2.2.2 Обновление/установка утилиты join-to-domain

- Для РЕД ОС 7.2 установите утилиту из репозитория, выполнив команду:

```
yum install join-to-domain
```

- Для РЕД ОС 7.3 выполните обновление утилиты до последней версии, выполнив команду:

```
dnf update join-to-domain
```

2.2.2.3 Ввод в домен с помощью утилиты join-to-domain в графическом режиме работы программы

- Для запуска join-to-domain в графическом режиме откройте «Главное меню» - «Системные» - «Ввод ПК в домен».
- Введите пароль пользователя root в открывшемся окне запроса.
- После успешной аутентификации в открывшемся окне утилиты выберите типа домена на базе SAMBA или FreeIPA. Нажмите кнопку <Ок>.
- В следующем окне утилиты заполните все необходимые поля и нажмите кнопку <Да> для запуска процесса присоединения ПК к домену.
- В случае успешного ввода в домен появится уведомление.
- Перезагрузите компьютер и войдите в РЕД ОС, используя логин и пароль пользователя домена.

2.2.2.4 Ввод в домен с помощью утилиты join-to-domain в консольном режиме работы программы

Откройте консоль и выполните запуск `join-to-domain.sh` с привилегиями суперпользователя root:

```
join-to-domain.sh
```

- В интерактивном режиме произведите настройку для ввода ПК в выбранном домене.
- Перезагрузите компьютер и войдите в РЕД ОС, используя логин и пароль пользователя домена.

Подробная инструкция по вводу в домен компьютера под управлением РЕД ОС приведена на официальном сайте https://redos.red-soft.ru/base/arm/arm-domen/arm-msad/join-to-domain/.

2.2.3 Ввод в домен ПК под управлением Альт

2.2.3.1 Установка пакета task-auth-ad-sssd

- Для ввода компьютера в Active Directory потребуется установить пакет task-auth-ad-sssd и все его зависимости (если он еще не установлен):

```
apt-get install task-auth-ad-sssd
```

- Синхронизация времени с контроллером домена производится автоматически.
- Предварительно должна быть выполнена настройка сети в консоли или графическом режиме.

2.2.3.2 Настройка сети в консольном режиме

- Задайте имя компьютера, выполнив команду:

```
hostnamectl set-hostname host-15.test.alt
```

- В качестве первичного DNS должен быть указан DNS-сервер домена. Для этого необходимо создать файл /etc/net/ifaces/eth0/resolv.conf со следующим содержимым:

```
nameserver 192.168.0.113
```

где `192.168.0.113` — IP-адрес DNS-сервера домена.

- Укажите службе `resolvconf` использовать DNS контроллера домена и домен для поиска. Для этого в файле `/etc/resolvconf.conf` добавить/отредактировать следующие параметры:

```
interface_order='lo lo[0-9]* lo.* eth0'

search_domains=test.alt
```

где `eth0` — интерфейс, на котором доступен контроллер домена, `test.alt` — домен.

- Обновите DNS адреса, выполнив команду:

```
resolvconf -u
```

- В результате выполненных действий в файле `/etc/resolv.conf` должны появиться строки:

```
search test.alt

nameserver 192.168.0.113
```

2.2.3.3 Ввод в домен в графическом режиме

- В Центре управления системой перейти в раздел Пользователи → Аутентификация.
- В открывшемся окне следует выбрать пункт «Домен Active Directory», заполнить поля и нажать кнопку <Применить>.
- В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку <OK>.
- При успешном подключении к домену будет выведено окно уведомления.
- Перезагрузите рабочую станцию.

2.2.3.4 Ввод в домен в консольном режиме

Для ввода ПК в домен выполните команду в командной строке:

```
system-auth write ad test.alt host-15 test 'administrator' 'Pa$$word'

Joined 'HOST-15' to dns domain 'test.alt'
```

Подробная инструкция по вводу в домен компьютера под управлением Альт приведена на официальном сайте https://docs.altlinux.org/ru-RU/alt-education/10.0/html/alt-education/activedirectory-login--chapter.html.

2.3 Требования к техническому обеспечению

Минимальные требования к техническим мощностям АРМ, с установленным ПО SecurLogon, при которых обеспечивается корректная работа ПО SecurLogon, приведены в **Таблица 4**.

Таблица 4 – Требования к техническому обеспечению

Компонент	Минимальная конфигурация
Требуемое дисковое пространство	Не менее 200 Мб
Свободная оперативная память	Не менее 2 Гб
USB-интерфейс	USB 2.0 тип A или совместимые

2.4 Требования к совместимости

2.4.1 Поддерживаемые устройства аутентификации

Для надежного хранения ключевой информации в программе SecurLogon выполнена совместимость с рядом наиболее популярных моделей устройств аутентификации:

- JaCarta 2 ГОСТ;
- JaCarta PRO;
- JaCarta PRO/ГОСТ;
- JaCarta-2 PRO/ГОСТ;
- JaCarta PKI;
- JaCarta PKI/Flash;
- JaCarta PKI/ГОСТ/Flash;
- JaCarta-2 PKI/ГОСТ;
- JaCarta PKI/ГОСТ;
- JaCarta SF/ГОСТ;
- Aladdin LiveOffice;
- eToken PRO (Java).

2.4.2 Поддерживаемое ПО

- Пользователи программного средства имеют возможность работать со следующими доменными службами:
  - Microsoft AD;
  - Samba DC;
  - ALD PRO;
  - FreeIPA.

- Пользователи программного средства имеют возможность работать со следующими центрами сертификации:
  - Aladdin Enterprise Certificate Authority;
  - Dog Tag Certificate System;
  - Microsoft Certificate Services.

2.5 Требования к пользовательским сертификатам

Для успешной двухфакторной аутентификации на рабочем месте при помощи сертификатов необходимо выполнение следующих условий:

- на электронный ключ необходимо записать пару – открытый ключ (сертификат) и закрытый ключ, помещенные в один контейнер;
- пользовательские сертификаты должны содержать следующие поля:
  - Поставщик (Issuer) - поле идентификации УЦ, выдавшего сертификат владельцу:
    - CN (CommonName) - наименование поставщика, подписывающего сертификат;
    - DC (DomainComponent) - компонент DNS имени (адреса) владельца сертификата, указывается несколько раз, в каждом случае это часть DNS пути.
    - Пример заполненного поля Issuer:
    - CN = DC_WIN-CA
    - DC = dc
    - DC = test
  - Субъект (Subject) - поле идентификации субъекта (владельца) сертификата.
    - CN (CommonName) - наименование субъекта (владельца) сертификата
    - DC (DomainComponent) - компонент DNS имени (адреса) владельца сертификата, указывается несколько раз, в каждом случае часть DNS пути.

    Пример заполненного поля Subject:

    CN = Domain User Test

    DC = dc

    DC = test
  - Дополнительное имя субъекта SAN (SubjectAltName) - дополнительные реквизиты владельца сертификата:
    - OtherName(Другое имя) - необходимо указать логин и домен пользователя по следующему шаблону Principal Name=login@domain.ru.
    - Пример заполненного поля SubjectAlternativeName Other Name:
    - Principal Name=d_user@dc.test
- у сертификата должен быть установлен период его действия;
- в сертификате должны быть указаны CRL или OCSP (если такие имеются).

3. Действия по приёмке поставленного средства

Приёмка программного обеспечения «Средство двухфакторной аутентификации Aladdin SecurLogon« предусматривает:

- проверку комплектности программного продукта;
- оценку результата подсчёта контрольной суммы для контроля целостности файлов по указанным значениям контрольных сумм в «RU.АЛДЕ.03.12.010 30 01-1 Средство двухфакторной аутентификации Aladdin SecurLogon. Формуляр».

3.1 Проверка комплектности

Проверку комплектности программного продукта производят путём сверки комплектности поставленного программного продукта с комплектностью, указанной в разделе 3 «RU.АЛДЕ.03.12.010 30 01-1 Средство двухфакторной аутентификации Aladdin SecurLogon. Формуляр».

3.2 Подсчёт контрольной суммы

Подсчёт контрольной суммы необходимо произвести с использованием предварительно установленного программного обеспечения «ФИКС-UNIX 1.0» по алгоритму «ГОСТ 34.11» пользователем с правами администратора на рабочей станции, оборудованной устройством чтения CD/DVD-дисков, под управлением программного средства в следующей последовательности:

- установить компакт-диск с дистрибутивом в устройство чтения CD/DVD-дисков;
- выполнить в командной строке:

```
sudo mount /media/cdrom -o nojoliet,norock
```

- перейти в директорию, содержащую исполняемый модуль программы «ФИКС-UNIX 1.0» (ufix), и выполнить следующие команды:

```
./ufix_eng -jR /media/cdrom/ > /tmp/contr_summ t.txt

./ufix_eng -e --alg s256 -E /tmp/contr_summ.txt /tmp/contr_summ.prj

./ufix_eng -h -E /tmp/contr_summ.prj /tmp/contr_summ.html
```

- открыть в браузере полученный файл выполнить в командной строке:

```
firefox /tmp/contr_summ.html
```

- выполнить команду:

```
 sudo umount /media/cdrom
```

3.3 Сравнение контрольной суммы

Сравнить значение контрольной суммы в строке «ВСЕГО», выданное на экран в результате подсчёта контрольных сумм программой «ФИКС-Unix 1.0», со значением, указанными в таблице 2 «RU.АЛДЕ.03.12.010 30 01-1 Средство двухфакторной аутентификации Aladdin SecurLogon. Формуляр».

Контрольные суммы DVD-диска продукта, рассчитанные с использованием программы подсчета контрольных сумм «ФИКС-Unix 1.0» должны соответствовать значениям, приведенным в таблице 2 «RU.АЛДЕ.03.12.010 30 01-1 Средство двухфакторной аутентификации Aladdin SecurLogon. Формуляр».

3.4 Результат приёмки

Результат приёмки считается положительным, если:

- комплектность программного средства соответствует заявленному «RU.АЛДЕ.03.12.010 30 01-1 Средство двухфакторной аутентификации Aladdin SecurLogon. Формуляр»;

- рассчитанные контрольные суммы, с использованием программы подсчета контрольных сумм «ФИКС-Unix 1.0», соответствуют значениям, приведенным в таблице 2 «RU.АЛДЕ.03.12.010 30 01-1 Средство двухфакторной аутентификации Aladdin SecurLogon. Формуляр».

4. Подготовка к установке программы

4.1 Установка Единого Клиента JaCarta

Произвести установку Единого Клиента JaCarta:

- Скопировать на компьютер в одну папку файлы из дистрибутива для дальнейшей инсталляции:
  - install.sh;
  - jacartauc_*_ro_x64.rpm;
  - jcpkcs11-2_*_x64.rpm;
  - jcsecurbio_*_x64.rpm;
  - RPM-GPG-KEY-ALADDIN_RD-AO.public (Открытый ключ АО «Аладдин Р.Д.»).
- Под пользователем с правами администратора запустить эмулятор терминала.
- В эмуляторе терминала прейти в папку с дистрибутивами, выполнив команду:

```
cd .../.../...
```

- Распакуйте архив с дистрибутивом Единого Клиента JaCarta в выбранную папку, выполнив команду:

```
unzip <наименование пакета>.zip -d /<путь до папки распаковки>
```

- Установить Единый Клиент JaCarta, выполнив команду с правами суперпользователя, находясь в папке распаковки архива с дистрибутивом Единого Клиента JaCarta:

```
bash install.sh
```

Подробное описание процедуры установки Единого Клиента JaCarta приведено в разделе 4 «Единый Клиент JaCarta. Руководства администратора «Аладдин Р.Д.» RU.АЛДЕ.03.01.013-01 32 01-2 [1]

4.1.1 Распаковка архива инсталляционного комплекта .tgz

- Скопировать архив с инсталлятором ПО SecurLogon на компьютер.
- Под пользователем с правами администратора запустить эмулятор терминала.
- В эмуляторе терминала прейти в папку, в которую скачан архив, выполнив команду:

```
cd <путь к папке размещения архива>
```

- Произвести распаковку архива, выполнив команду:

```
tar -xf {имя файла} -C /<путь распаковки архива>/
```

Архив будет распакован в указанную в пути папку. Состав распакованного архива приведен в **Таблица 5** для совместимых ОС.

Таблица 5 – Состав распакованного архива с ПО SecurLogon

Файл	Описание	ОС
`SecurLogon_<версия>_al1.6_x64.deb` `update.sh`	пакет ПО SecurLogon запуск сценария автоматического обновления ПО	Astra Linux Special Edition 1.7 (Воронеж)
`SecurLogon_<версия>_al1.6_x64.deb` `update.sh`	пакет ПО SecurLogon запуск сценария автоматического обновления ПО	Astra Linux Special Edition 1.6 (Смоленск)

Файл	Описание	ОС
`SecurLogon_<версия>_al2.12.43_x64.deb` `update.sh`	пакет ПО SecurLogon запуск сценария автоматического обновления ПО	Astra Linux Special Edition 2.12 (Орёл)
`SecurLogon_<версия>_alt8_x64.rpm` `update.sh`	пакет ПО SecurLogon запуск сценария автоматического обновления ПО	Альт 8 СП
`SecurLogon_<версия>_alt9_x64.rpm` `update.sh`	пакет ПО SecurLogon запуск сценария автоматического обновления ПО	Альт 9 Альт 10
`SecurLogon_<версия>_ro7.2_x64.rpm` `update.sh`	пакет ПО SecurLogon запуск сценария автоматического обновления ПО	РЕД ОС 7.2
`SecurLogon_<версия>_ro7.3_x64.rpm` `update.sh`	пакет ПО SecurLogon запуск сценария автоматического обновления ПО	РЕД ОС 7.3

5. Установка программы

5.1 Инициализация процесса установки программы

- Запустите процесс установки программы и автоматической загрузки зависимостей во время выполнения установки пакета с правами суперпользователя (от имени пользователя root, либо с использованием sudo) из папки с распакованным архивом, выполнив команду:

РЕД ОС	`sudo dnf install ./<наименование пакета>.rpm`
Astra Linux	`sudo apt install ./<наименование пакета>.deb`
Альт	`sudo dnf install ./<наименование пакета>.rpm`

5.2 Процесс установки

После инициализации процесса установки интерактивный инсталлятор запущен. В процессе установки в системе должен присутствовать необходимый диск с дистрибутивом ОС в CD-ROM или доступ к официальному репозиторию. Происходит автоматическая загрузка и установка пакетов из репозитория. Состав пакетов для каждой ОС приведен в Примечаниях к таблице 3 в разделе 2, подразделе 2.1 настоящего Руководства Администратора.

5.3 Дополнительные возможные действия при установке

5.3.1 Справка

Получить справку по установочному скрипту можно, выполнив команду из папки, в которой ранее была произведена распаковка архива (см. Таблица 7):

```
sudo ./install.sh -help
```

5.3.2 Установка зависимостей для AD

В случае сетевой аутентификации в доменной среде Active Directory, требуется установка зависимости для доменной службы Active Directory. Произвести установку зависимости из папки, в которую ранее была произведена распаковка архива, выполнив команду:

```
sudo ./install.sh --ad
```

5.3.3 Установка зависимостей для FreeIPA

В случае сетевой аутентификации в доменной среде FreeIPA, требуется установка зависимости для доменной службы FreeIPA. Произвести установку зависимости из папки, в которую ранее была произведена распаковка архива, выполнив команду:

```
sudo ./install.sh --freeipa
```

5.3.4 Скачивание и архивация зависимостей.

Для создания локального репозитория и возможного переноса сформированных пакетов на другое рабочее место произведите скачивание и архивацию зависимостей, выполнив команду из папки, в которую ранее была произведена распаковка архива:

```
sudo ./install.sh --download
```

5.4 Описание файлов установленного пакета

Список файлов установленного пакета ПО SecurLogon приведен в **Таблица 6**.

Таблица 6 – Описание файлов установленного пакета ПО SecurLogon

Путь установки	Имя файла	Описание	Операционная система
/etc/pam.d	пакет SecurLogon: jc-tf-auth jc-tf-auth_nopki jc-tf-net-auth jc-tf-net-auth_nopki	конфигурационные файлы, отвечающие за аутентификацию пользователя	РЕД ОС 7.2 РЕД ОС 7.3
/lib64/security/	пакет SecurLogon: pam_jc_nopki.so pam_jc_pki.so pam_jc_sss.so	системные функции аутентификации	РЕД ОС 7.2 РЕД ОС 7.3
/usr/bin/	пакет SecurLogon: jcsecurlogon-pkexec пакет jcsecurlogond: jc-lock jc-greeter.py jc-screenlocker.py jc_screenlocker	модули графического интерфейса	РЕД ОС 7.2 РЕД ОС 7.3
/usr/local/etc/jcsecurlogon	пакет SecurLogon: jcsecurlogon.conf пакет jcsecurlogond: jcsecurlogond.conf	конфигурационные файлы управления локальной и сетевой аутентификации	РЕД ОС 7.2 РЕД ОС 7.3
/usr/sbin/	пакет SecurLogon: jcsecurlogon jcsecurlogonupdater пакет jcsecurlogond: jcsecurlogond	модуль настройки двухфакторной аутентификации, сервис обновлений ПО, модуль безопасности	РЕД ОС 7.2 РЕД ОС 7.3
/usr/share/applications	пакет SecurLogon: jcsecurlogonRedOS.desktop	файл для создания ярлыка	РЕД ОС 7.2 РЕД ОС 7.3
/usr/share/icons	пакет SecurLogon: jcsecurlogon.ico	файл хранения значка программы	РЕД ОС 7.2 РЕД ОС 7.3
/usr/share/polkit-1/action	пакет SecurLogon: ru.aladdin-rd.pkexec.jcsecurlogon.policy	файл правил для удалённого запуска SecurLogon	РЕД ОС 7.2 РЕД ОС 7.3
/etc/init.d/	пакет jcsecurlogond: jcsecurlogond	модуль безопасности системы	РЕД ОС 7.2 РЕД ОС 7.3
/etc/xdg/AladdinRD/	пакет jcsecurlogond: jc-greeter.conf	конфигурационный файл для темы входа и блокировки	РЕД ОС 7.2 РЕД ОС 7.3
/usr/share/xgreeters/	пакет jcsecurlogond: jc_lightdm_greeter.desktop	файл для запуска графической темы входа	РЕД ОС 7.2 РЕД ОС 7.3
/usr/local/etc/	пакет jcsecurlogond: jcsecurlogon	модуль настройки двухфакторной аутентификации	РЕД ОС 7.2 РЕД ОС 7.3
/etc/pam.d/	пакет securlogon: jc-tf-auth jc-tf-auth_nopki jc-tf-net-auth	конфигурационные файлы, отвечающие за аутентификацию пользователя	Astra Linux Special Edition 1.6 (Смоленск)

Путь установки	Имя файла	Описание	Операционная система
	jc-tf-net-auth_nopki		
/lib/x86_64-linux-gnu/security/	пакет securlogon: pam_jc_pki.so pam_jc_nopki.so pam_jc_sss.so	системные функции аутентификации	Astra Linux Special Edition 1.6 (Смоленск)
/usr/bin/	пакет securlogon: jcsecurlogon-pkexec	модули графического интерфейса	Astra Linux Special Edition 1.6 (Смоленск)
/usr/local/etc/	пакет securlogon: jcsecurlogon пакет jcsecurlogond: jcsecurlogon	модуль настройки двухфакторной аутентификации	Astra Linux Special Edition 1.6 (Смоленск)
/usr/sbin/	пакет securlogon: jcsecurlogonupdater пакет jcsecurlogond: jc-greeter.py jc-screenlocker.py jc_screenlocker jcsecurlogond	сервис обновлений ПО, модуль темы входа, модули блокировки сеанса	Astra Linux Special Edition 1.6 (Смоленск)
/usr/share/applications/	пакет securlogon: jcsecurlogon.desktop	файл для создания ярлыка	Astra Linux Special Edition 1.6 (Смоленск)
/usr/share/icons/	пакет securlogon: jcsecurlogon.png	файл хранения значка программы	Astra Linux Special Edition 1.6 (Смоленск)
/usr/share/polkit-1/actions/	пакет securlogon: ru.aladdin-rd.pkexec.jcsecurlogon.policy	файл правил для удалённого запуска SecurLogon	Astra Linux Special Edition 1.6 (Смоленск)
/usr/local/etc/jcsecurlogon/	пакет securlogon: jcsecurlogon.conf пакет jcsecurlogond: jcsecurlogond.conf	конфигурационные файлы управления локальной и сетевой аутентификации	Astra Linux Special Edition 1.6 (Смоленск)
/etc/init.d/	пакет jcsecurlogond: jcsecurlogond	модуль безопасности системы	Astra Linux Special Edition 1.6 (Смоленск)
/usr/lib/x86_64-linux-gnu/	пакет jcsecurlogond: libfly-dmgreet_jacarta.so	библиотека для предоставления графической темы входа	Astra Linux Special Edition 1.6 (Смоленск)
/etc/xdg/AladdinRD	пакет jcsecurlogond: jc-greeter.conf	конфигурационный файл для темы входа и блокировки	Astra Linux Special Edition 1.6 (Смоленск)

6. Запуск программы

6.1 Запуск программы в терминале после запуска графической оболочки ОС

- Синтаксис запуска программы выглядит таким образом (от имени суперпользователя с правами root):

```
sudo jcsecurlogon
```

6.1.1 Дополнительные параметры запуска программы и настройки аутентификации в терминале

- Общая структура команды с использованием опций:

```
sudo jcsecurlogon [опция]
```

Основные опции, которые можно использовать при запуске программы SecurLogon в терминале приведены в Таблица 7.

Таблица 7 – Опции при запуске программы SecurLogon

Опция	Описание
общие опции	
--h или --help	Отображение справки по параметрам
--help-all	Отображение справки по параметрам, включая специфические опции
-v или --version	Отображения версии
--license-file <файл>	Для принятия лицензии. Если путь до файла с лицензией содержит пробелы, то его необходимо указывать в кавычках
--notification	Отображение уведомления о продлении лицензии
--kdc <host_name>	Адрес KDC
опции для создания профиля на электронном ключе	
--generate-profile	Сгенерировать профиль
--slot-id <ID>	Идентификатор слота электронного ключа JaCarta в шестнадцатеричном виде (HEX)
--pin <PIN>	PIN-код пользователя
--profile-user <пользователь>	Имя пользователя
--password <пароль>	Пароль профиля
--domain <домен>	Название домена
--rewrite	Переписать профиль если таковой уже существует
вывод примера настройки аутентификации	
--help-network-install	Пример настройки сетевой аутентификации с PKI
--help-network-otp-install	Пример настройки сетевой аутентификации с OTP

Опция	Описание
--help-license	Пример ввода лицензионного ключа
--help-network-pki-with-otp-install	Пример настройки сетевой аутентификации с PKI и дополнительной OTP аутентификацией
--help-local-pki-install	Пример настройки локальной аутентификации с PKI
опции для настройки сетевой двухфакторной аутентификации с использованием развёрнутой инфраструктуры PKI	
--missing-deps	Список зависимостей для настройки сетевой аутентификации
--network-install	Настройка сетевой двухфакторной аутентификации без графического интерфейса
--network-otp-install	Настройка OTP аутентификации без графического интерфейса
--additional-otp	Настройка дополнительной OTP аутентификации, для сетевой аутентификации с PKI
--c, --cert <файл>	Корневой сертификат сервера
--license-file <файл>	Файл лицензии
опции для настройки сетевой двухфакторной аутентификации без использования развёрнутой инфраструктуры PKI	
--network-no-pki-install	Настройка сетевой аутентификации без PKI без графического интерфейса
опции для настройки локальной двухфакторной аутентификации без использования развёрнутой инфраструктуры PKI	
--local-no-pki-install	Настройка локальной аутентификации без PKI без графического интерфейса
опции для настройки локальной двухфакторной аутентификации с использованием развёрнутой инфраструктуры PKI	
--local-pki-install	Настройка локальной аутентификации с PKI без графического интерфейса
--local-user-name <user_name>	Имя локального пользователя
опции для настройки OTP аутентификации	
--network-otp-install	Настройка OTP аутентификации без графического интерфейса
опции для подключения к целевому компьютеру с использованием двухфакторной аутентификации через удалённый доступ	
--rdp-server <IP адрес>	IP-адрес целевого RDP-сервера
--rdp-port <порт>	RDP-порт (опционально, если не указан, то используется порт 3389)
--slot-id <ID>	Идентификатор слота электронного ключа JaCarta в шестнадцатеричном виде (HEX)
--profile-user <пользователь>	Имя пользователя целевого компьютера
--profile-host <хост>	Имя сервера подключения
--smartcard-rdp	Удалённый доступ по сертификату на электронном ключе JaCarta

Опция	Описание
	Если данный параметр присутствует, то для аутентификации будет использован сертификат пользователя, находящийся на электронном ключе JaCarta
настройка темы входа и действий при извлечении электронного ключа	
--jc-greeter <on/off>	Включить/Выключить тему входа SecurLogon
--jc-greeter-pin-only <on/off>	Включить/Выключить настройку 'Вход только по PIN-коду'
--jc-greeter-eject-action <action>	Действия при извлечении электронного ключа JaCarta Доступные действия: 0 - Бездействие, 1 – Блокировать сессию пользователя, 2 - Выключить компьютер
--otp-pass-if-user-not-found <true/false>	Продолжать авторизацию, если пользователь не найден на сервере JAS
--otp-pass-if-tokens-not-found <true/false>	Продолжать авторизацию, если для пользователя не найдены токены на сервере JAS
опции для вывода параметров внешней системы	
--otp-server <ip_address/host_name>	Адрес JAS-сервера
--otp-port <port>	Порт JAS-сервера
--otp-protocol <HTTP/HTTPS>	Протокол подключения
--otp-systemId <systemId>	Строковый идентификатор внешней системы
--otp-path-to-api-endpoint <pathToApiEndpoint>	Путь до api endpoint
опции для вывода идентификатора сертификата пользователя	
--local-cert-id <cert_id>	Идентификатор сертификата, который будет привязан к пользователю

6.2 Запуск программы в консоли без запуска графической оболочки ОС

- Для запуска программы в консольном режиме, выполните команду:

```
sudo QT_QPA_PLATFORM=offscreen jcsecurlogon -h
```

Основные опции, которые можно использовать при запуске программы SecurLogon из консоли приведены в Таблица 7.

6.3 Запуск программы в графическом интерфейсе

6.3.1 Запуск программы для ОС Astra Linux Special Edition 1.6 (Смоленск) и Astra Linux Common Edition 2.12 (Орёл)

Для запуска программы выполните следующие действия в соответствии с Рисунок 5:

- откройте главное меню, щелкнув левой кнопкой мыши пиктограмму  ;
- выберете строку <Утилиты>;
- в открывшемся меню выберете <SecurLogon>;

- запустите приложение, щелкнув левой кнопкой мыши.

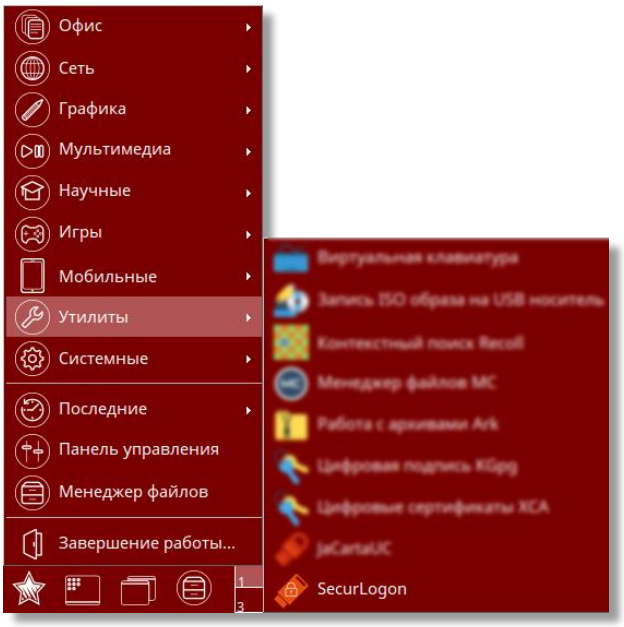

Рисунок 5 – Запуск программы в графическом интерфейсе ОС Astra Linux

6.3.2 Запуск программы для ОС Альт 8 СП, Альт 9 и Альт 10

Для запуска программы выполните следующие действия в соответствии с Рисунок 6:

- откройте главное меню, щелкнув левой кнопкой мыши пиктограмму ;
- выберете строку <Стандартные>;
- в открывшемся меню выберете <SecurLogon>;
- запустите приложение, щелкнув левой кнопкой мыши.

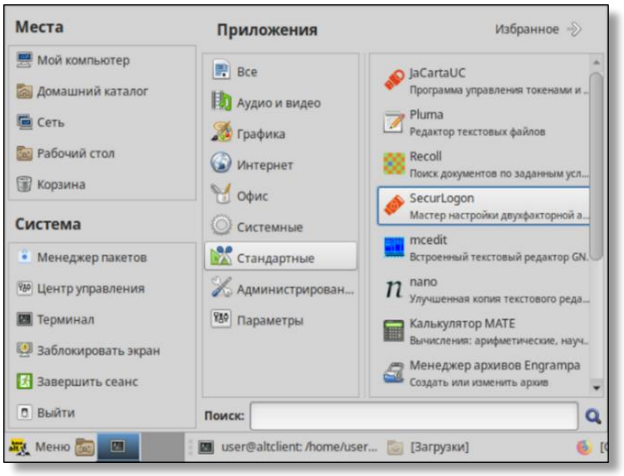

Рисунок 6 – Запуск программы в графическом интерфейсе ОС Альт 8 СП, Альт 9 и Альт 10

6.3.3 Запуск программы для ОС РЕД ОС 7.2 и РЕД ОС 7.3

Для запуска программы выполните следующие действия в соответствии с Рисунок 7:

- откройте главное меню, щелкнув левой кнопкой мыши пиктограмму ;
- выберете строку <Стандартные>;
- в открывшемся меню выберете <SecurLogon>;

- запустите приложение, щелкнув левой кнопкой мыши.

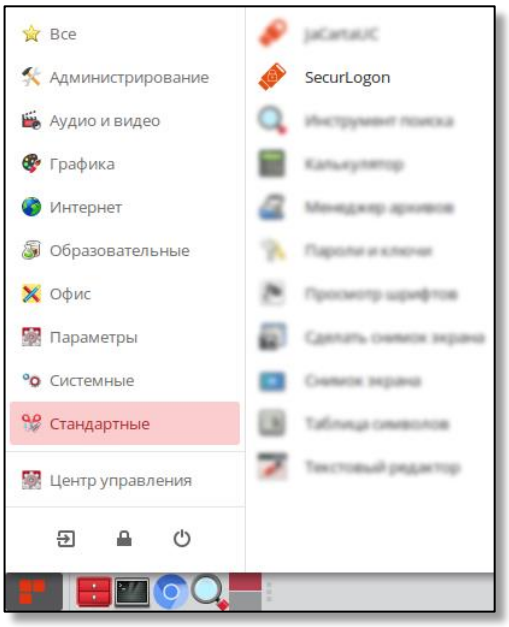

Рисунок 7 – Запуск программы в графическом интерфейсе ОС РЕД ОС 7.2 и РЕД ОС 7.3

7. Настройка программы

7.1 Аутентификация пользователя в программе

После запуска программы в графическом интерфейсе в появившемся диалоговом окне (см. Рисунок 8) требуется ввести пароль учетной записи администратора безопасности и нажать кнопку <Аутентификация> для продолжения запуска программы.

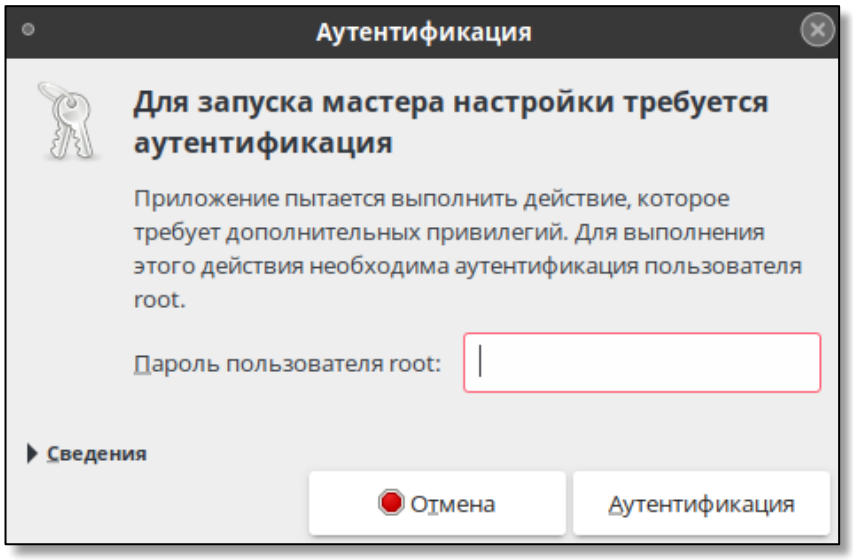

Рисунок 8 – Окно аутентификации пользователя в программе

7.2 Приветственная форма программы

После аутентификации пользователя открывается приветственная форма (см. Рисунок 9, Рисунок 10). Экранная форма содержит краткую справку о назначении программы, возможность настройки интерфейса перед началом работы посредством кнопок:

-  - нажатием на кнопку осуществляется переключение языка интерфейса (русский/английский соответственно);

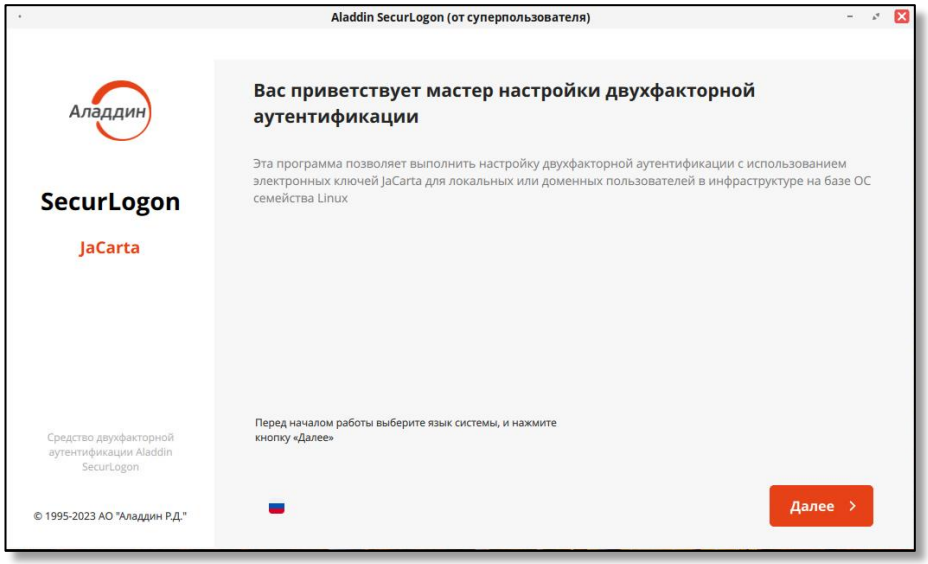

Рисунок 9 – Первичное приветственное окно

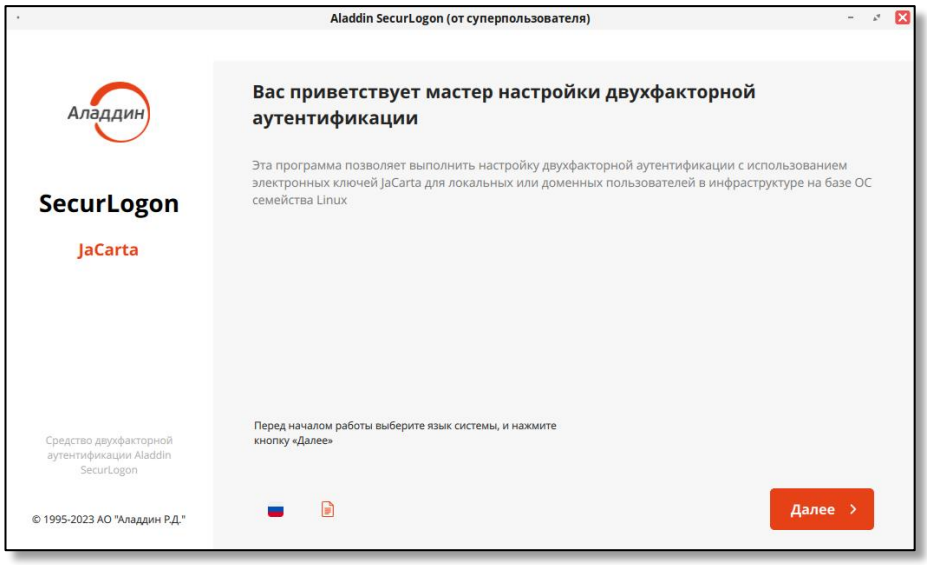

Рисунок 10 – Приветственное окно после первичного запуска (выбора способа активации)

-  - нажатие на кнопку выводит окно (см. Рисунок 11) для просмотра информации о всех ранее вводимых ключах активации (действительных или с истекшим сроком действия) и возможностью загрузки новой лицензии. По нажатию на кнопку <Новая лицензия> будет открыто окно активации программы (см. Рисунок 13).

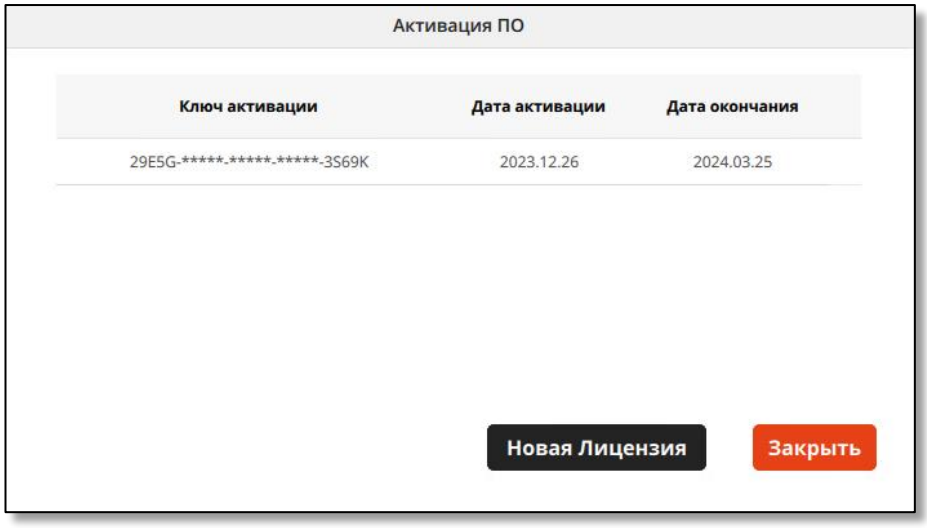

Рисунок 11 – Окно «Активация ПО»

7.3 Лицензионное соглашение (первичный запуск)

В диалоговом окне (см. Рисунок 12) внимательно прочитайте лицензионное соглашение, прежде чем открыть пакет с программным обеспечением и/или использовать его содержимое.

Необходимо полностью прочитать лицензионное соглашение, прокрутив вниз весь текст соглашения при помощи колеса прокрутки мыши.

Для продолжения работы программы необходимо принять условия соглашения, поставив галочку в поле <Я прочитал лицензионное соглашение и принимаю его> и нажать ставшую активной кнопку <Далее>.

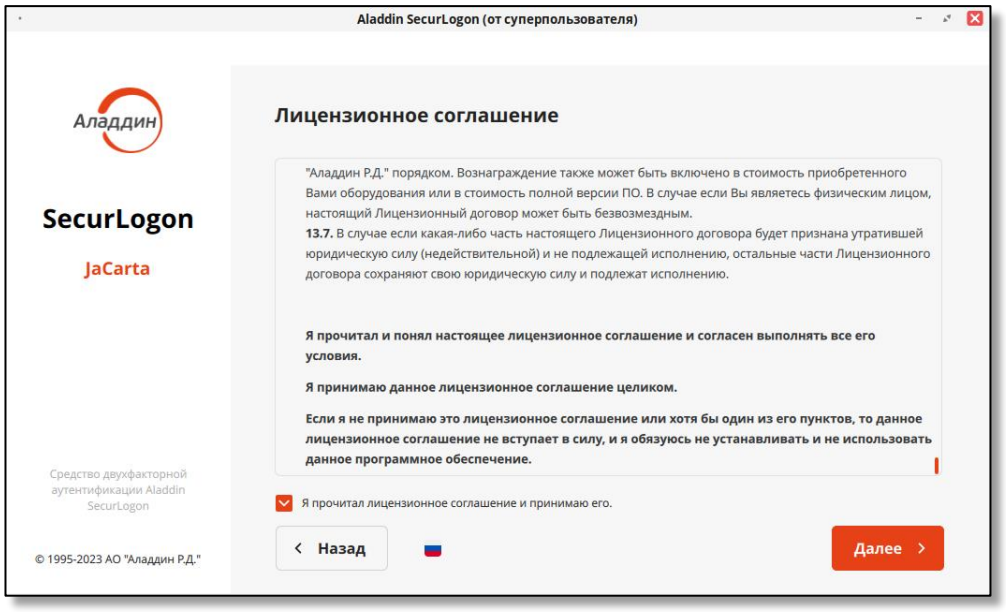

Рисунок 12 – Окно лицензионного соглашения при первичном запуске программы

7.4 Активация программы (первичный запуск)

После принятия лицензионного соглашения при первом запуске необходимо активировать ПО SecurLogon ключом активации или воспользоваться тестовым периодом (см. Рисунок 13).

- Активация возможна тремя способами:
  - путем ввода ключа активации в поле <По ключу активации>;
  - путем выбора файла с ключом активации формата .lic;
  - путём активации тестового периода без предоставления лицензии в течение 90 дней. Если у вас нет данной кнопки, значит ранее вы уже использовали пробный период и требуется ввести ключ активации или загрузить файл с ключом активации для продолжения использования программы.

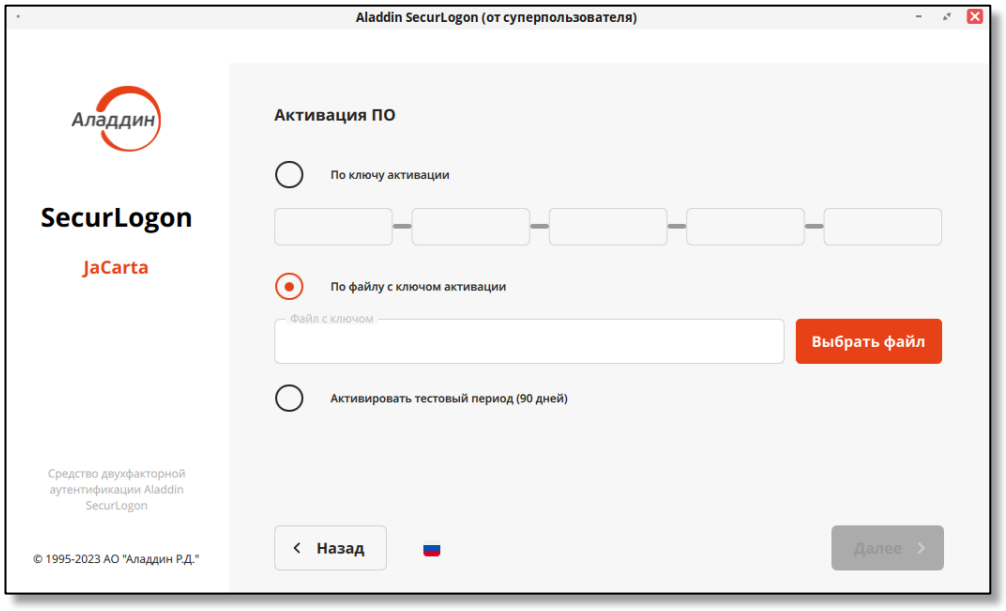

Рисунок 13 – Окно активации программы

- После ввода ключа активации, выбора файла, содержащего ключ активации, или активации пробного периода нажать ставшей активной кнопку <Далее>.
- Если появилось окно успешной проверки ключа активации (см. Рисунок 14), то ваш ключ верен.

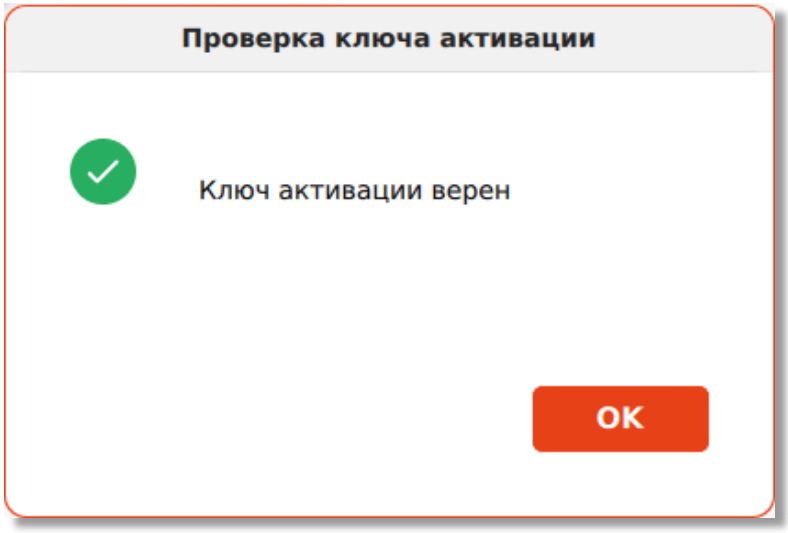

Рисунок 14 – Окно «Успешная проверка ключа активации»

8. Работа с программой

После запуска и безопасной настройки программного средства производится настройка двухфакторной аутентификации.

Необходимо выбрать способ аутентификации пользователя для предоставления доступа к информационным ресурсам (см. Рисунок 15).

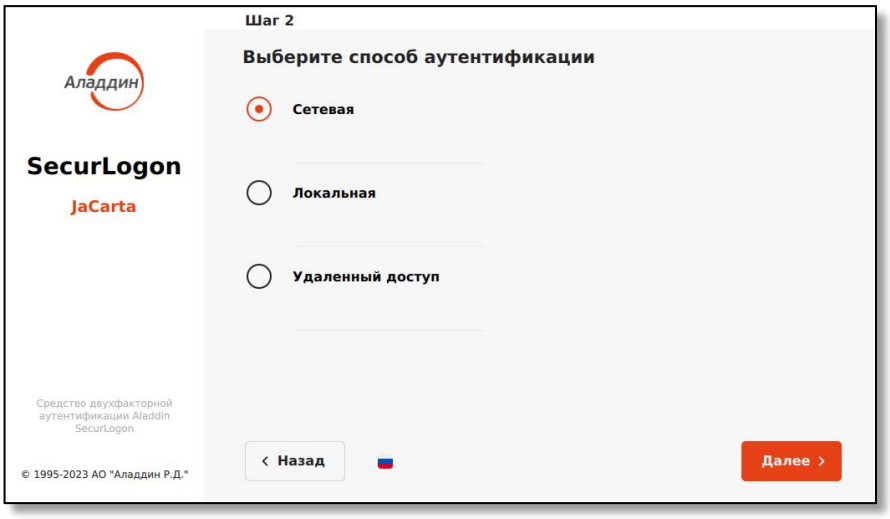

Рисунок 15 – Окно настройки аутентификации. Шаг 1

Далее определяется вид аутентификации (простая, строгая, усиленная) путём настройки метода аутентификации.

8.1 Настройка локальной аутентификации

Если на первом шаге настройки аутентификации (см. Рисунок 15) выбран способ локальной аутентификации, то осуществляется переход на второй шаг (см. Рисунок 16).

При первичной настройке доступен для выбора только пункт <Настроить двухфакторную аутентификацию при входе в систему>. Для перехода на следующий шаг нажмите кнопку <Далее>.

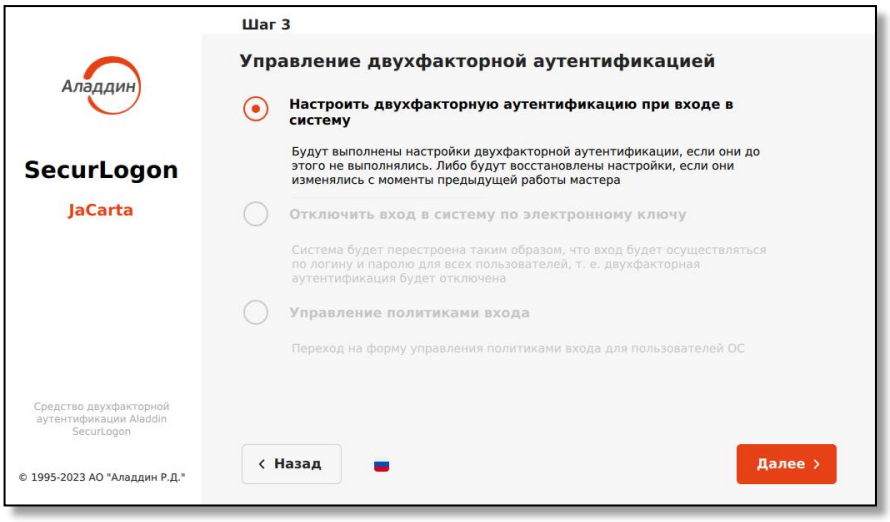

Рисунок 16 - Окно настройки локальной аутентификации. Шаг 2

8.1.1 Строгая аутентификация

На данном шаге к настраиваемому ПК должен быть подсоединен электронный ключ. В памяти электронного ключа может быть установлено одно или несколько приложений.

- Далее переходим к третьем шагу в окне настройки локальной аутентификации (см. Рисунок 17). На шаге 3 (см. Рисунок 17) выбираем способ входа в систему <С использованием PKI>. Для перехода к следующему шагу нажмите кнопку <Далее>.

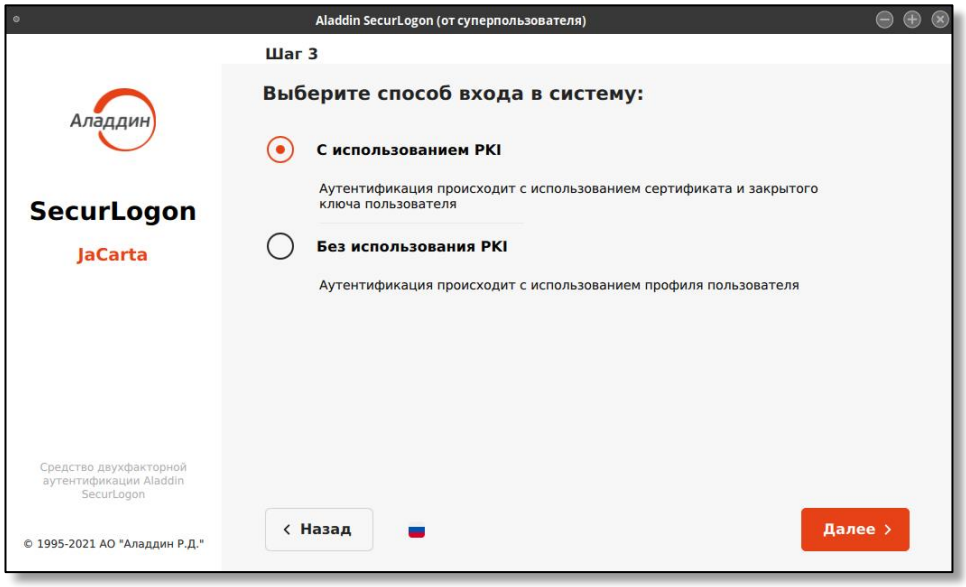

Рисунок 17 - Окно настройки локальной аутентификации. Шаг 3

8.1.1.1 Выбор электронного ключа

- В поле диалогового окна шага 4 (см. Рисунок 18) будут показаны все записанные приложения на подключенном электронном ключе.

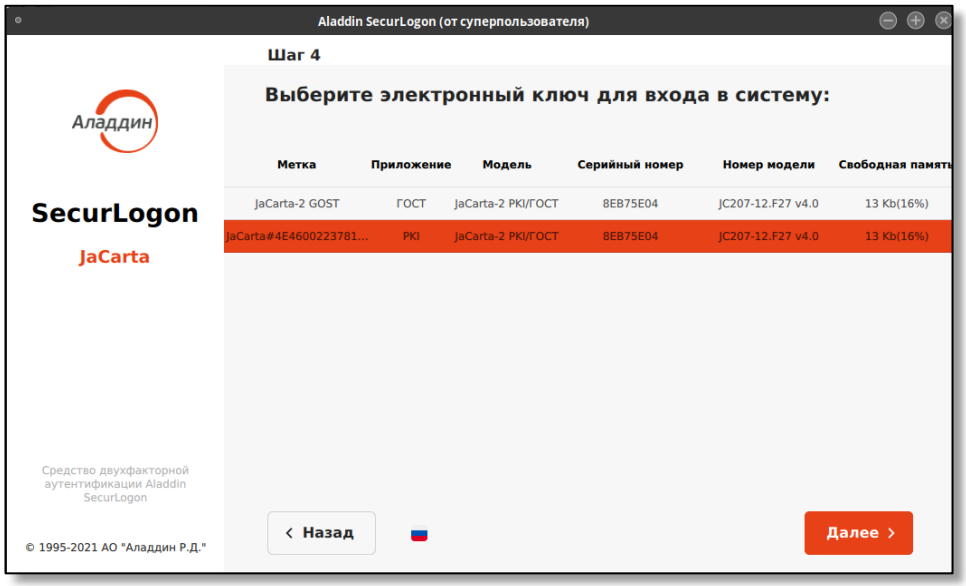

Рисунок 18 - Окно настройки локальной аутентификации с использованием PKI. Шаг 4

В столбцах указана следующая информация для каждого приложения электронного ключа:

- в столбце «метка приложения» указано название программного ключа (имя токена);
- в столбце «приложение» указано название приложения, установленного в память электронного ключа, определяющего функциональность модели электронного ключа;
- в столбце «модель» указана модель электронного ключа;
- в столбце «серийный номер» указан 8-значный серийный номер электронного ключа;
- в столбце «номер модели» указана модель электронного ключа;

– в столбце «свободная память» указано свободное место на электронном ключе в Кбайтах и % от общего объема электронного ключа.

- Выберите нужное приложение и нажмите кнопку <Далее>.

8.1.1.2 Настройка строгой локальной аутентификации (с PKI)

- В поле диалогового окна шага 5 (см. Рисунок 19) отображаются все имеющиеся сертификаты для выбранного на предыдущем шаге приложения.

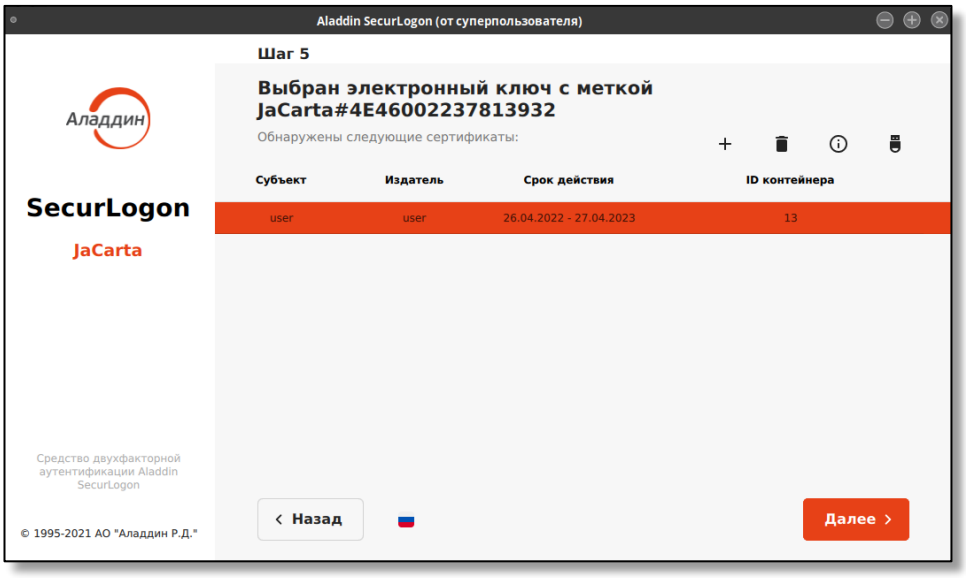

Рисунок 19 - Окно настройки локальной аутентификации с использованием PKI. Шаг 5

В столбцах экранной формы для каждого сертификата отображена следующая информация:

– имя субъекта;

– издатель;

– срок действия сертификата;

– ID контейнера.

На текущей экранной форме расположена панель управления сертификатами (см. Рисунок 20).

Рисунок 20 – Панель управления сертификатами

На данной панели представлены следующие возможности:

 - создание нового сертификата;

 - просмотр данных выбранного сертификата;

 - удаление выбранного сертификата;

 - настройка действия при извлечении электронного ключа.

При первоначальном выборе любого действия (щелчку на кнопку вышеописанной возможности) необходимо аутентифицировать присоединённый электронный ключ – в открывшемся окне введите PIN-код пользователя электронного ключа (см. Рисунок 21). Количество попыток ввода PIN-кода пользователя определяется настройками электронного ключа.

После верно введённого PIN-кода осуществляется переход в окно выбранной возможности.

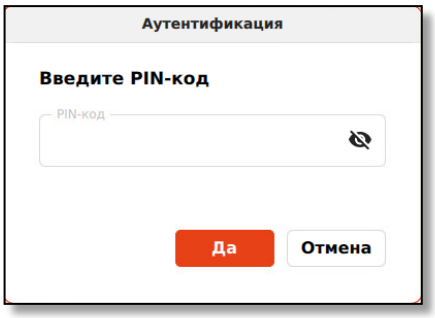

Рисунок 21 – Окно аутентификации для ввода ПИН-кода электронного ключа

8.1.1.2.1 Создание нового сертификата

Для создания нового сертификата пользователя в панели управления профилями нажмите на кнопку [+], после чего появится окно создания нового сертификата (см. Рисунок 22).

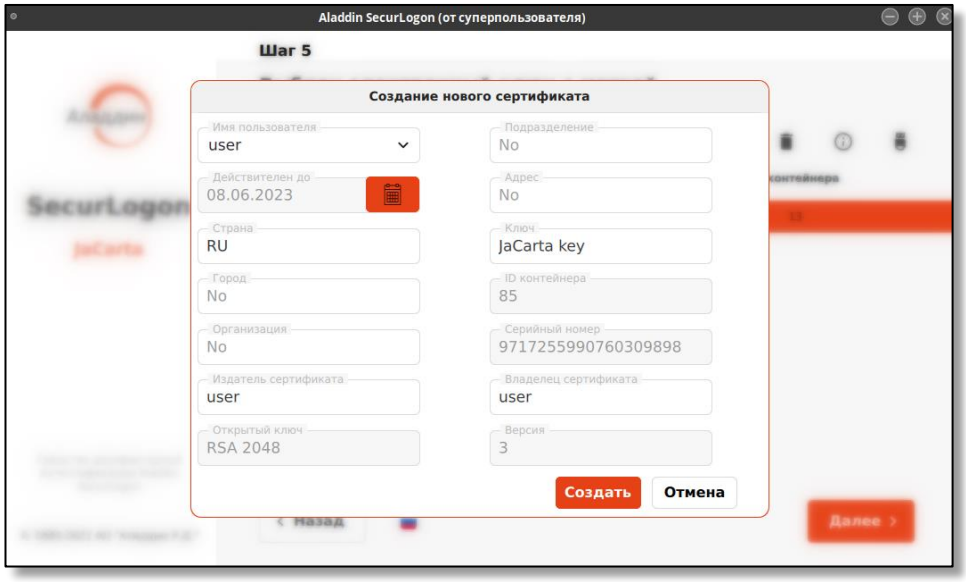

Рисунок 22 – Окно создания нового сертификата

Список настраиваемых полей окна создания сертификата приведен в Таблица 8.

Таблица 8 – Список заполняемых полей нового сертификата

Тип вводимой информации (поля ввода)	Описание вводимого значения
Имя пользователя	Субъект, кому будет выдан сертификат
Действителен до	Срок окончания действия сертификата
Страна	Страна
Город	Населённый пункт
Организация	Наименование организации
Издатель сертификата	Субъект, который издал сертификат
Открытый ключ	Алгоритм формирования открытого ключа
Подразделение	Наименование подразделения организации
Адрес	Адрес организации
Ключ	Используемый электронный ключ JaCarta
ID контейнера	Идентификатор ключевого контейнера

Тип вводимой информации (поля ввода)	Описание вводимого значения
Серийный номер	Серийный номер сертификата является целым числом, устанавливаемым для каждого сертификата. Значение должно быть уникальным для каждого сертификата
Владелец сертификата	Субъект, являющийся обладателем закрытого ключа, соответствующего открытому ключу в сертификате
Версия	Версия сертификата. Используемое значение – «3»

После заполнения всех полей, нажмите кнопку <Создать>, при успешном создании сертификата вы увидите уведомление об успехе операции (см. Рисунок 23).

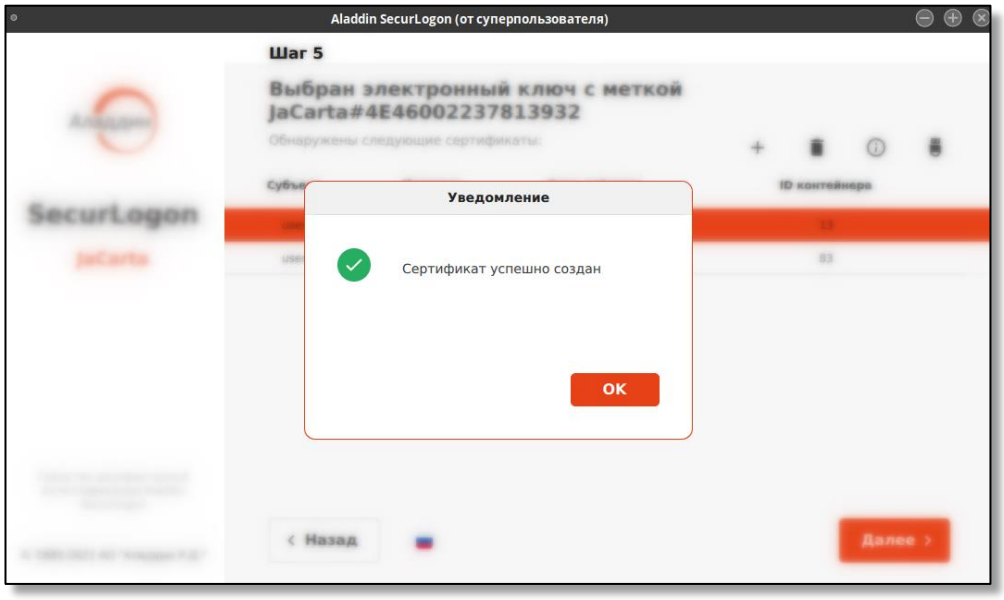

Рисунок 23 – Окно уведомления об успешном создании сертификата

8.1.1.2.2 Просмотр данных сертификата

Для просмотра информации о сертификате пользователя на панели управления сертификатами (см. Рисунок 20) нажмите кнопку [ⓘ], после чего появится окно <О сертификате> (см. Рисунок 24).

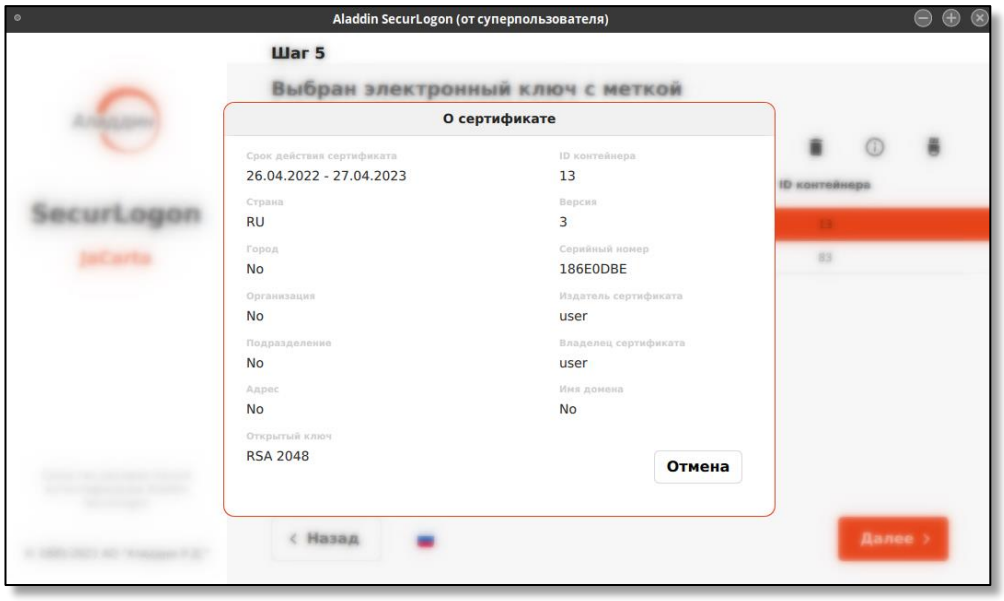

Рисунок 24 – Окно просмотра сведений о сертификате

Нажмите кнопку <Отмена>, для закрытия окна.

8.1.1.2.3 Удаление сертификата

Для удаления сертификата с электронного ключа на панели управления сертификатами (см. Рисунок 20) нажмите на кнопку 🗑, после чего, вы увидите окно подтверждения удаления сертификата (см. Рисунок 25).

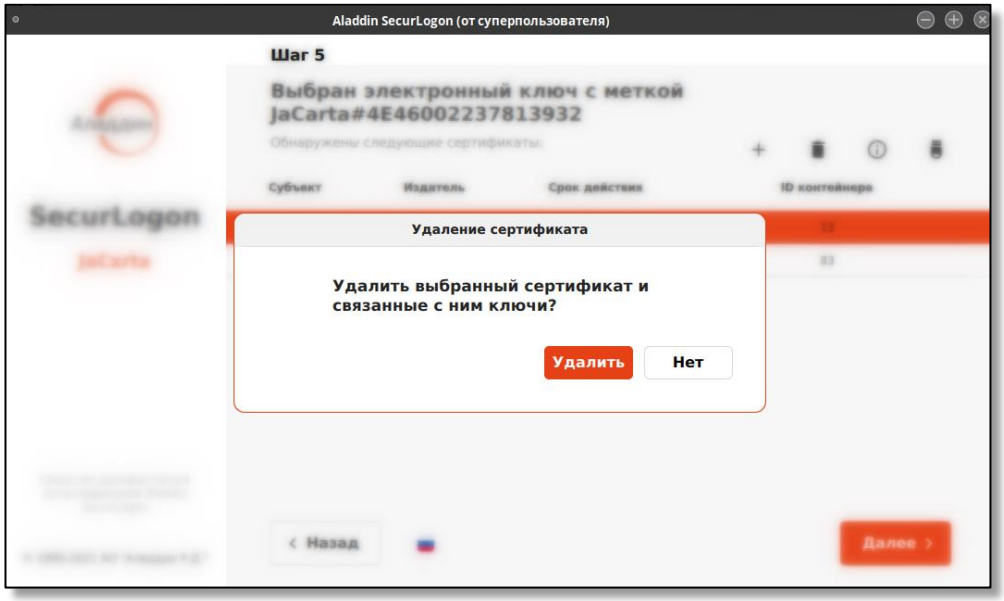

Рисунок 25 – Окно подтверждения удаления сертификата

Подтвердите удаление сертификата нажатием на кнопку <Удалить>, при успешном удалении сертификата вы увидите уведомление об успехе операции (см. Рисунок 25).

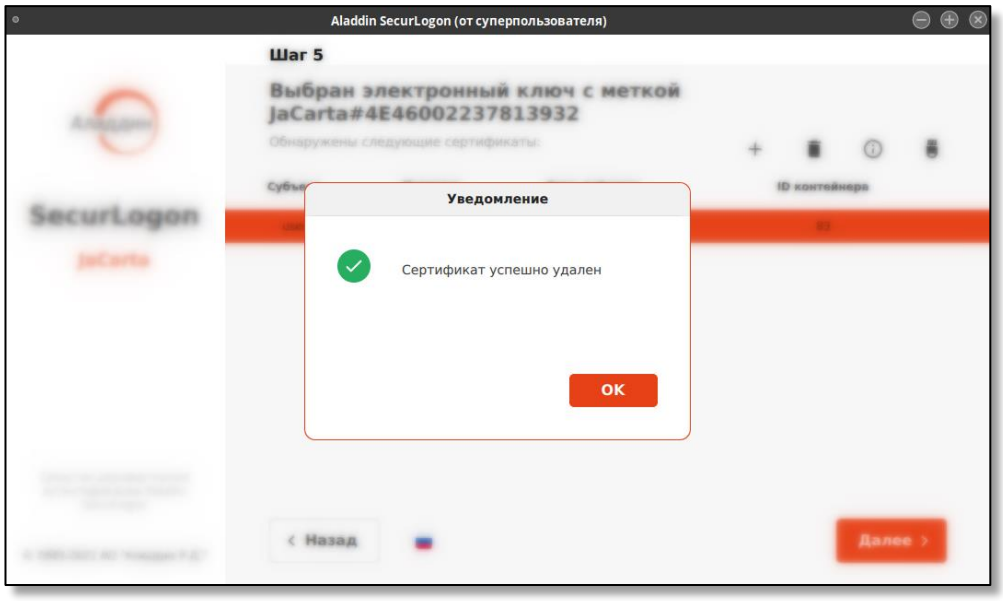

Рисунок 26 – Окно уведомления об успешном удалении сертификата

8.1.1.2.4 Действия при извлечении электронного ключа

Для настройки действия при извлечении электронного ключа из разъёма нажмите кнопку  на панели управления сертификатами (см. Рисунок 20) и выберете нужное действие:

- бездействие – при извлечении электронного ключа ничего не произойдет, текущий сеанс продолжается в штатном режиме;
- блокировать сессию пользователя – при извлечении электронного ключа сессия пользователя будет заблокирована;
- выключить компьютер.

Если у пользователя настроена политика входа «Только по паролю», то двухфакторная аутентификация в этом случае не используется. Поэтому, вне зависимости от настроенного действия, при извлечении электронного ключа ничего не произойдет.

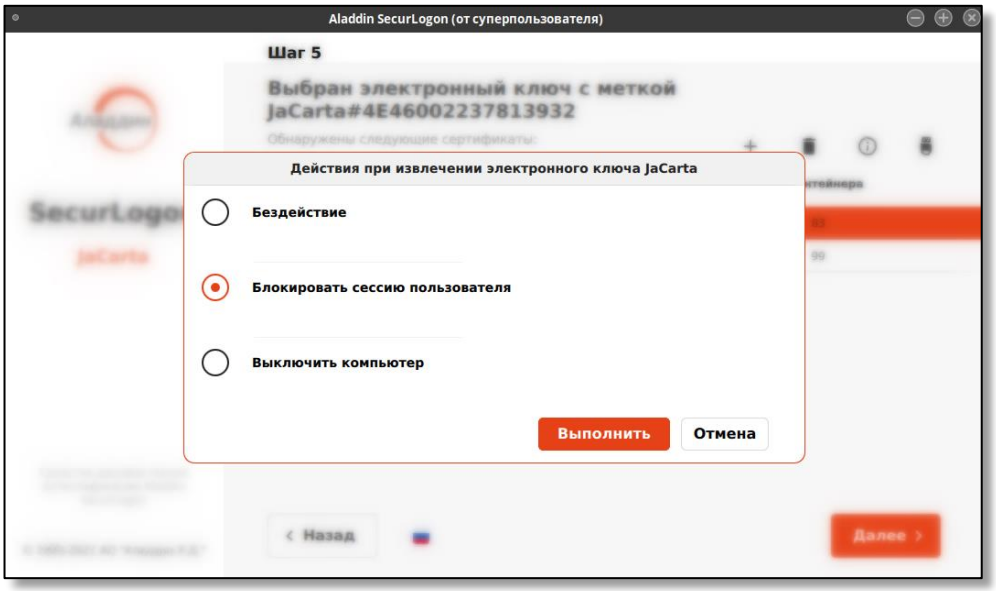

Рисунок 27 – Окно выбора действия при извлечении электронного ключа

Подтвердите действие, нажав кнопку <Выполнить>, при успешном сохранении выбора действия при извлечении электронного ключа вы увидите уведомление об успехе операции (см. Рисунок 28).

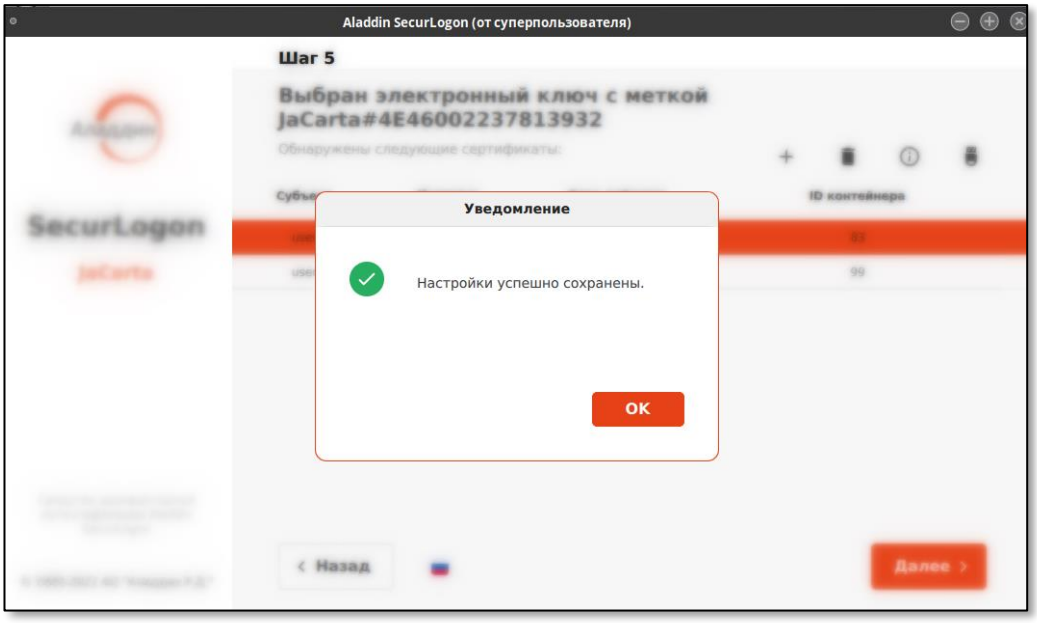

Рисунок 28 – Окно уведомления об успешном сохранении выбора действия при извлечении электронного ключа

Также настройку действия при извлечении электронного ключа можно выполнить на финальном этапе настройки двухфакторной аутентификации.

8.1.1.3 Привязка сертификата к учетной записи пользователя

После окончания работы с сертификатами нажмите на экранной форме шага 5 (см. Рисунок 19) кнопку <Далее>. Осуществляется переход на следующий шаг настройки локальной двухфакторной аутентификации (см. Рисунок 29). В данном окне будут отображены все учетные записи текущей операционной системы рабочего места, на котором происходит настройка аутентификации.

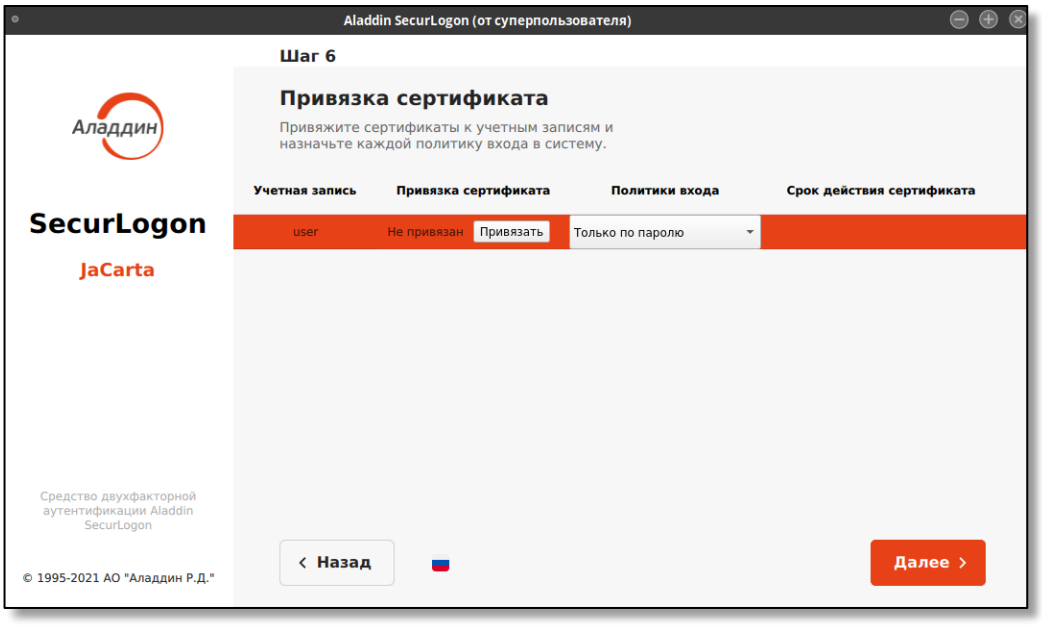

Рисунок 29 - Окно настройки локальной аутентификации с использованием PKI. Шаг 6

На данном шаге осуществляется выбор пользователя и для него доступны следующие действия:

- привязка сертификата. По нажатию на кнопку <Привязать> на экранной форме шага 6 (см. Рисунок 29) в случае, если сертификат ранее не был привязан, всплывает окно управления сертификатами пользователя (см. Рисунок 30).

В данном окне нужно выбрать сертификат, который будет привязан к выбранному пользователю, и произвести настройку политики входа пользователя.

Возможно задание следующих политик входа:

– По паролю или PIN-коду. То есть, если электронный ключ подсоединен к ПК, то для аутентификации пользователя используется политика «Только по PIN-коду», если электронный ключ не подсоединен к ПК, то используется политика входа в ОС «Только по паролю».

– Только по паролю – для входа в необходимо ввести имя и пароль учетной записи ОС, двухфакторная аутентификация не используется.

– Только по PIN-коду – вход возможен только при подключенном электронном ключе, требуется выбрать пользователя и ввести PIN-код электронного ключа. PIN-коды по умолчанию при поставке приведены в таблице 3, раздела 3.2 «Единый Клиент JaCarta. Руководства администратора «Аладдин Р.Д.» RU.АЛДЕ.03.01.013-01 32 01-2 [1]. Настройка PIN-кода электронного ключа осуществляется при помощи ПО «Единый Клиент JaCarta» и подробно описано в разделе 10 «Единый Клиент JaCarta. Руководства администратора «Аладдин Р.Д.» RU.АЛДЕ.03.01.013-01 32 01-2 [1].

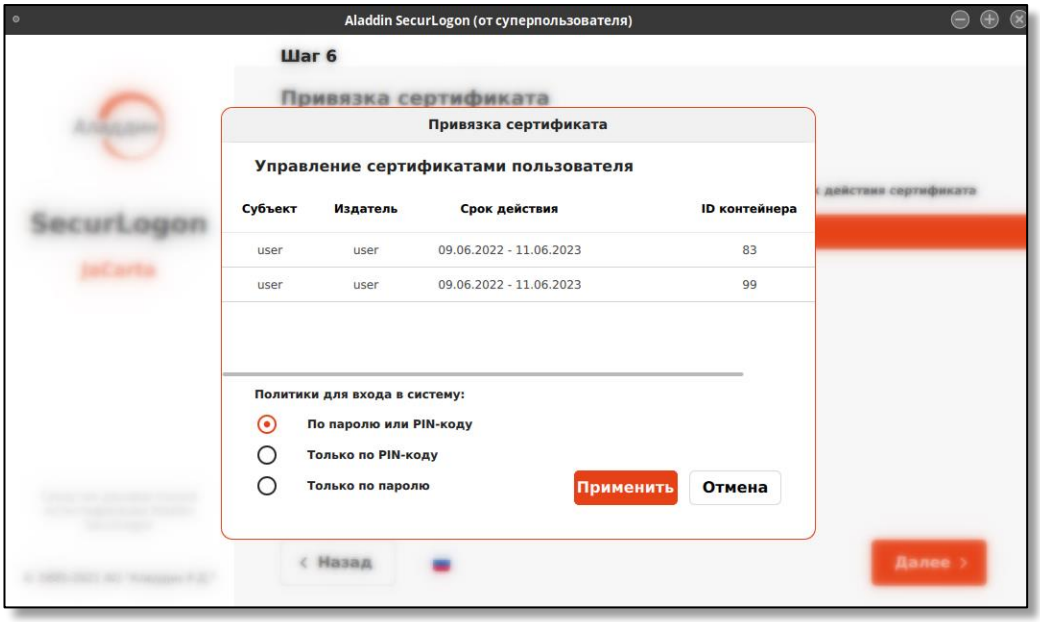

Рисунок 30 – Окно привязки сертификата

По завершению действий доступны:

– кнопка <Применить>, по нажатию на которую все совершенные изменения сохранятся – выбранный сертификат и политика входа будут применены к выбранному ранее пользователю, окно «Привязка сертификата» будет закрыто;

– кнопка <Отмена>, по нажатию на которую все не сохраненные изменения будут сброшены, окно «Привязка сертификата» будет закрыто.

- отвязка сертификата. В случае, если ранее сертификат был привязан к учетной записи пользователя доступно действие по нажатию кнопки на экранной форме шага 6 (см. Рисунок 29) <Отвязать>. По нажатию кнопки <Отвязать> открывается окно подтверждения действия (см. Рисунок 31), где можно подтвердить намерение, нажав кнопку <Да>, или опровергнуть, нажав кнопку <Нет>. После подтверждения намерения окно подтверждения будет закрыто, сертификат будет отвязан от учетной записи пользователя и политика входа будет установлена на «Только по паролю».

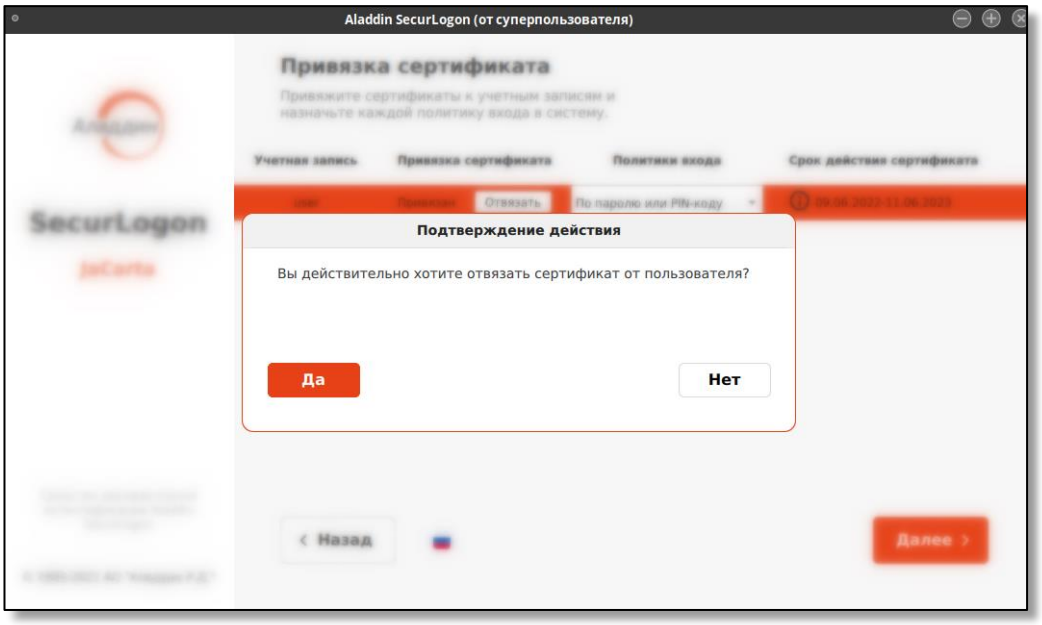

Рисунок 31 – Окно подтверждения отвязки сертификата от пользователя

- изменения политики входа. По нажатию на значение поля в столбце «Политика входа» всплывает меню (см. Рисунок 32). При выборе пункта меню открывается окно привязки сертификата (см. Рисунок 30).

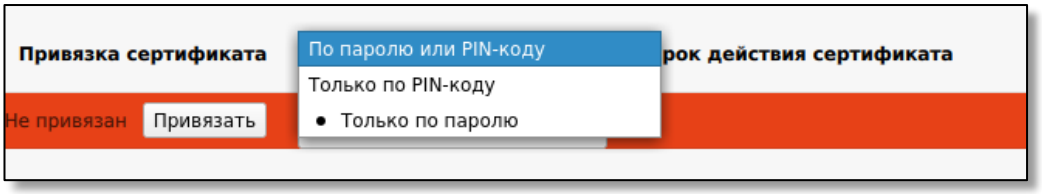

Рисунок 32 – Меню изменения политики входа при локальной аутентификации с использованием PKI

- просмотр сведений о сертификате, по нажатию на кнопку [ⓘ], в случае, если ранее был привязан сертификат к учетной записи пользователя (см. Рисунок 33), будет открыто окно со сведениями о сертификате (см. Рисунок 24).

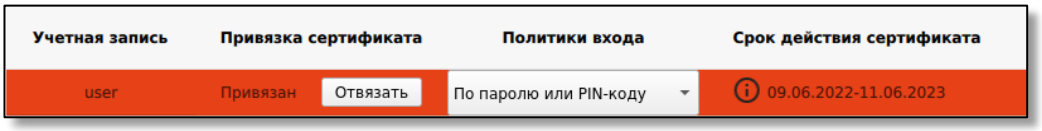

Рисунок 33 – Выбор учетной записи пользователя с привязанным сертификатом

8.1.1.4 Завершение настройки аутентификации

После окончания работы с учетными записями пользователей нажмите на экранной форме шага 6 (см. Рисунок 29) кнопку <Далее>. Осуществляется переход на следующий шаг настройки локальной двухфакторной аутентификации с PKI (см. Рисунок 34).

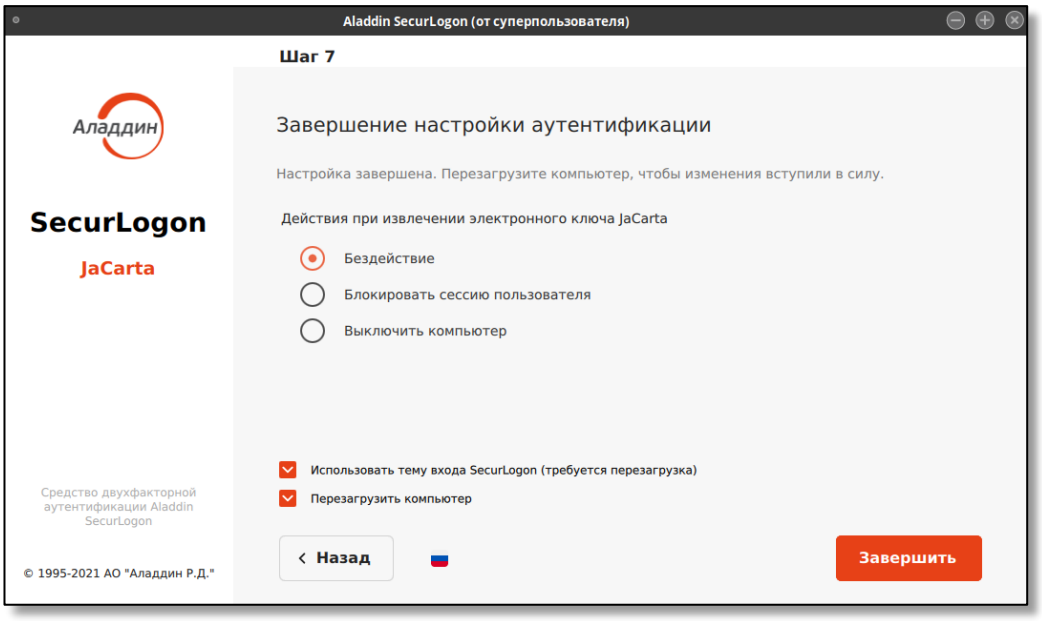

Рисунок 34 - Окно настройки локальной аутентификации с использованием PKI. Шаг 7

На данном шаге возможно настроить действие при извлечении электронного ключа из разъема ПК, выбрав нужное значение на экранной форме шага 7.

Также можно применить тему SecurLogon (см. Приложение А) для входа пользователя в систему перед началом сеанса. Все изменения будут применены по нажатию на кнопку <Завершить> и перезагрузке компьютера.

8.1.2 Усиленная аутентификация

На данном шаге к настраиваемому ПК должен быть подсоединен электронный ключ.

На электронном ключе допускается наличие нескольких апплетов.

На шаге 3 (см. Рисунок 35) выбираем способ входа в систему <Без использования PKI>. Для перехода к следующему шагу нажмите кнопку <Далее>.

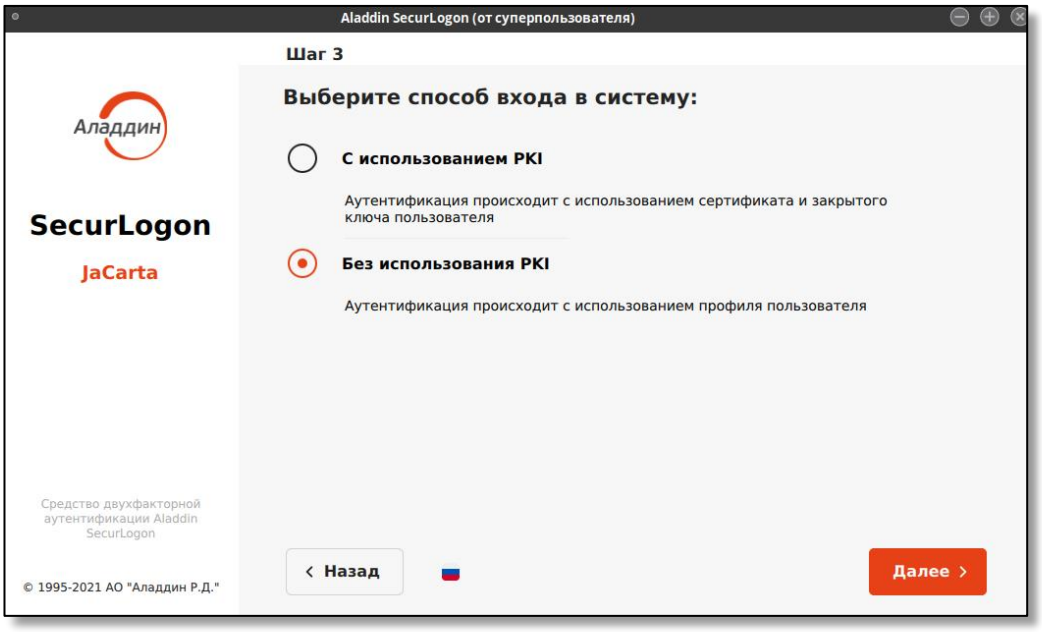

Рисунок 35 - Окно настройки локальной аутентификации. Шаг 3

8.1.2.1 Выбор электронного ключа

В поле диалогового окна шага 4 (см. Рисунок 36) показаны все записанные приложения на текущем электронном ключе, в столбцах указана следующая информация для каждого приложения:

- в столбце «метка приложения» указано название электронного ключа (имя токена);
- в столбце «приложение» указано название приложения, установленного в память электронного ключа, определяющее функциональность модели электронного ключа;
- в столбце «модель» указана модель электронного ключа;
- в столбце «серийный номер» указан 8-значный серийный номер электронного ключа;
- в столбце «номер модели» указана модель электронного ключа;
- в столбце «свободная память» указано свободное место на электронном ключе в Кбайтах и % от общего объема электронного ключа.

Выберите нужное приложение и нажмите кнопку <Далее>.

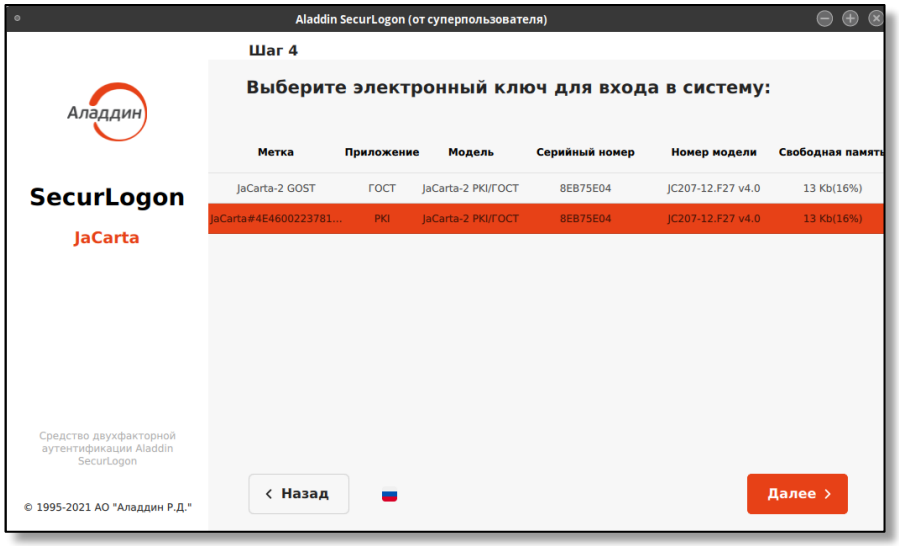

Рисунок 36 - Окно настройки локальной аутентификации без использования PKI. Шаг 4

8.1.2.2 Управление профилями пользователей

В поле диалогового окна шага 5 (см. Рисунок 37) отображаются все профили для выбранного на предыдущем шаге приложения электронного ключа.

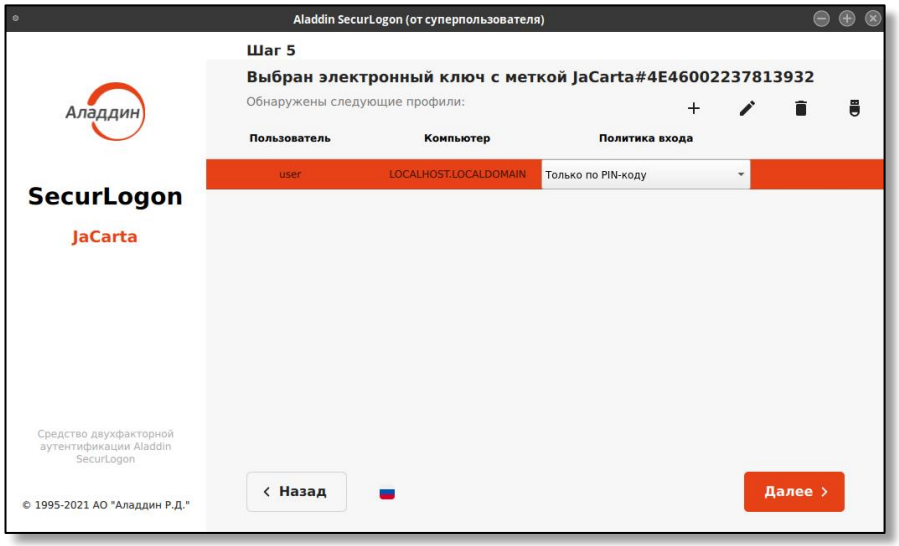

Рисунок 37 - Окно настройки локальной аутентификации без использования PKI. Шаг 5

В столбцах экранной формы для каждого сертификата отображена следующая информация:

- пользователь. В данном столбце отображены все профили пользователей, созданные на текущем электронном ключе;
- компьютер. В этом столбце отображены имена компьютеров, для работы на которых настроены соответствующие профили пользователей;
- политика входа. Определяется администратором только для профилей пользователей, учетные записи которых существуют на текущем рабочем месте, или настраивается локально на каждом компьютере с соответствующей учетной записью для каждого профиля.

На данном шаге 5 осуществляется выбор профиля пользователя и для него доступны следующие действия:

- изменения политики входа. По нажатию на значение поля в столбце «Политика входа» всплывает меню (см. Рисунок 38).

  Возможно задание следующих политик входа:

  - По паролю или PIN-коду. То есть, если электронный ключ подсоединен к ПК, то для аутентификации пользователя используется политика «Только по PIN-коду», если электронный ключ не подсоединен к ПК, то используется политика входа в ОС «Только по паролю».
  - Только по паролю – для входа в систему необходимо ввести имя и пароль учетной записи ОС, двухфакторная аутентификация не используется.
  - Только по PIN-коду – вход возможен только при подключенном электронном ключе, требуется выбрать пользователя и ввести PIN-код электронного ключа. PIN-коды по умолчанию при поставке приведены в таблице 3, раздела 3.2 RU.АЛДЕ.03.01.013-01 32 01-2 «Единый Клиент JaCarta. Руководства администратора «Аладдин Р.Д. « [1]. Настройка PIN-кода электронного ключа осуществляется при помощи ПО «Единый Клиент JaCarta» и подробно описано в разделе 10 RU.АЛДЕ.03.01.013-01 32 01-2 «Единый Клиент JaCarta. Руководства администратора «Аладдин Р.Д. « [1].

  После выбора нужного значения происходит автоматическая смена политики входа.

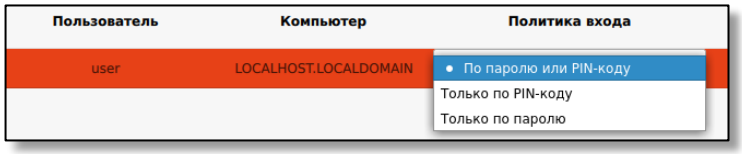

Рисунок 38 – Меню изменения политики входа при локальной аутентификации без PKI

- управление профилями пользователей посредством панели (см. Рисунок 39).

Рисунок 39 – Панель управления профилями

На данной панели представлены следующие возможности:

 - создание нового профиля;

 - редактирование данных выбранного профиля;

 - удаление выбранного профиля;

 - настройка действия при извлечении электронного ключа.

При первоначальном выборе любого действия (щелчку на кнопку вышеописанной возможности) необходимо аутентифицировать присоединённый электронный ключ – в открывшемся окне введите PIN-код пользователя электронного ключа (см. Рисунок 40). Количество попыток ввода PIN-кода пользователя определяется настройками электронного ключа.

После верно введённого PIN-кода осуществляется переход в окно выбранной возможности.

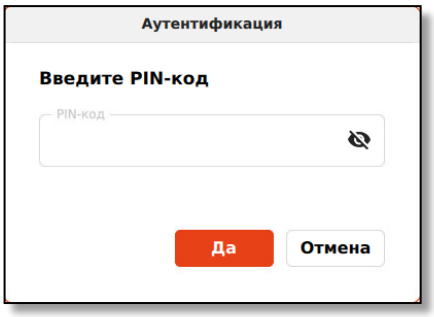

Рисунок 40 – Окно аутентификации для ввода ПИН-кода электронного ключа

8.1.2.2.1 Создание нового профиля

Для создания нового профиля пользователя в панели управления профилями нажмите на кнопку ⊞, после чего появится окно создания нового профиля (см. Рисунок 41).

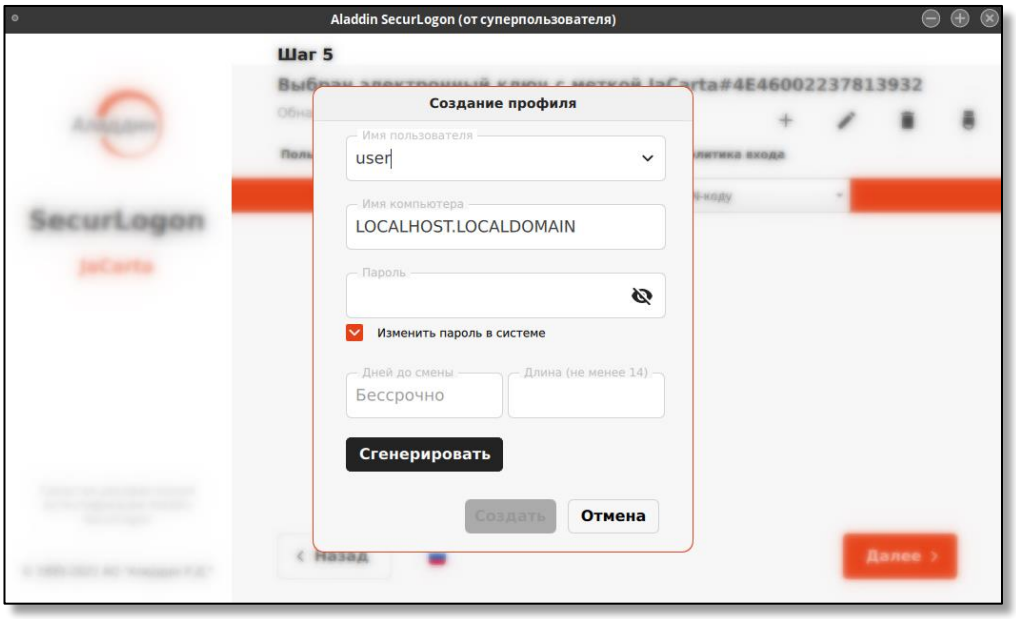

Рисунок 41 – Окно создания нового профиля

Заполните данные нового профиля, указав в соответствующих полях:

- имя пользователя – введите новое имя пользователя или выберите из списка. Имя пользователя должно совпадать с учетной записью пользователя на ОС рабочего места, на котором настраивается двухфакторная аутентификация;
- имя компьютера – введите имя компьютера, на котором будет использован текущий профиль;
- пароль – придумайте достаточно сложный пароль для текущего пользователя. Так же, вы можете автоматически сгенерировать пароль, указав в поле «Длина» – символьную длину пароля, не менее 14 символов и не более 63.

При вводе пароля в процессе создания профиля пользователя, соответствующего одной из учетных записей ОС текущего рабочего места, возможно назначить вводимый или генерируемый пароль для профиля пользователя одновременно и паролем для этой учетной записи пользователя в ОС, установив галочку «Изменить пароль в системе» (см. Рисунок 42), таким образом будет произведена замена пароля соответствующей учетной записи на текущем рабочем месте. В случае, если профиль пользователя создается для учетной записи другого рабочего места и совпадает с учетной записью ОС текущего рабочего места, то галочку «Изменить пароль в системе» нужно снять.

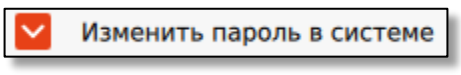

Рисунок 42 – Выбор функции «Изменение пароля в системе»

При вводе пароля при создании профиля пользователя для несуществующей учетной записи текущей ОС рабочего места администратора, галочка «Изменить пароль в системе» будет автоматически снята и недоступна (см. Рисунок 43). В этом случае пароль создаваемого профиля пользователя должен совпадать с паролем учетной записи пользователя рабочего места, для которого производится настройка аутентификации.

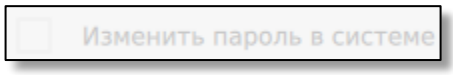

Рисунок 43 – Выбор функции «Изменение пароля в системе» недоступен

- дней до смены – введите количество дней до смены пароля. Данное поле может быть не заполнено, в таком случае заданный пароль будет постоянным. В случае, если задать в данном поле интервал для смены пароля, то каждые несколько дней (в зависимости от заданного интервала) будет автоматически сгенерирован новый пароль, длинной не менее указанного количества символов в соседнем поле «Длина (не менее 14) «. В данном случае аутентифицирующийся пользователь и уполномоченный пользователь не будут уведомлены о смене пароля, процедура будет выполняться в фоновом режиме. Пользователю будет доступна настроенная аутентификация по PIN-коду электронного ключа.

  После заполнения всех полей, нажмите ставшую активной кнопку <Создать>.

При создании профиля для локальной учётной записи пользователя на текущем рабочем месте на экран будет выведено окно подтверждения действий (см. Рисунок 44), для подтверждения действия нажмите кнопку <Да>.

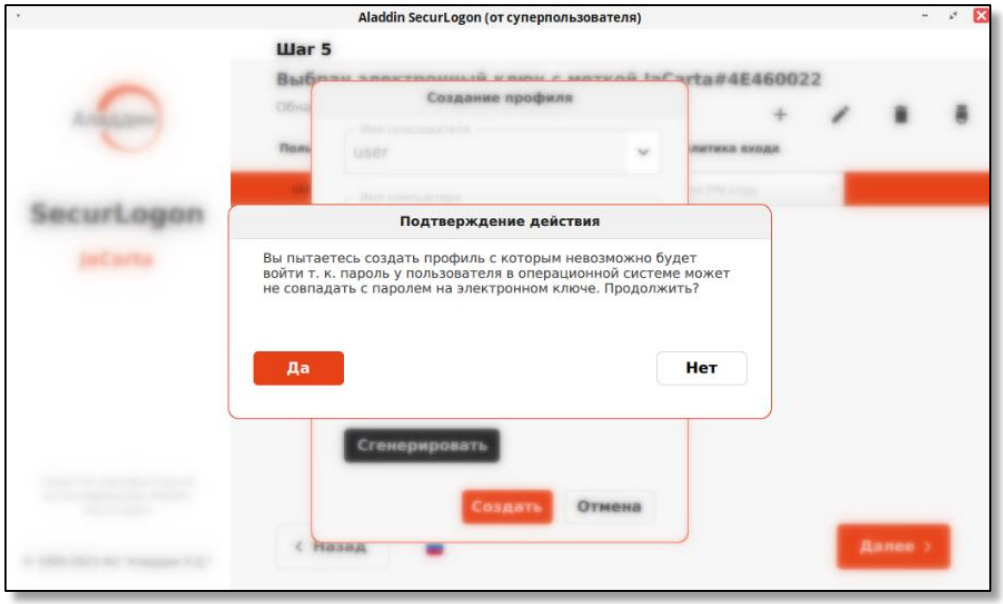

Рисунок 44 – Окно подтверждения действий при создании профиля

При создании профиля для локальной учётной записи пользователя стороннего рабочего места на экран будет выведено окно с уведомлением о том, что созданный профиль можно применить только на том ПК, имя которого вы указали при создании профиля (см. Рисунок 45), для подтверждения действия нажмите кнопку <Ок>.

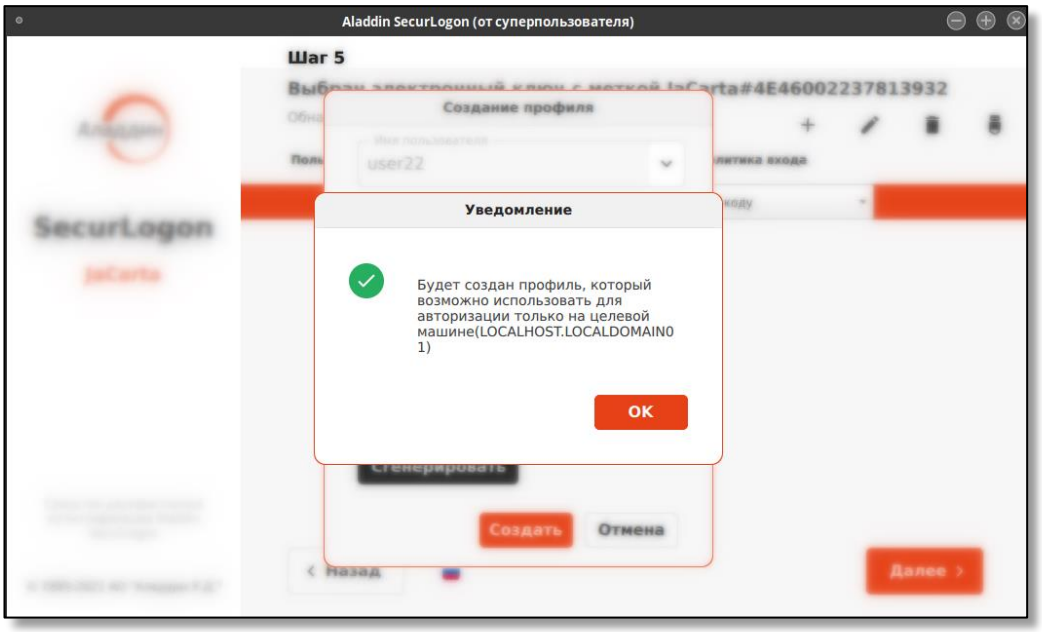

Рисунок 45 – Окно уведомления о создании профиля

При успешном создании профиля вы увидите уведомление об успехе операции (см. Рисунок 46).

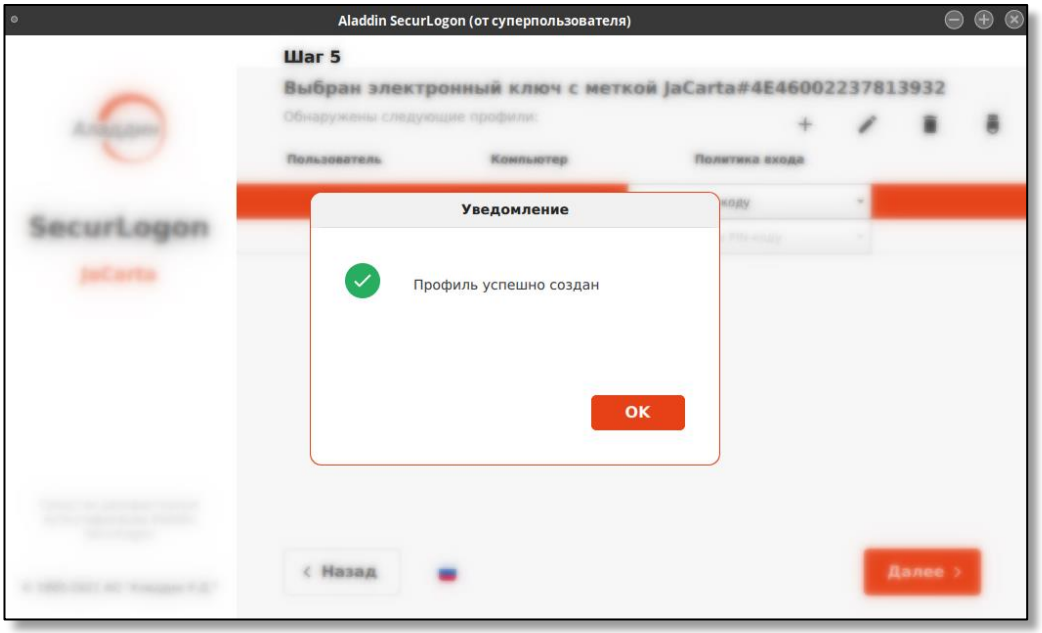

Рисунок 46 – Окно уведомления об успешном создании профиля

8.1.2.2.2 Редактирование выбранного профиля

Для редактирования выбранного профиля на экранной форме шага 5 (см. Рисунок 37) нажмите на кнопку  , при редактировании профиля доступны поля:

– пароль – задайте пароль для текущего профиля пользователя, в соответствии с (в соответствии с **Приложение Б. Правила формирования пароля**). Так же, вы можете автоматически сгенерировать пароль, указав в поле «Длина» – символьную длину пароля, не менее 14 символов и не более 63.

При вводе пароля в процессе создания профиля пользователя, соответствующего одной из учетных записей ОС текущего рабочего места, возможно назначить вводимый или генерируемый пароль для профиля пользователя одновременно и паролем для этой учетной записи пользователя в ОС, установив галочку «Изменить пароль в системе» (см. Рисунок 42), таким образом будет произведена замена пароля соответствующей учетной записи на текущем рабочем месте. В случае, если профиль пользователя создается для учетной записи другого рабочего места и совпадает с учетной записью ОС текущего рабочего места, то галочку «Изменить пароль в системе» нужно снять.

– дней до смены – введите количество дней до смены пароля. Данное поле может быть не заполнено, в таком случае заданный пароль будет постоянным. В случае, если задать в данном поле интервал для смены пароля, то каждые несколько дней (в зависимости от заданного интервала) будет автоматически сгенерирован новый пароль, длинной не менее указанного количества символов в соседнем поле «Длина (не менее 14) «. В данном случае аутентифицирующийся пользователь и уполномоченный пользователь не будут уведомлены о смене пароля, процедура будет выполняться в фоновом режиме. Пользователю будет доступна настроенная аутентификация по PIN-коду электронного ключа.

После того, как пароль будет введен или сгенерирован, кнопка <Сохранить> станет активной. Нажав кнопку <Сохранить>, профиль будет отредактирован.

Для выхода из режима редактирования профиля без сохранения изменений нажмите кнопку <Отмена>.

8.1.2.2.3 Удаление выбранного профиля

Для удаления выбранного профиля пользователя на экранной форме шага 5 (см. Рисунок 37) нажмите на кнопку  , после чего вы увидите:

– окно подтверждения удаления профиля (см. Рисунок 47), если при создании профиля пользователя пароль был задан вручную или удаляемый профиль пользователя находится на другом ПК. При нажатии кнопки <Удалить> вы подтверждаете действие и профиль пользователя будет удален. Нажав кнопку <Нет> вы отменяете удаление профиля пользователя.

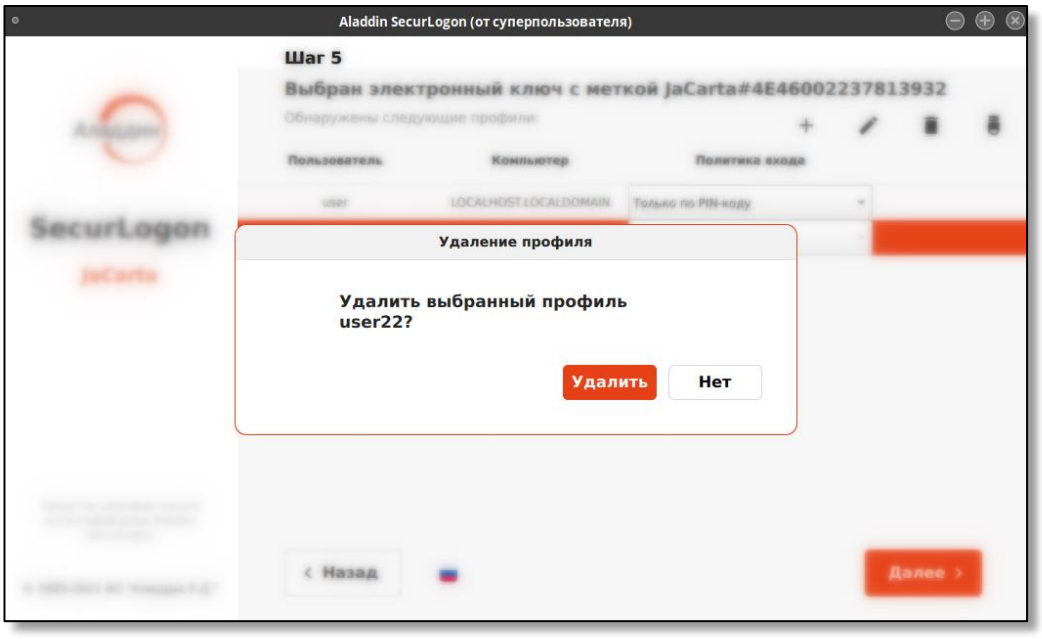

Рисунок 47 – Окно подтверждения удаления профиля пользователя при ручном вводе пароля

– вы увидите окно подтверждения удаления профиля (см. Рисунок 48), если при создании профиля для текущего рабочего места пользователя пароль был сгенерирован автоматически. При нажатии кнопки <Нет> действие по удалению профиля пользователя будет прекращено.

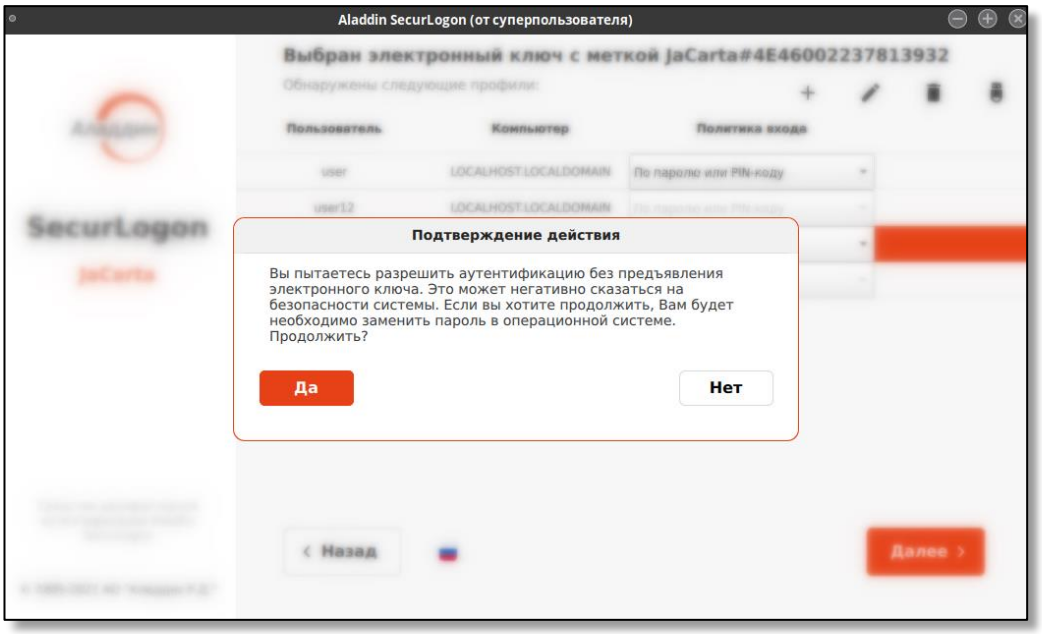

Рисунок 48 – Окно подтверждения удаления профиля пользователя при автоматической генерации пароля

При нажатии кнопки <Да>, будет предложено изменить пароль учетной записи пользователя текущего рабочего места удаляемого профиля (см. Рисунок 49). При нажатии кнопки <Отмена> действие по удалению профиля пользователя будет прекращено.

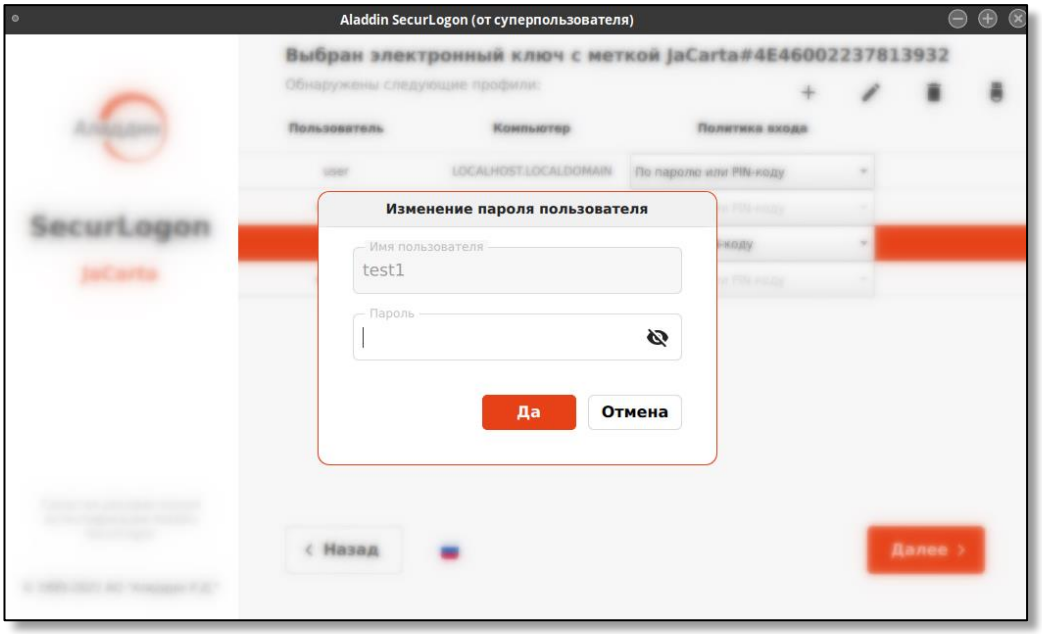

Рисунок 49 – Окно изменения пароля учетной записи пользователя при удалении профиля пользователя приложения электронного ключа

После ввода пароля нажмите кнопку <Да>, чтобы сохранить изменения пароля и продолжить удаление выбранного профиля пользователя, появится окно подтверждения удаления профиля пользователя (см. Рисунок 50). Нажмите кнопку <Нет>, чтобы отменить удаление выбранного профиля пользователя.

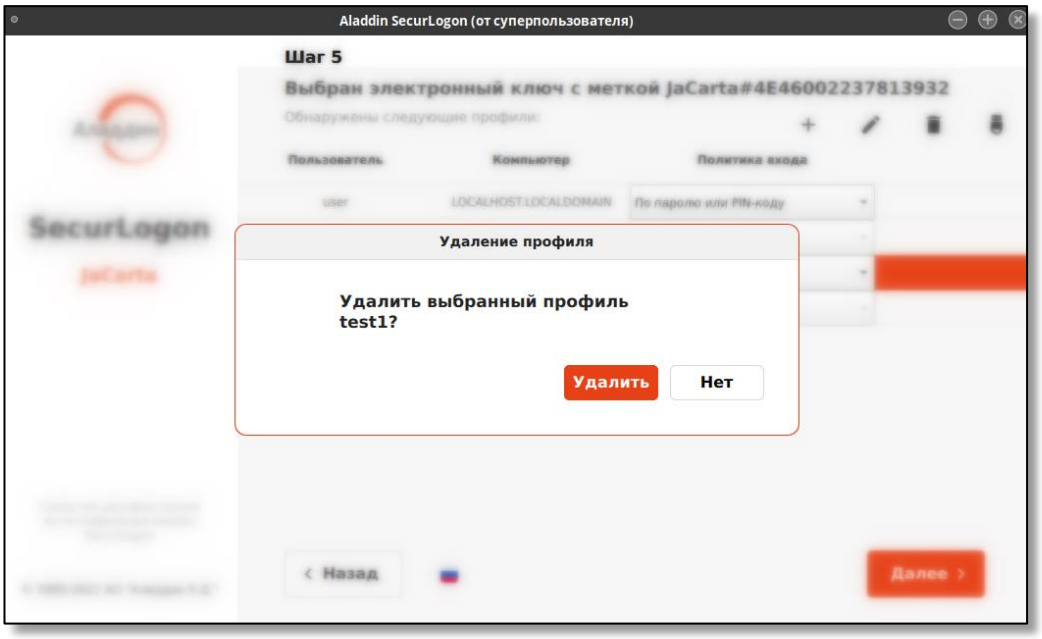

Рисунок 50 – Окно подтверждения удаления профиля пользователя

Нажмите кнопку <Удалить>, чтобы завершить удаление профиля пользователя. В случае успешного выполнения действия будет показано окно уведомления об успешной операции (см. Рисунок 51).

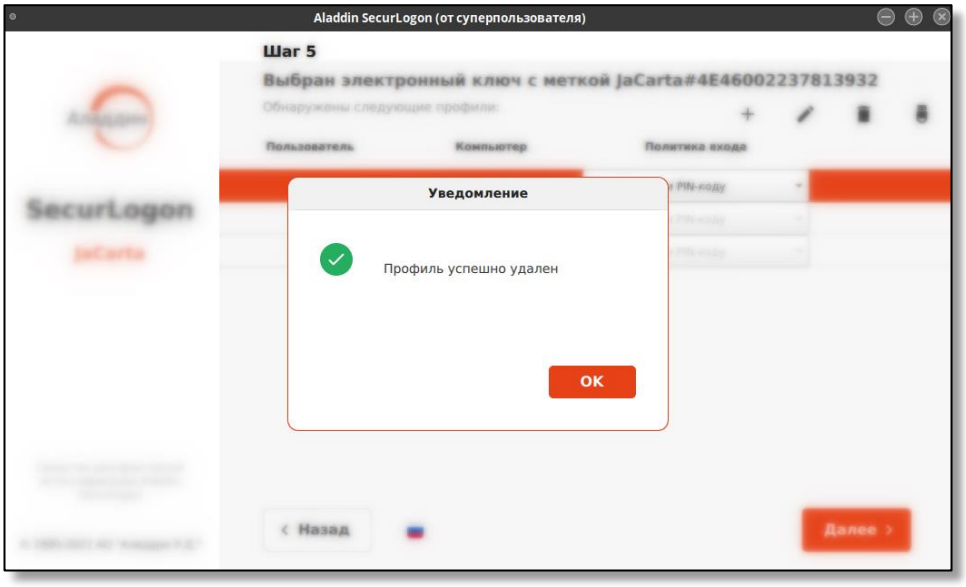

Рисунок 51 – Окно уведомления об успешном удалении профиля пользователя

8.1.2.2.4 Действия при извлечении электронного ключа

Для настройки действия при извлечении электронного ключа из разъёма нажмите кнопку  на панели управления сертификатами (см. Рисунок 52) и выберете нужное действие:

- бездействие – при извлечении электронного ключа ничего не произойдет, текущий сеанс продолжается в штатном режиме;
- блокировать сессию пользователя – при извлечении электронного ключа сессия пользователя будет заблокирована;
- выключить компьютер.

Если у пользователя настроена политика входа «Только по паролю», то двухфакторная аутентификация в этом случае не используется. Поэтому, вне зависимости от настроенного действия, при извлечении электронного ключа ничего не произойдет.

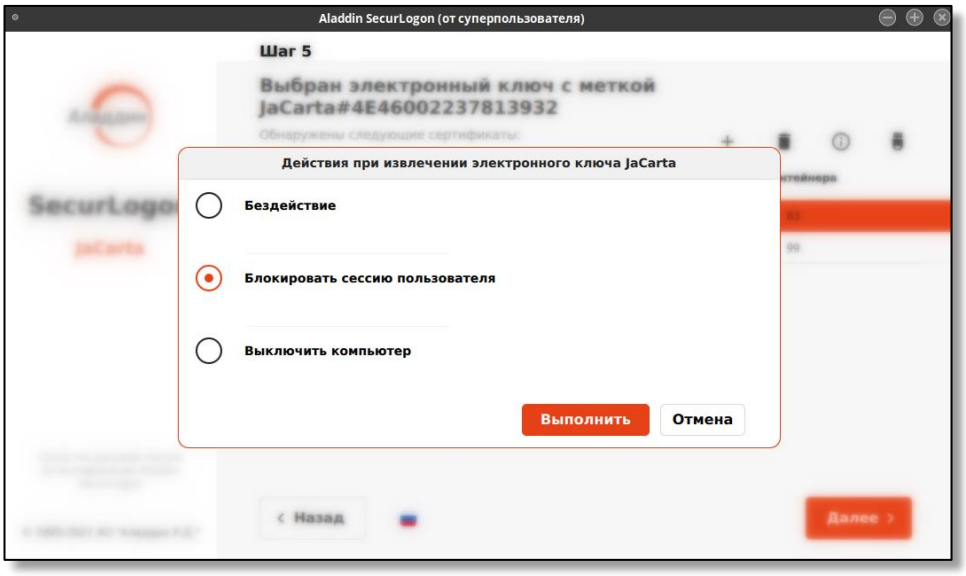

Рисунок 52 – Окно выбора действия при извлечении электронного ключа

Подтвердите действие, нажав кнопку <Выполнить>, при успешном сохранении выбора действия при извлечении электронного ключа вы увидите уведомление об успехе операции (см. Рисунок 53).

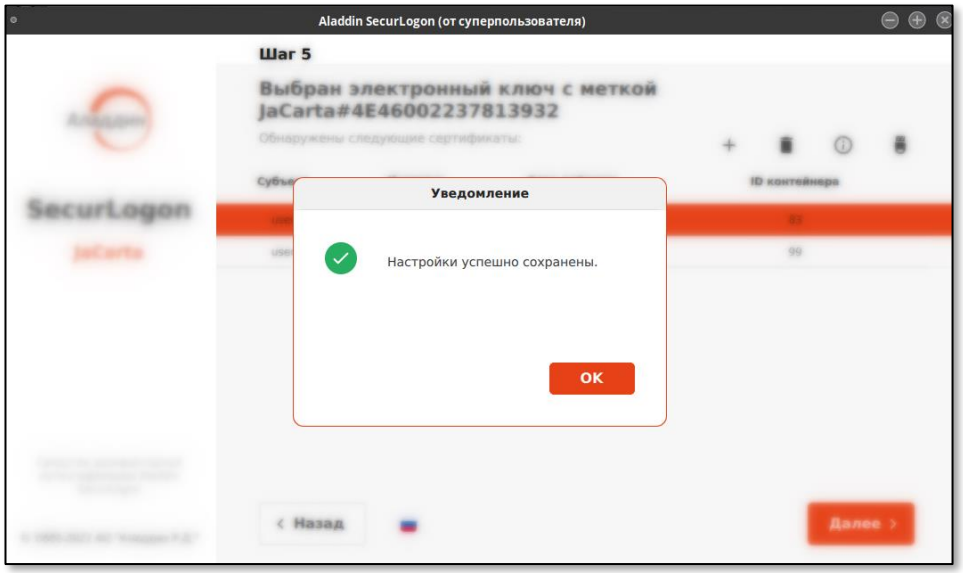

Рисунок 53 – Окно уведомления об успешном сохранении выбора действия при извлечении электронного ключа

Также настройку действия при извлечении электронного ключа можно выполнить на финальном этапе настройки двухфакторной аутентификации.

8.1.2.3 Завершение настройки аутентификации

После окончания работы с профилями пользователей нажмите на экранной форме шага 5 (см. Рисунок 37) кнопку <Далее>. Осуществляется переход на следующий шаг настройки локальной двухфакторной аутентификации (см. Рисунок 34).

На данном шаге 6 возможно настроить действие при извлечении электронного ключа из разъема ПК, выбрав нужное значение на экранной форме шага 6.

Также можно применить тему SecurLogon (см. Приложение А) для входа пользователя в систему перед началом сеанса, где предлагается выбрать учетную запись пользователя по нажатию на радиокнопку и ввести пароль и/или PIN-код в соответствии с назначенной политикой входа.

Все изменения будут применены по нажатию на кнопку <Завершить> и перезагрузке компьютера.

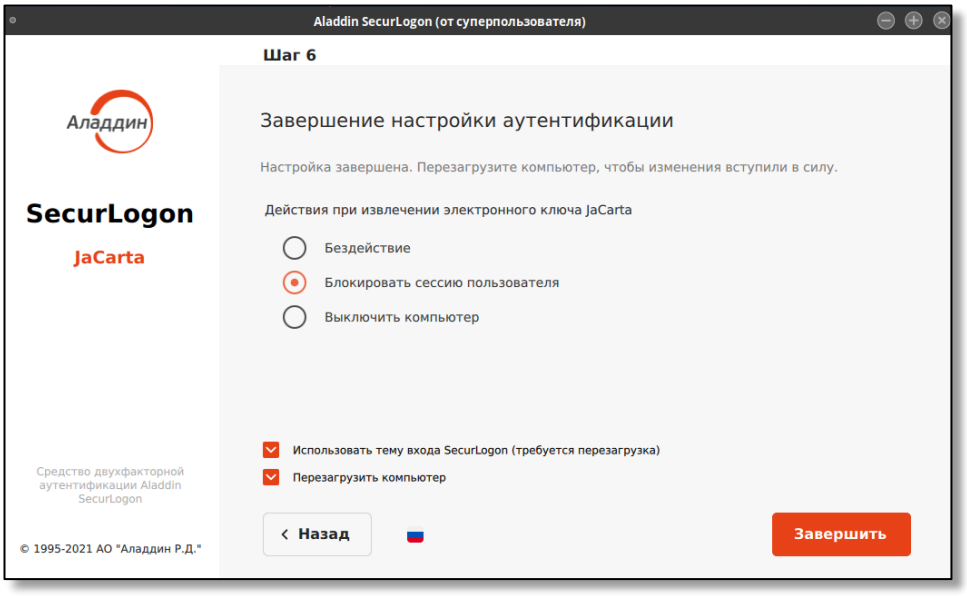

Рисунок 54 - Окно настройки локальной аутентификации без использования PKI. Шаг 6

8.1.3 Отключение локальной аутентификации

Чтобы изменить ранее настроенную локальную двухфакторную аутентификацию:

- запустите программу;
- выполните аутентификацию путем ввода пароля администратора (см. Рисунок 8);
- в приветственном окне (см. Рисунок 9), нажмите кнопку <Далее>;
- в окне шага 1 выберите способ аутентификации «Локальный», нажмите кнопку <Далее>;
- в окне шага 2 (см. Рисунок 16) выберите действие «Отключить вход в систему по электронному ключу», нажмите кнопку <Далее>, после чего на экране появится окно «Подтверждение действия» (см. Рисунок 55), в данном окне необходимо отклонить изменения, нажав кнопку <Нет> или подтвердить отключение аутентификации, нажав кнопку <Да>.

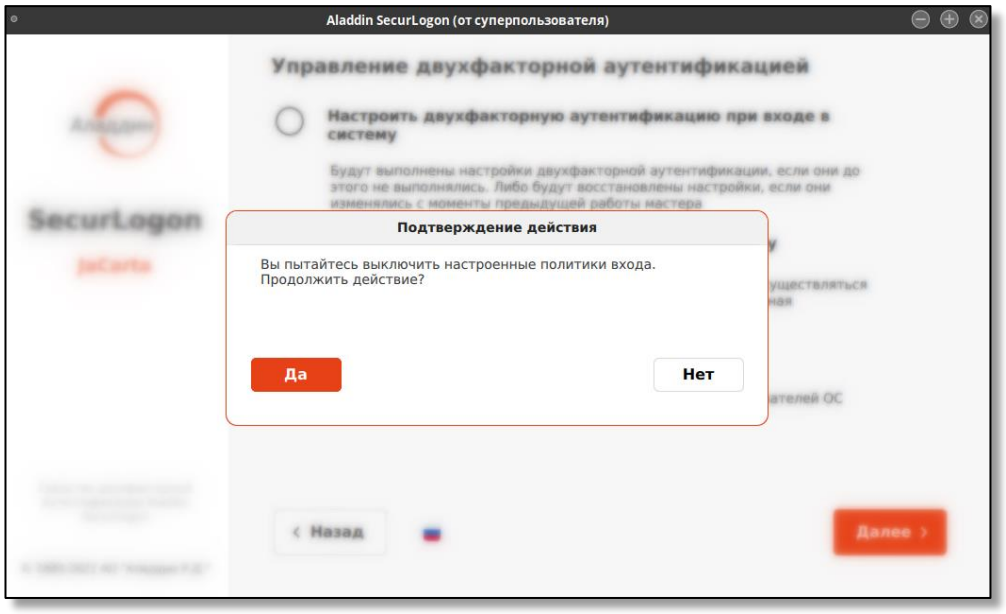

Рисунок 55 – Окно подтверждения отключения локальной двухфакторной аутентификации

После подтверждения отключения аутентификации, если в системе есть пользователи с автоматически сгенерированными паролями, то в следующем окне необходимо произвести аутентификацию для доступа к электронному ключу (см. Рисунок 56), нажать кнопку <Да> для продолжения отключения входа по электронному ключу.

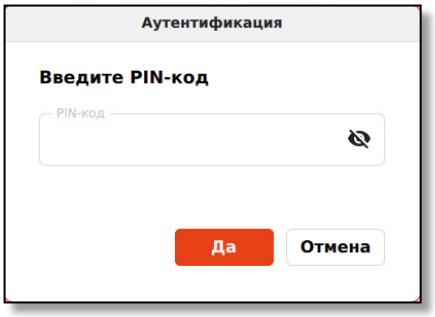

Рисунок 56 – Окно ввода PIN-кода при отключении локальной аутентификации для профилей пользователей с автоматически сгенерированным паролем

Далее в окне «Изменение пароля пользователя» (см. Рисунок 57) необходимо задать новый пароль для каждой учетной записи пользователя с автоматически сгенерированным паролем. После этого нужно установить пароль, нажав кнопку <Да>, и перейти к завершению настройки аутентификации (см. Рисунок 58).

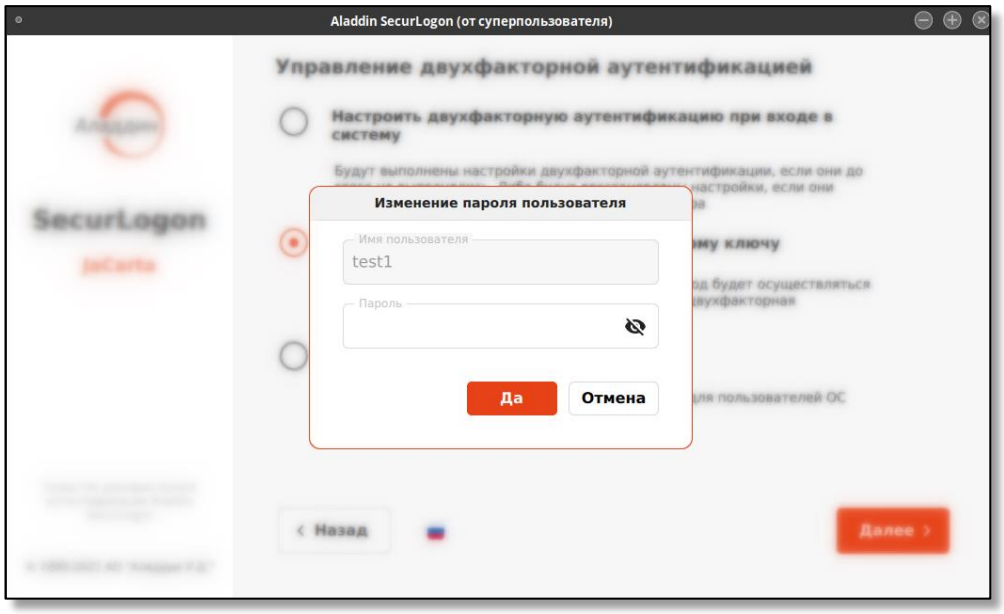

Рисунок 57 – Окно изменения пароля пользователя при отключении локальной аутентификации

Если в системе нет пользователей с автоматически сгенерированным паролем при создании профиля пользователя, то осуществляется автоматический переход к завершению отключения локальной аутентификации (см. Рисунок 58).

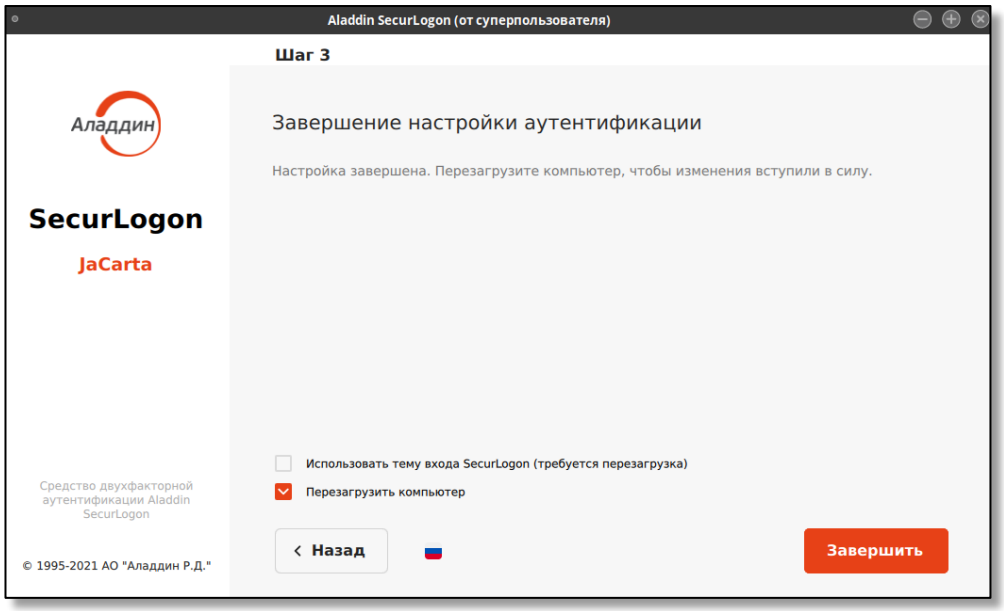

Рисунок 58 – Окно завершения отключения локальной аутентификации

На форме «Завершение настройки аутентификации», чтобы завершить операцию нажмите кнопку <Завершить>.

8.1.4 Управление политиками входа

Для изменения ранее настроенных политик входа пользователей на шаге 2 (см. Рисунок 16) выбираем способ управления двухфакторной аутентификацией «Управление политиками входа». Для перехода к следующему шагу нажмите кнопку <Далее>.

8.1.4.1 Локальная строгая или усиленная аутентификация с использованием электронного ключа (с/без PKI)

В поле диалогового окна шага 3 (см. Рисунок 59) показаны все приложения, записанные на подсоединенном электронном ключе. Выберите нужное приложение и нажмите кнопку <Далее> для продолжения действий по изменению политики входа.

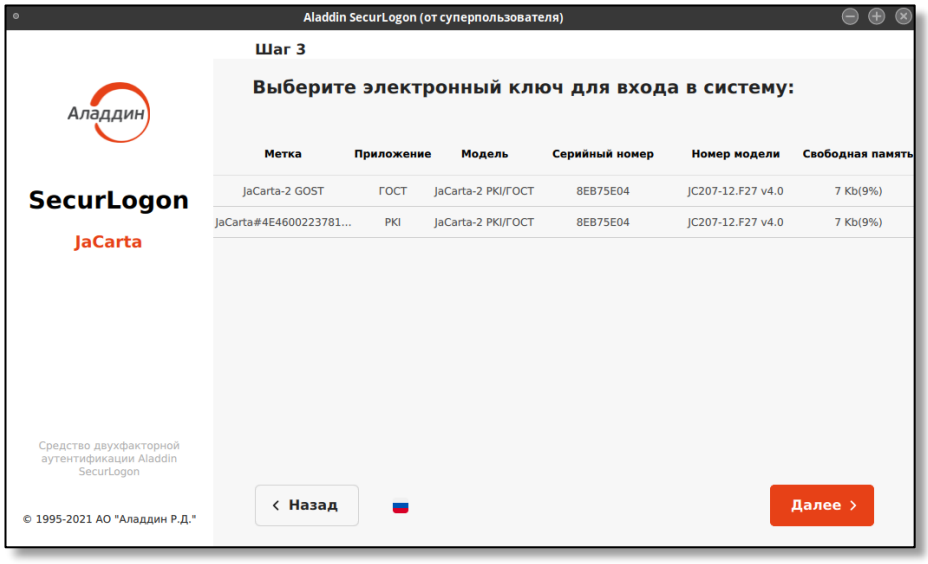

Рисунок 59 – Окно управления политиками входа учетных записей с использованием электронного ключа. Шаг 3

Дальнейшие действия по настройке политики входа повторяют действия, описанные в пункте 8.1.1.2 для локальной строгой аутентификации (с использованием PKI) и в пункте 8.1.2.2 – для локальной усиленной аутентификации (без использования PKI).

В случае, если на электронном ключе записано только одно приложение, то шаг выбора электронного ключа для входа в систему будет пропущен и по умолчанию выбран текущий подключенный единственный электронный ключ. После шага 2 будет осуществлен переход к окну выбора сертификатов единственного электронного ключа.

8.1.4.2 Локальная строгая аутентификация (с PKI) без использования электронного ключа

В поле диалогового окна шага 3 (см. Рисунок 60) показаны все учетные записи пользователей текущей ОС, для которых возможно изменение политики входа.

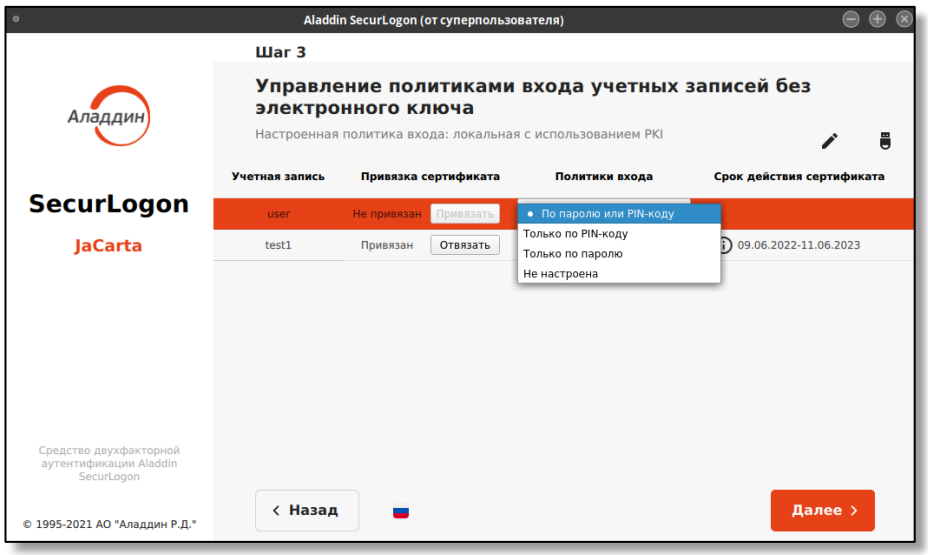

Рисунок 60 – Окно управления политиками входа учетных записей без электронного ключа с PKI

- Возможные политики входа:
  - По паролю или PIN-коду – если токен вставлен, то используется политика “Только по PIN-коду”, если токена нет в системе, то используется политика “Только по паролю”.
  - Только по паролю – вход осуществляется по паролю, при этом двухфакторная аутентификация не используется.
  - Только по PIN-коду – вход возможен только при подключенном электронном ключе.
  - Не настроена – данный пользователь не имеет политик входа и на него не распространяется двухфакторная аутентификация.

  По нажатию на кнопку <Отвязать> для выбранного пользователя будут отвязаны все сертификаты.
- По нажатию кнопки  возможна настройка действия при извлечении электронного ключа из разъёма. Нажмите кнопку  и выберете нужное действие (см. Рисунок 61).

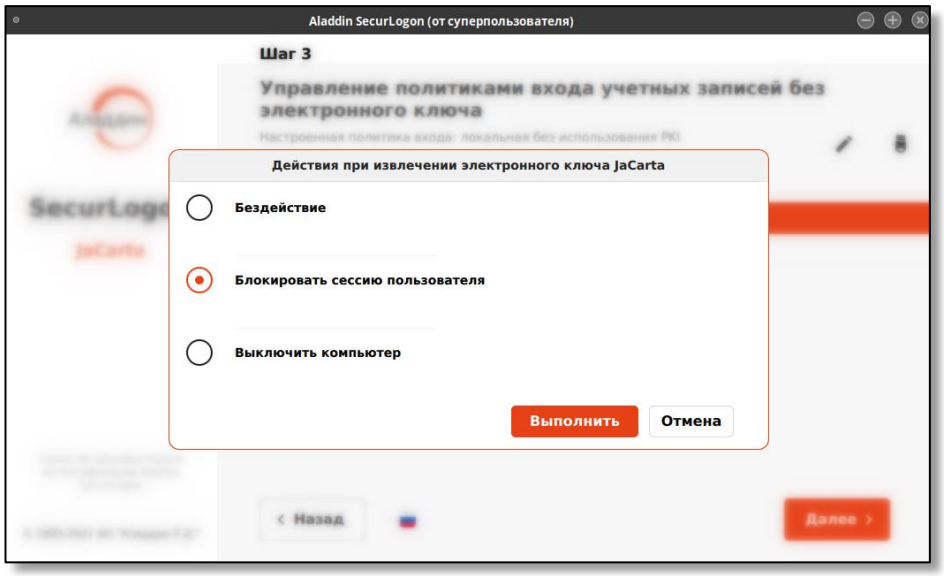

Рисунок 61 – Окно выбора действия при извлечении электронного ключа

Подтвердите действие, нажав кнопку <Выполнить>, при успешном сохранении выбора действия при извлечении электронного ключа вы увидите уведомление об успехе операции (см. Рисунок 62).

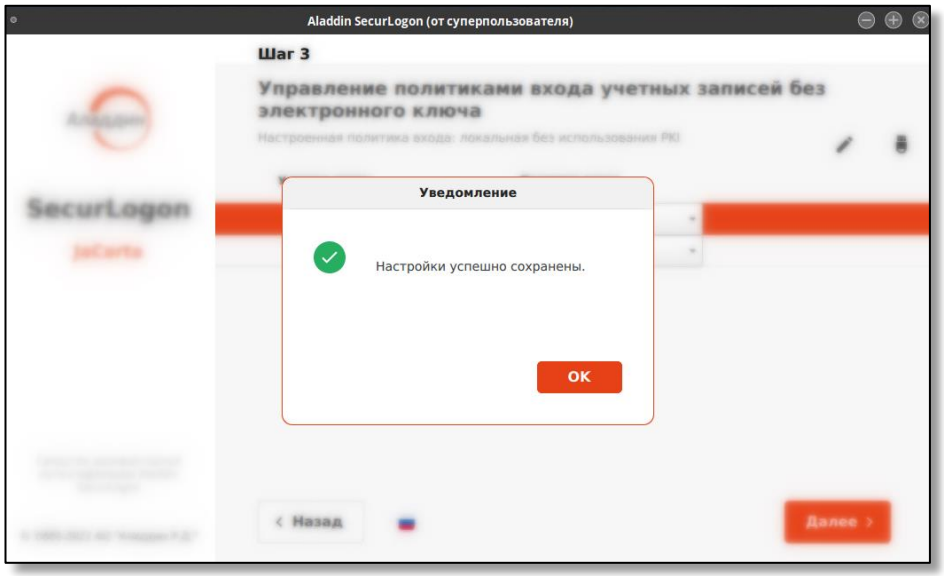

Рисунок 62 – Окно уведомления об успешном сохранении выбора действия при извлечении электронного ключа

- По нажатию на кнопку  возможно изменить текущий пароль пользователя для входа в ОС. В появившемся окне подтверждения (см. Рисунок 63) необходимо нажать кнопку <Нет> для прекращения действий или кнопку <Да> для продолжения изменения пароля.

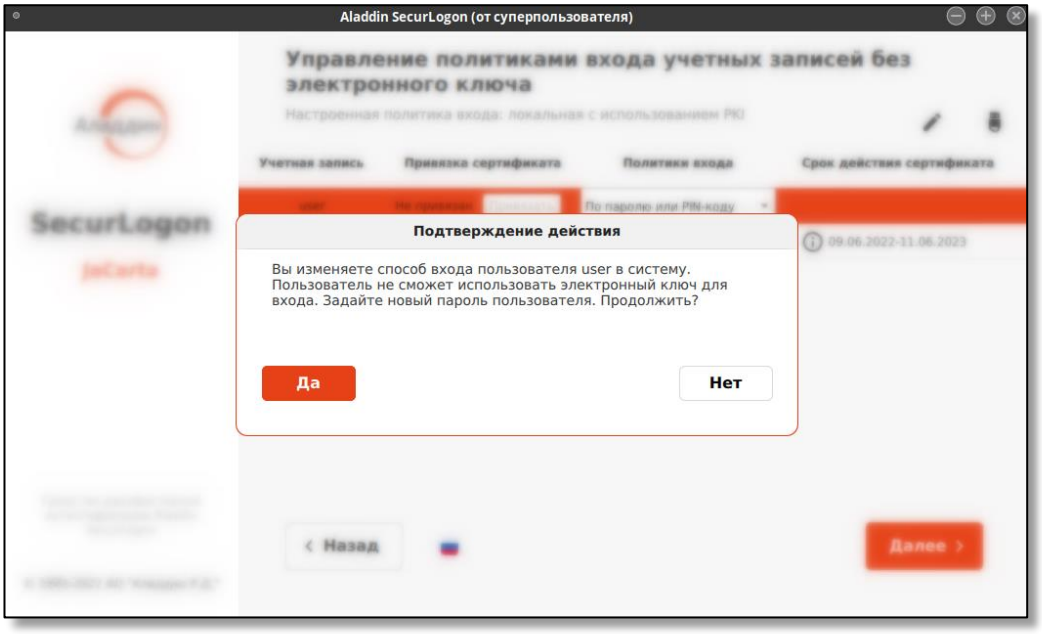

Рисунок 63 – Окно подтверждения изменения пароля пользователя для входа в систему

При подтверждении намерения в появившемся окне (см. Рисунок 64) необходимо задать новый пароль пользователя для входа в ОС без электронного ключа и нажать кнопку <Да>.

В случае, если нажата кнопка <Отмена>, пароль для входа в ОС останется прежним.

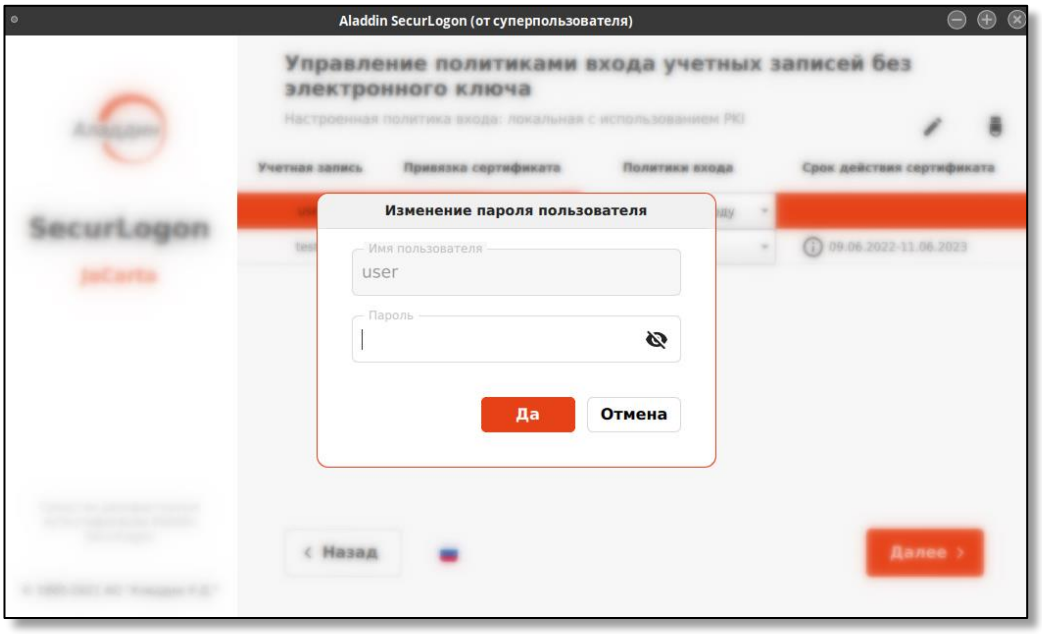

Рисунок 64 – Окно изменения пароля пользователя для входа в ОС

По нажатию кнопки <Далее> переходим к окну завершения настройки аутентификации.

8.1.4.3 Локальная усиленная аутентификация (без PKI) без использования электронного ключа

В поле диалогового окна шага 3 (см. Рисунок 65) показаны все учетные записи пользователей текущей ОС, для которых возможно изменение политики входа.

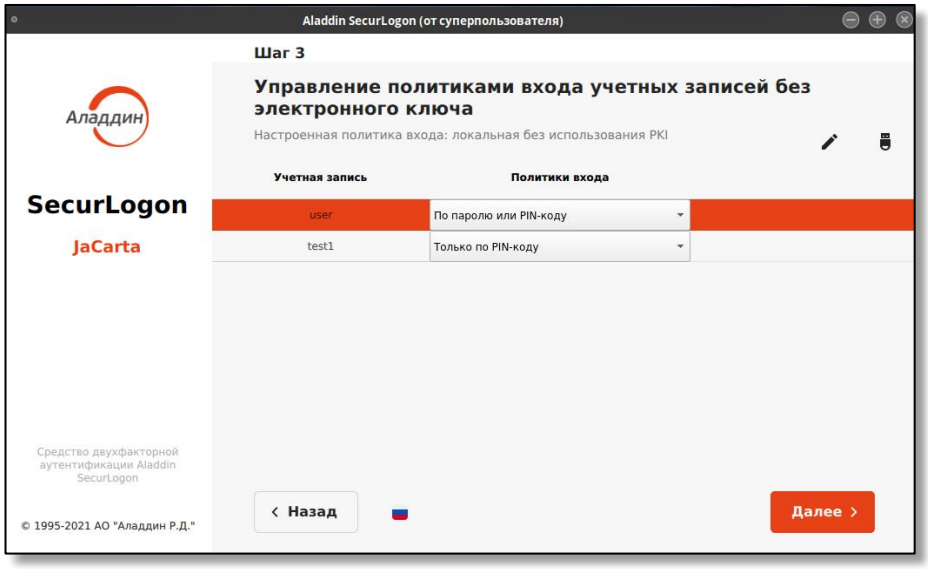

Рисунок 65 - Окно управления политиками входа учетных записей без электронного ключа без PKI

- Возможные политики входа:
  - По паролю или PIN-коду – если токен вставлен, то используется политика “Только по PIN-коду”, если токена нет в системе, то используется политика “Только по паролю”.
  - Только по паролю – вход осуществляется по паролю, при этом двухфакторная аутентификация не используется.
  - Только по PIN-коду – вход возможен только при подключенном электронном ключе.
  - Не настроена – данный пользователь не имеет политик входа и на него не распространяется двухфакторная аутентификация.
- По нажатию кнопки  возможна настройка действия при извлечении электронного ключа из разъёма. нажмите кнопку и выберете нужное действие.

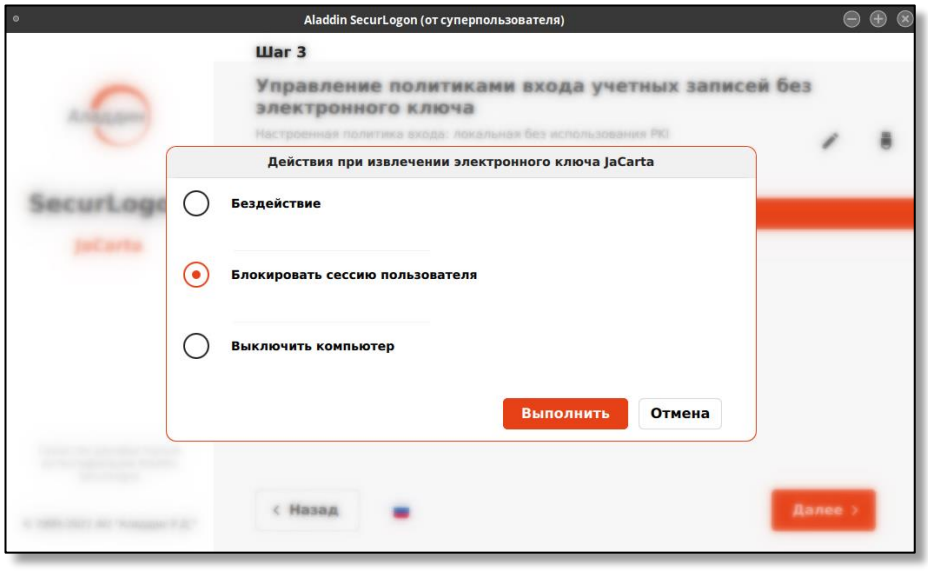

Рисунок 66 – Окно выбора действия при извлечении электронного ключа

Подтвердите действие, нажав кнопку <Выполнить>, при успешном сохранении выбора действия при извлечении электронного ключа вы увидите уведомление об успехе операции (см. Рисунок 67).

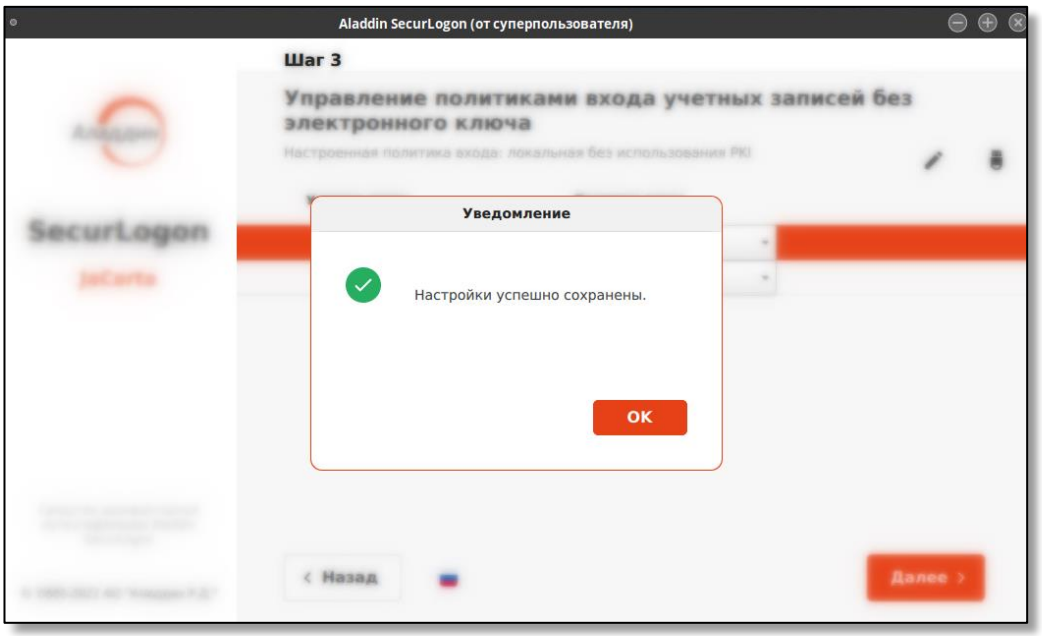

Рисунок 67 – Окно уведомления об успешном сохранении выбора действия при извлечении электронного ключа

- По нажатию на кнопку  возможно изменить текущий пароль пользователя для входа в ОС. В появившемся окне подтверждения (см. Рисунок 68) необходимо нажать кнопку <Нет> для прекращения действий или кнопку <Да> для продолжения изменения пароля.

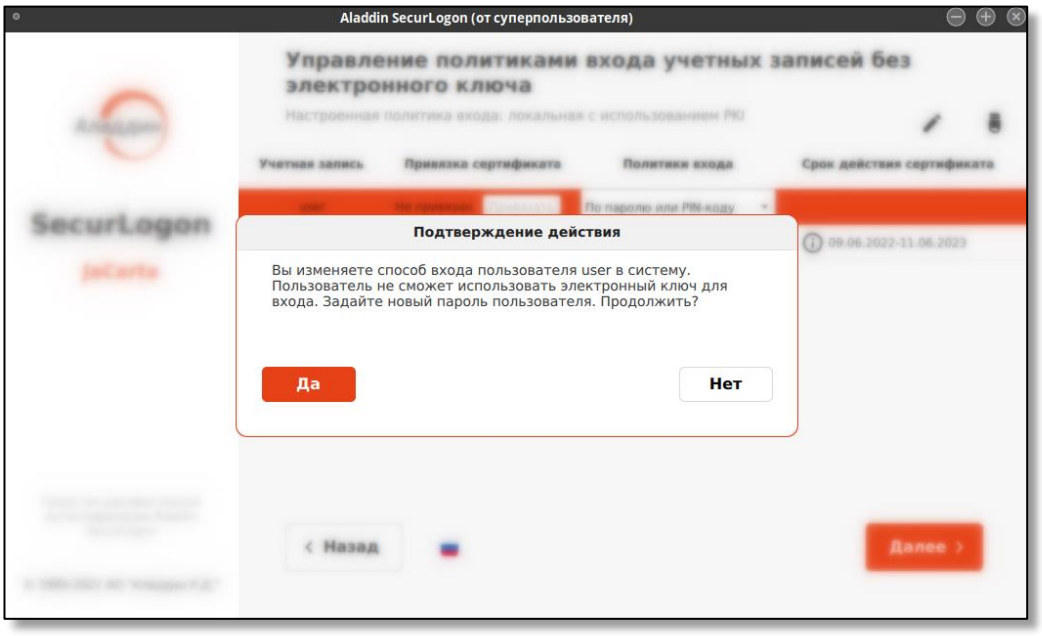

Рисунок 68 – Окно подтверждения изменения пароля пользователя для входа в систему

При подтверждении намерения в появившемся окне (см. Рисунок 69) необходимо задать новый пароль пользователя для входа в ОС без электронного ключа и нажать кнопку <Да>.

В случае, если нажата кнопка <Отмена>, пароль для входа в ОС останется прежним.

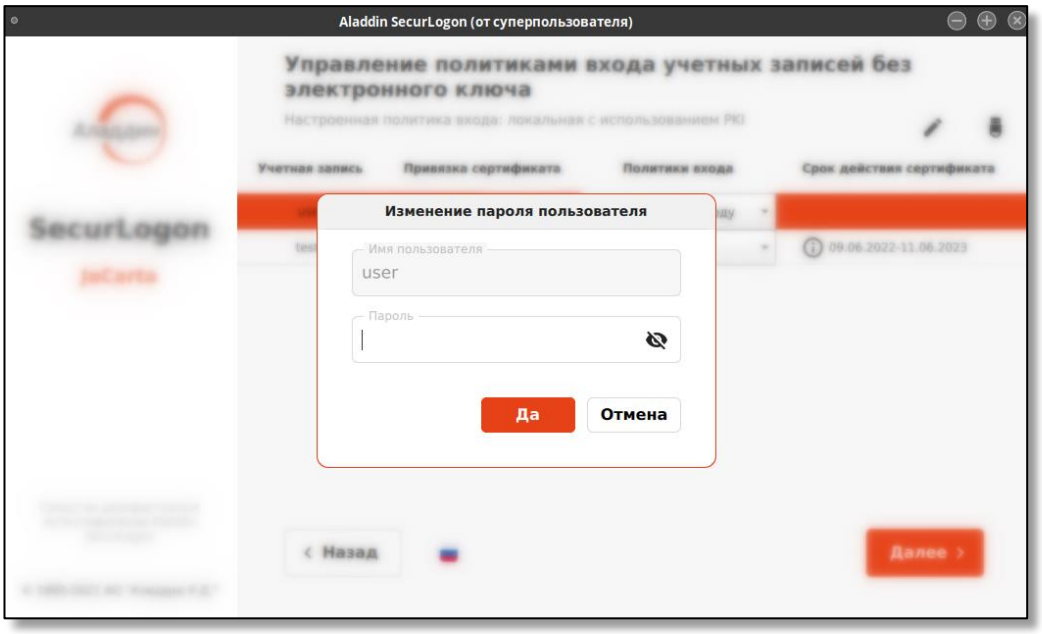

Рисунок 69 – Окно изменения пароля пользователя для входа в ОС

По нажатию кнопки <Далее> переходим к окну завершения настройки аутентификации.

8.2 Настройка сетевой аутентификации

Если на предыдущем шаге настройки аутентификации (см. Рисунок 15) выбран способ сетевой аутентификации, то осуществляется переход на следующий шаг (см. Рисунок 70).

При первичной настройке доступен для выбора только пункт <Настроить двухфакторную аутентификацию при входе в систему>. Для перехода на следующий шаг нажмите кнопку <Далее>.

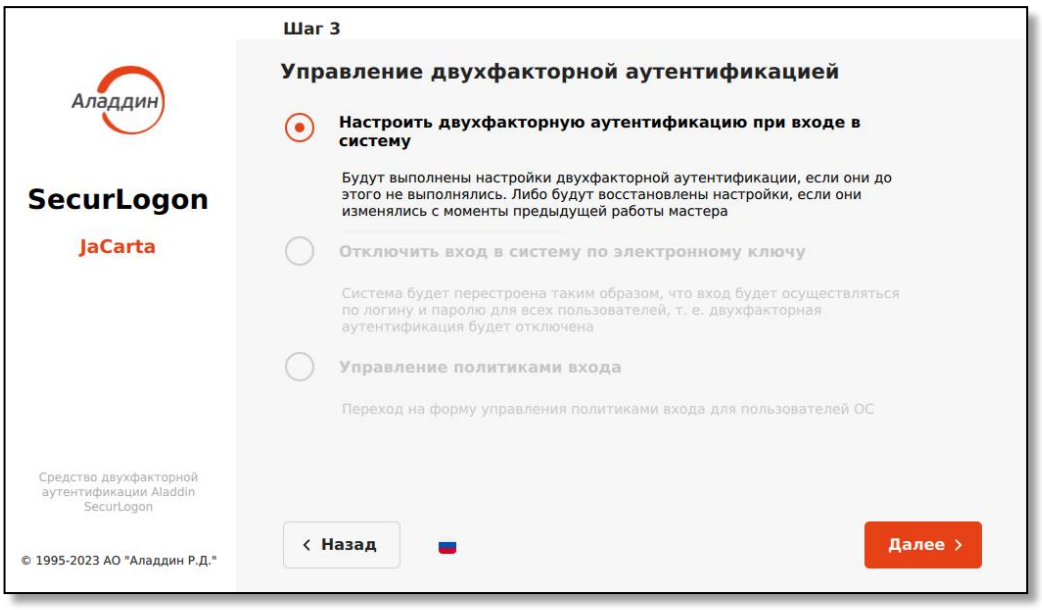

Рисунок 70 – Окно настройки сетевой аутентификации. Шаг 3

8.2.1 Строгая аутентификация

- Далее выбираем способ входа в систему <С использованием PKI> (см. Рисунок 71). Для перехода к следующему шагу нажмите кнопку <Далее>.

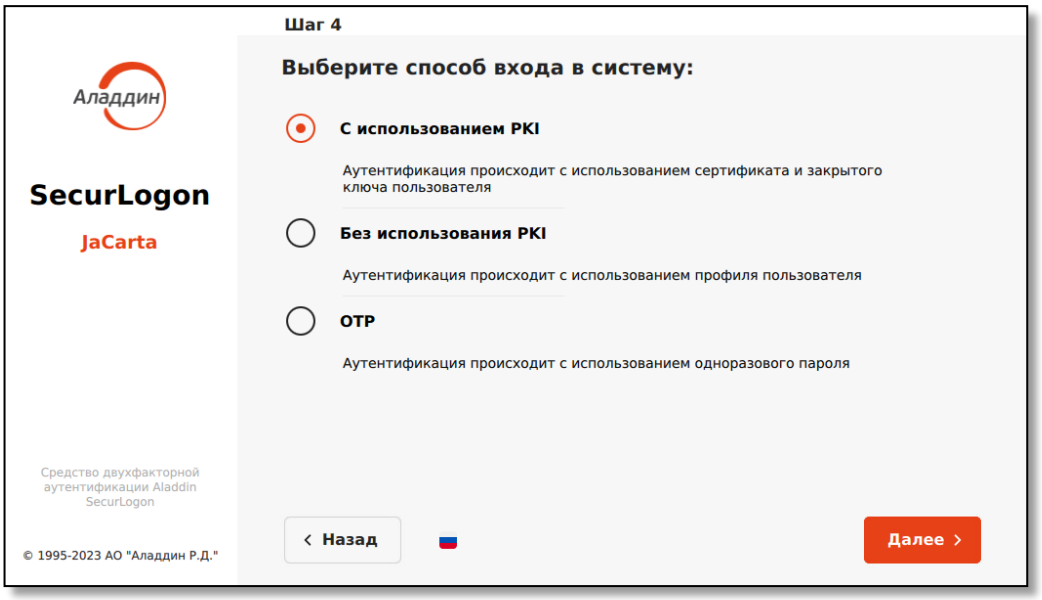

Рисунок 71 – Окно настройки сетевой аутентификации. Шаг 4

8.2.1.1 Предварительная подготовка к настройке сетевой строгой аутентификации (с использованием PKI)

- На данном шаге к настраиваемому ПК должен быть подсоединен электронный ключ. На электронном ключе допускается наличие нескольких апплетов.
- Убедиться, что настраиваемый ПК зарегистрирован в домене.
- Убедиться, что служба sssd настроена и запущена.
- Экспортировать на электронный ключ или в файловую систему настраиваемого ПК цепочку сертификатов корневого центра сертификации PKCS7 в формате .p7b (в кодировке base64 или PEM) или корневой сертификат в кодировке base64 в одном из форматов:
  - .crt;
  - .cet;
  - .key;
  - .pem.
- Экспортировать корневые сертификаты на электронный ключ рекомендуется с помощью ПО «Единый клиент» не младше версии 3166. В этом случае при экспорте сертификатов ID контейнер устанавливается по умолчанию.

> *Если вы хотите экспортировать на электронный ключ и корневые, и пользовательские сертификаты, а затем использовать этот ключ для аутентификации, то необходимо, чтобы у всех корневых сертификатов на электронном ключе обязательно было установлено ID контейнера (CKA_ID).*

8.2.1.2 Настройка сетевой строгой аутентификации (с PKI)

На следующем шаге (см. Рисунок 72) произведите настройку сетевой аутентификации.

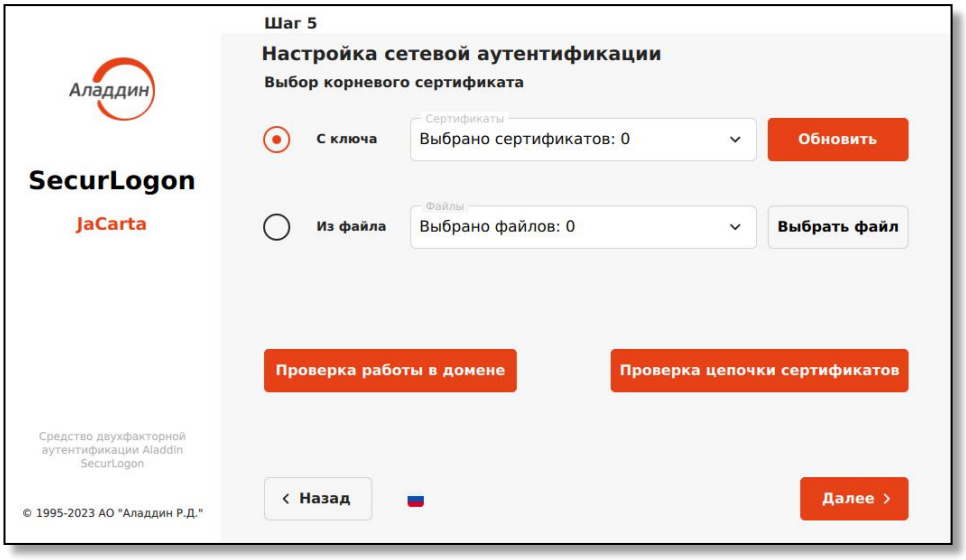

Рисунок 72 - Окно настройки сетевой аутентификации с использованием PKI. Шаг 5

Для настройки сетевой аутентификации выполните следующие действия:

- выберете цепочку сертификатов корневого удостоверяющего центра по радиокнопке, выбрав из двух опций:
  - загрузка корневого сертификата с подключенного электронного ключа. По нажатию на кнопку <Обновить> происходит автоматическое считывание сертификатов с подключенного электронного ключа.
  - из файла на локальном или сетевом диске, по нажатию на кнопку <Выбрать файл>.
- произведите проверку цепочки сертификатов, нажав кнопку <Проверка цепочки сертификатов>. В открывшемся окне (см. Рисунок 73), выберите проверяемый пользовательский сертификат с подключенного электронного ключа. При необходимости для повторного считывания сертификатов с электронного ключа нажмите кнопку <Обновить>. Нажмите кнопку <Ок> для выполнения проверки цепочки сертификатов.

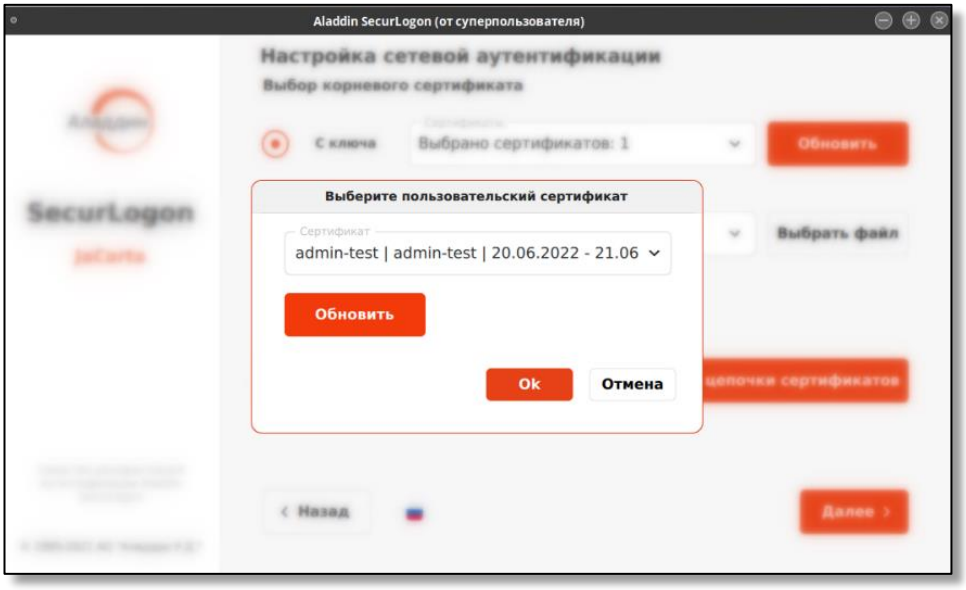

Рисунок 73 – Окно выбора пользовательского сертификата

При успешной верификации пользовательского сертификата вы увидите уведомление об успехе операции (см. Рисунок 74).

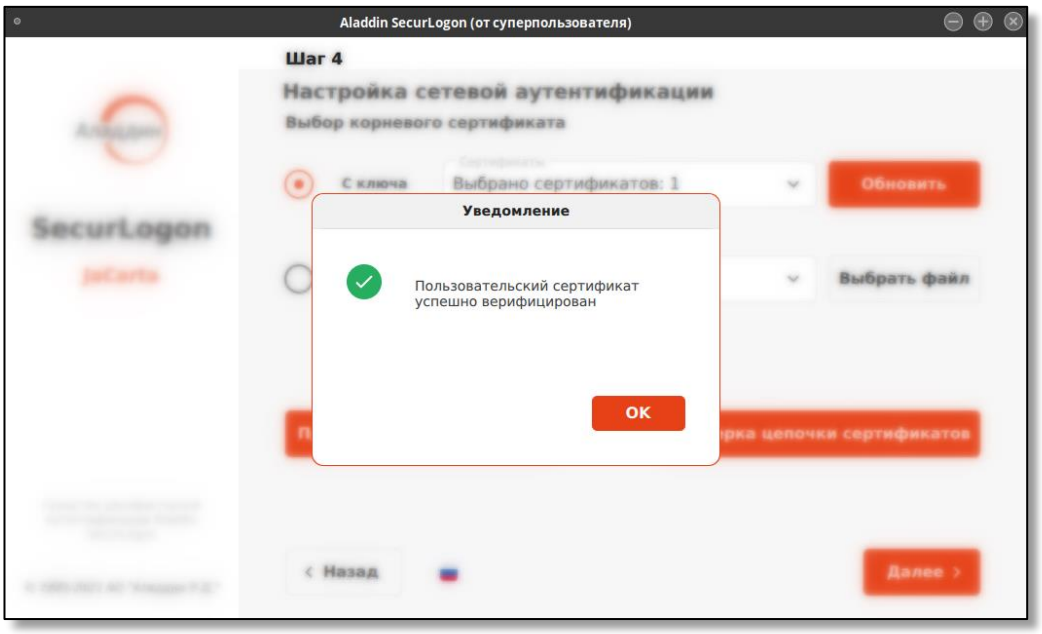

Рисунок 74 – Окно уведомления об успешной проверке пользовательского сертификата

- Далее в диалоговом окне шага 4 (см. Рисунок 72) нажмите кнопку <Проверка работы в домене>, в открывшемся окне (см. Рисунок 75) введите учетные данные доменного пользователя, для которого на предыдущем шаге проверяли сертификат, доменное имя подставляется автоматически с возможностью корректировки путем ввода с клавиатуры. Нажмите кнопку <Ok> для проверки настройки учетной записи пользователя в домене.

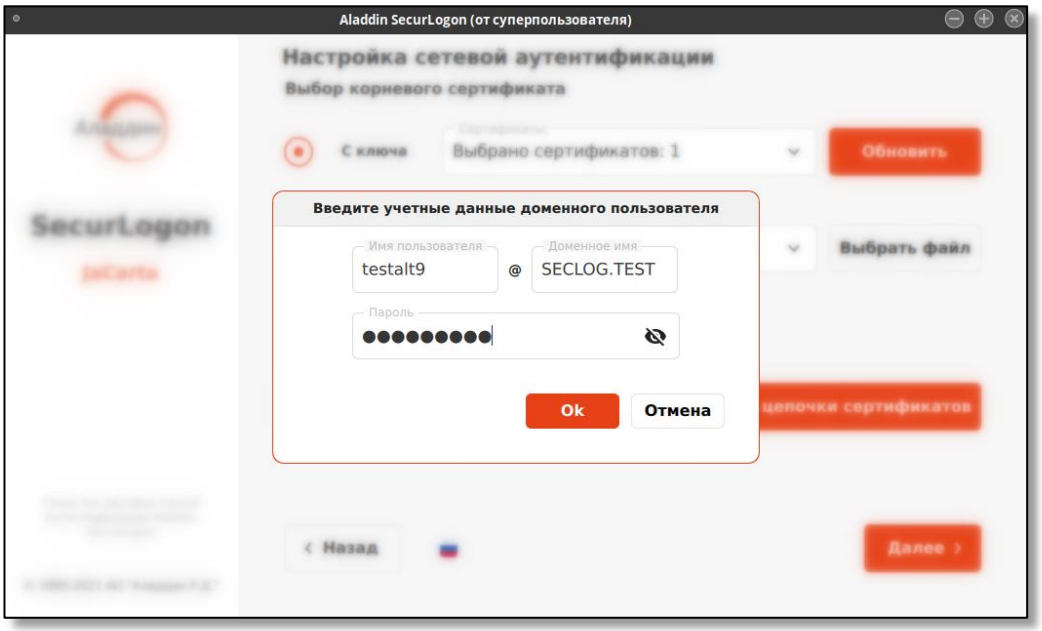

Рисунок 75 – Окно проверки учетных данных пользователя в домене

При успешной проверке учетной записи пользователя вы увидите уведомление об успехе операции.

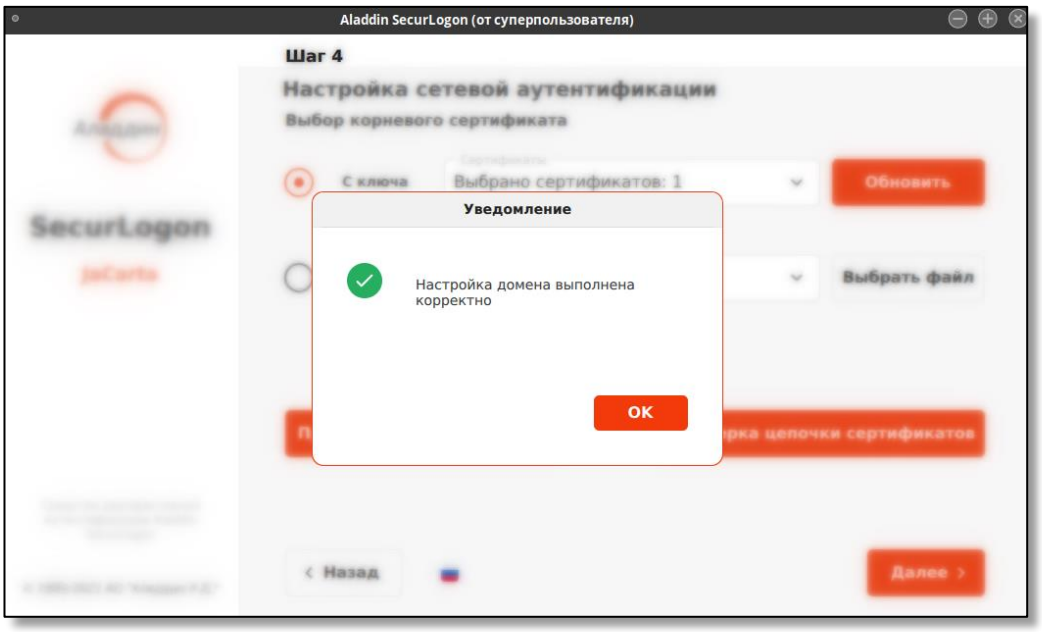

Рисунок 76 – Окно уведомления об успешной проверке учетных данных пользователя в домене

- В диалоговом окне текущего шага (см. Рисунок 72) нажмите кнопку <Далее>, при переходе к следующему шагу будет показано окно Рисунок 77, в данном окне имя центра распределения ключей Kerberos (KDC) заполняется автоматически.
- При необходимости добавить сервер нажмите кнопку <+>, в текущем окне в появившейся строке введите имя центра распределения ключей Kerberos.
- При нажатии на пиктограмму 🗑 строка с именем KDC будет удалена.

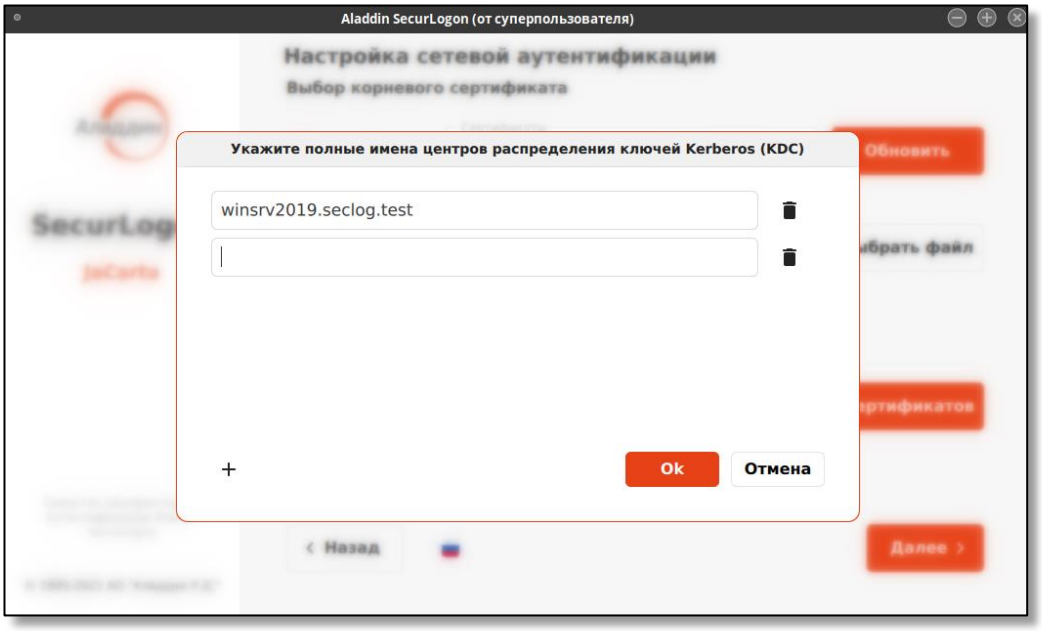

Рисунок 77 – Окно подключения центров распределения ключей Kerberos (KDC)

Нажмите кнопку <Ok> для настройки сетевой двухфакторной строгой аутентификации (с PKI).

- Далее будет предложено дополнительно настроить OTP аутентификацию (см. Рисунок 78).

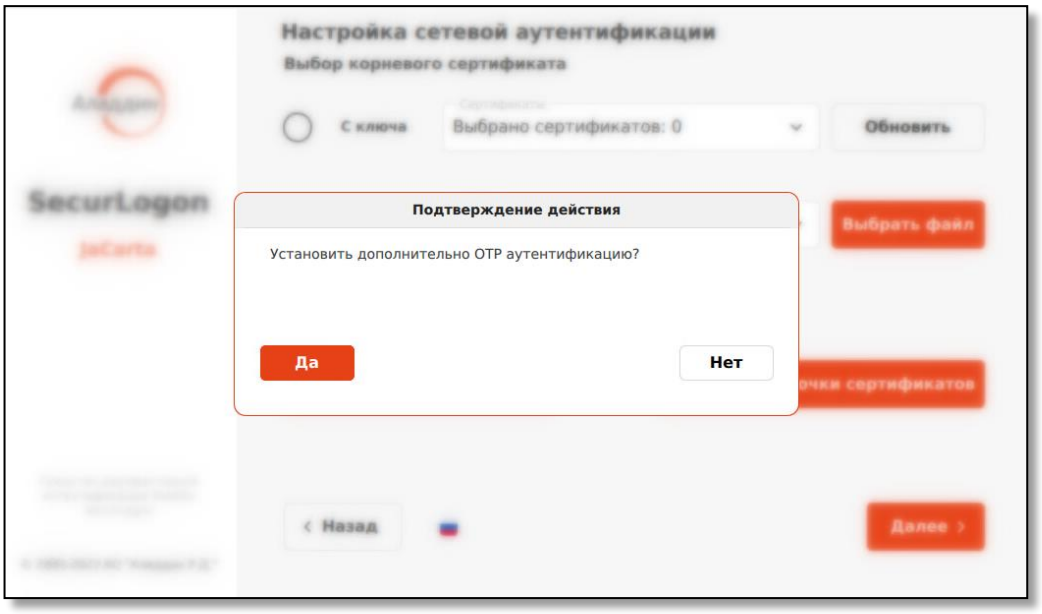

Рисунок 78 – Окно запроса установки OTP аутентификации

При подтверждении по нажатию на кнопку <Да> уполномоченный пользователь переходит в окно настройки OTP аутентификации (см. Рисунок 79). Подробное описание настройки приведено в подразделе 8.2.2 «OTP».

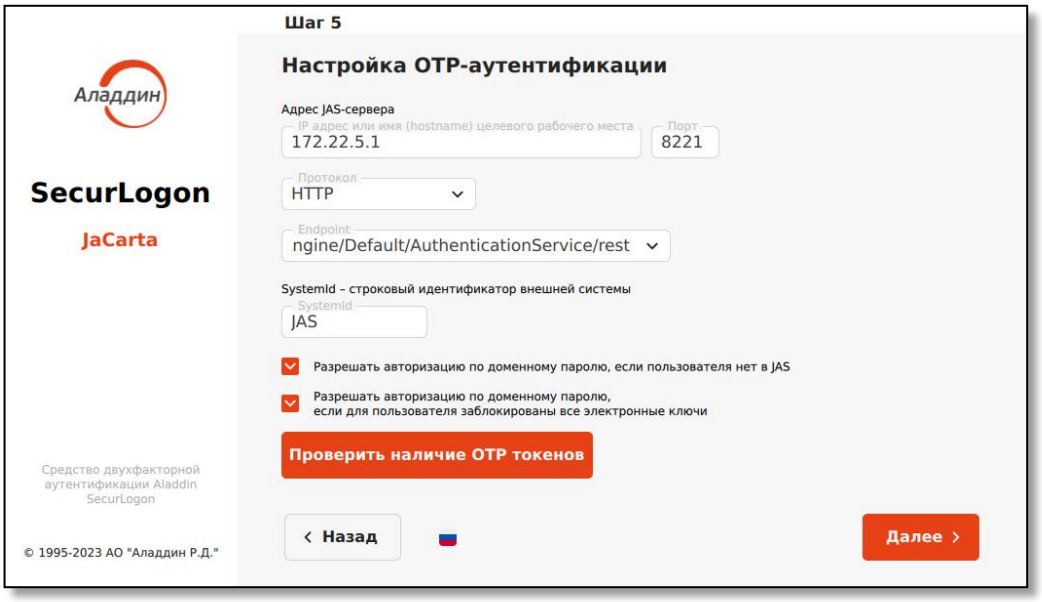

Рисунок 79 – Окно настройки OTP аутентификации

8.2.1.3 Завершение настройки строгой аутентификации

При отказе от настройки OTP аутентификации по нажатию на кнопку <Нет> или после завершения настройки OTP аутентификации осуществляется переход к завершающему шагу. (см. Рисунок 80).

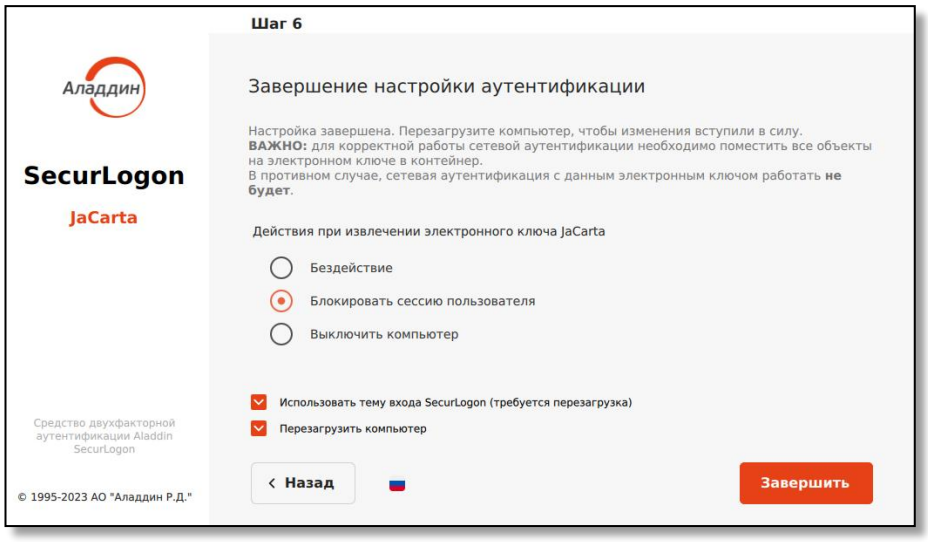

Рисунок 80 - Окно настройки сетевой аутентификации с использованием PKI. Шаг 6

На данном шаге произведите настройку действия при извлечении электронного ключа из разъема ПК во время активного сеанса пользователя, выбрав нужное значение на экранной форме:

- бездействие. При извлечении электронного ключа сеанс пользователя остаётся активным;
- блокировать сессию пользователя. При извлечении электронного ключа сеанс пользователя будет заблокирован, работа программ не завершается, необходимо выполнить повторную аутентификацию для возобновления сеанса;
- выключить компьютер. При извлечении электронного ключа текущий сеанс пользователя будет завершён, работа программ завершена, компьютер будет выключен.

Также можно применить тему SecurLogon (см. Приложение А) для входа пользователя в систему перед началом сеанса, где предлагается выбрать учетную запись пользователя по нажатию на радиокнопку и ввести пароль и/или PIN-код в соответствии с назначенной политикой входа, а также доступен набор действий до идентификации и аутентификации пользователя.

Все изменения будут применены по нажатию на кнопку <Завершить> и перезагрузке компьютера.

1.1.1 Усиленная аутентификация

На шаге 4 (см. Рисунок 81) выбираем способ входа в систему <Без использования PKI>. Для перехода к следующему шагу нажмите кнопку <Далее>.

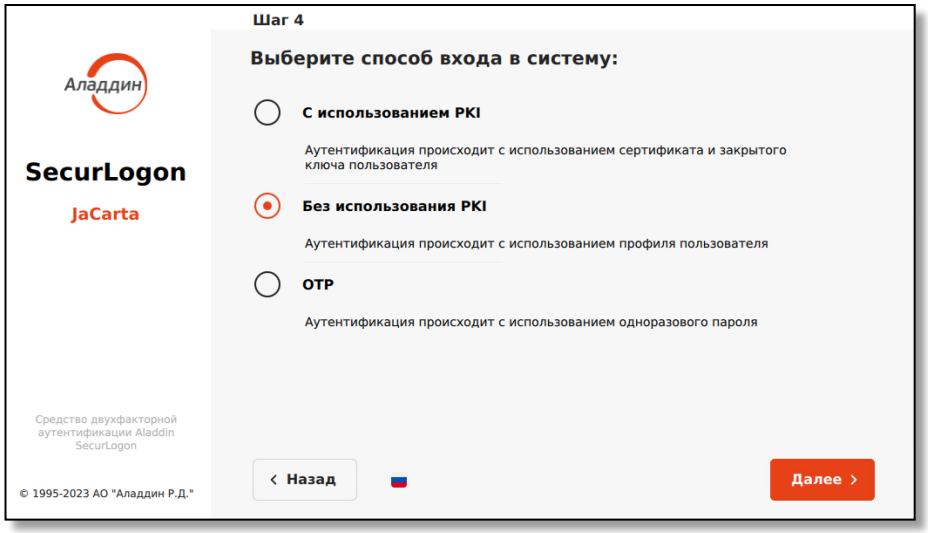

Рисунок 81 – Окно настройки сетевой аутентификации без использования PKI. Шаг 4

8.2.1.4 Предварительная подготовка к настройке сетевой усиленной аутентификации (без PKI)

- На данном шаге к настраиваемому ПК должен быть подсоединен электронный ключ. На электронном ключе допускается наличие нескольких апплетов.
- Убедиться, что настраиваемый ПК зарегистрирован в домене.
- Убедиться, что учётная запись пользователя, профиль которого будет создан далее при помощи SecurLogon, зарегистрирован в домене.
- Убедиться, что служба sssd настроена и запущена.
- Добавить учётную запись пользователя, для которого выполняется настройка аутентификации, в созданные группы.

8.2.1.5 Выбор электронного ключа

В поле диалогового окна шага 4 (см. Рисунок 82) показаны все записанные приложения на текущем электронном ключе, в столбцах указана следующая информация для каждого приложения:

- в столбце «метка приложения» указано название электронного ключа (имя токена);
- в столбце «приложение» указано название приложения, установленного в память электронного ключа, определяющее функциональность модели электронного ключа;
- в столбце «модель» указана модель электронного ключа;
- в столбце «серийный номер» указан 8-значный серийный номер электронного ключа;
- в столбце «номер модели» указана модель электронного ключа;
- в столбце «свободная память» указано свободное место на электронном ключе в Кбайтах и % от общего объема электронного ключа.

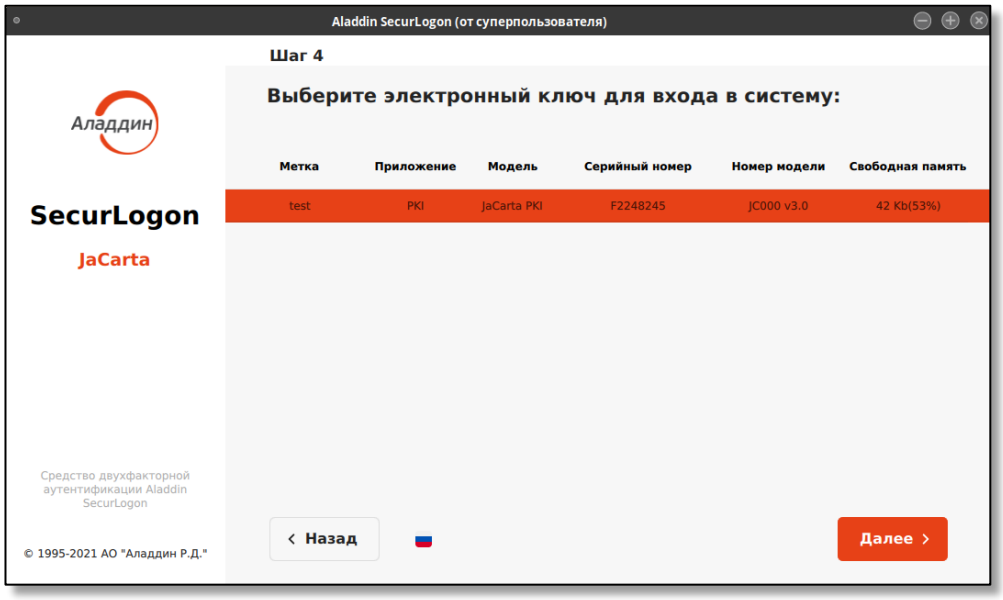

Рисунок 82 – Окно настройки сетевой аутентификации без использования PKI. Шаг 5

Выберите нужное приложение и нажмите кнопку <Далее>.

8.2.1.6 Выбор сертификата электронного ключа

В поле диалогового окна шага 5 (см. Рисунок 83) отображаются все имеющиеся сертификаты для выбранного на предыдущем шаге приложения.

В столбцах экранной формы для каждого сертификата отображена следующая информация:

- пользователь. В данном столбце отображены все профили пользователей, созданные на текущем электронном ключе;

– компьютер. В этом столбце отображены имена компьютеров, для работы на которых настроены соответствующие профили пользователей;

– политика входа определяется администратором для профилей пользователей домена.

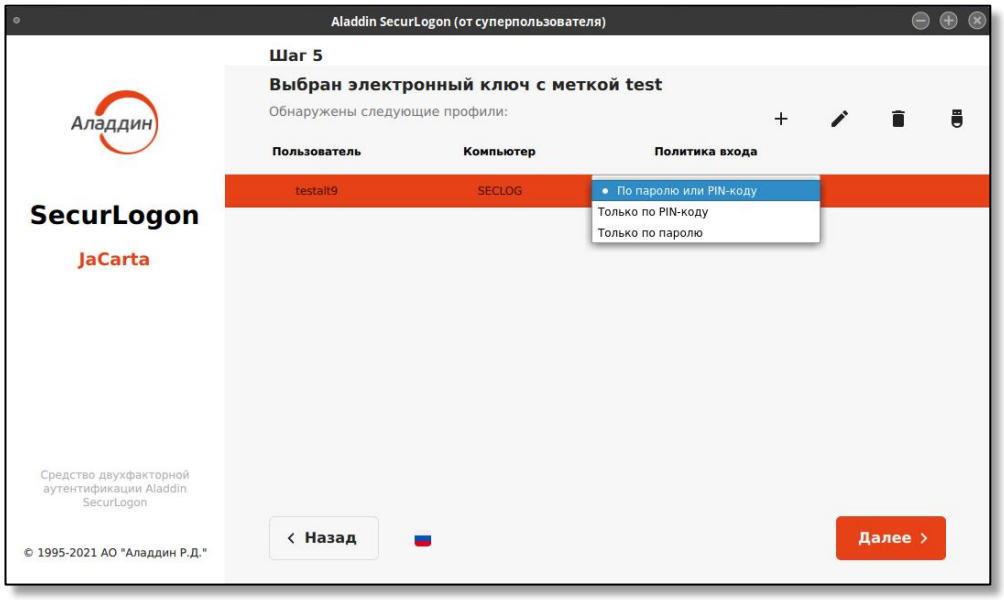

Рисунок 83 – Окно настройки сетевой аутентификации без использования PKI. Шаг 5

На данном шаге 5 осуществляется выбор профиля пользователя и для него доступны следующие действия:

- изменения политики входа. По нажатию на значение поля в столбце «Политика входа» всплывает меню (см. Рисунок 84).

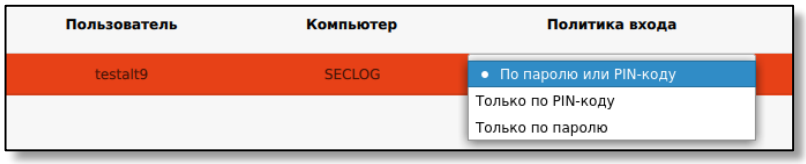

Рисунок 84 – Меню изменения политики входа при сетевой аутентификации без PKI

Возможно задание следующих политик входа:

– По паролю или PIN-коду. То есть, если электронный ключ подсоединен к ПК, то для аутентификации пользователя используется политика «Только по PIN-коду», если электронный ключ не подсоединен к ПК, то используется политика входа в ОС «Только по паролю».

– Только по паролю – для входа в ОС необходимо ввести имя и пароль учетной записи, двухфакторная аутентификация не используется.

– Только по PIN-коду – вход возможен только при подключенном электронном ключе, требуется выбрать пользователя и ввести PIN-код электронного ключа пользователя. PIN-коды по умолчанию при поставке приведены в таблице 3, раздела 3.2 RU.АЛДЕ.03.01.013-01 32 01-2 «Единый Клиент JaCarta. Руководства администратора «Аладдин Р.Д. « [1]. Настройка PIN-кода электронного ключа осуществляется при помощи ПО «Единый Клиент JaCarta» и подробно описано в разделе 10 RU.АЛДЕ.03.01.013-01 32 01-2 «Единый Клиент JaCarta. Руководства администратора «Аладдин Р.Д. « [1].

После выбора нужного значения происходит автоматическая смена политики входа.

- управление профилями пользователей посредством панели (см. Рисунок 85).

Рисунок 85 – Панель управления профилями

На данной панели представлены следующие возможности:

- создание нового профиля;
- редактирование данных выбранного профиля;
- удаление выбранного профиля;
- настройка действия при извлечении электронного ключа.

8.2.1.6.1 Создание нового профиля

Для создания нового профиля пользователя в панели управления профилями нажмите на кнопку , после чего появится окно «Аутентификация» (см. Рисунок 86), в случае если ранее не была проведена аутентификация на выбранном электронном ключе.

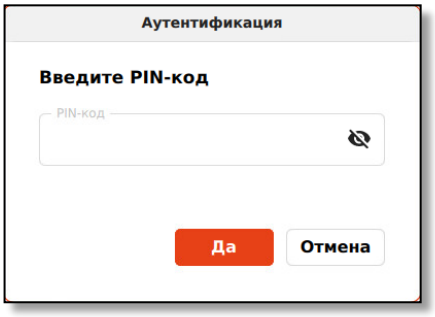

Рисунок 86 – Окно аутентификации для ввода ПИН-кода электронного ключа

Для авторизации на электронном ключе в окне “Аутентификация” введите PIN-код пользователя.

Количество попыток ввода PIN-кода пользователя определяется настройками электронного ключа.

После верно введённого PIN-кода вы увидите окно «Создание профиля» (см. Рисунок 87).

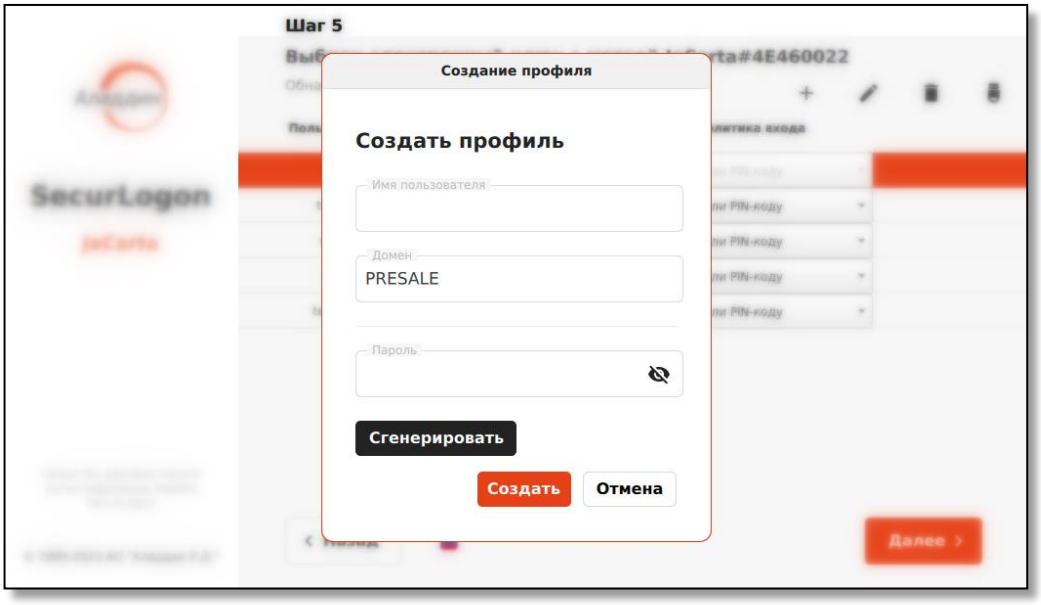

Рисунок 87 – Окно создания нового профиля

Заполните данные нового профиля, указав в соответствующих полях:

- имя пользователя – введите новое имя пользователя. Имя пользователя должно совпадать с учетной записью пользователя в домене;

- домен – имя домена, в котором настроена учетная запись пользователя, для которой активируем сетевую двухфакторную аутентификацию, заполняется автоматически с возможностью редактирования поля;
- пароль – должен совпадать с паролем учетной записи в домене (правила ввода пароля см. Приложение Б. Правила формирования пароля).

Пароль пользователя может быть сгенерирован автоматически. По нажатию на кнопку <Сгенерировать> в открывшемся окне подтверждения выберите <Да> для продолжения смены пароля доменной учётной записи на автосгенерированный (см. Рисунок 88).

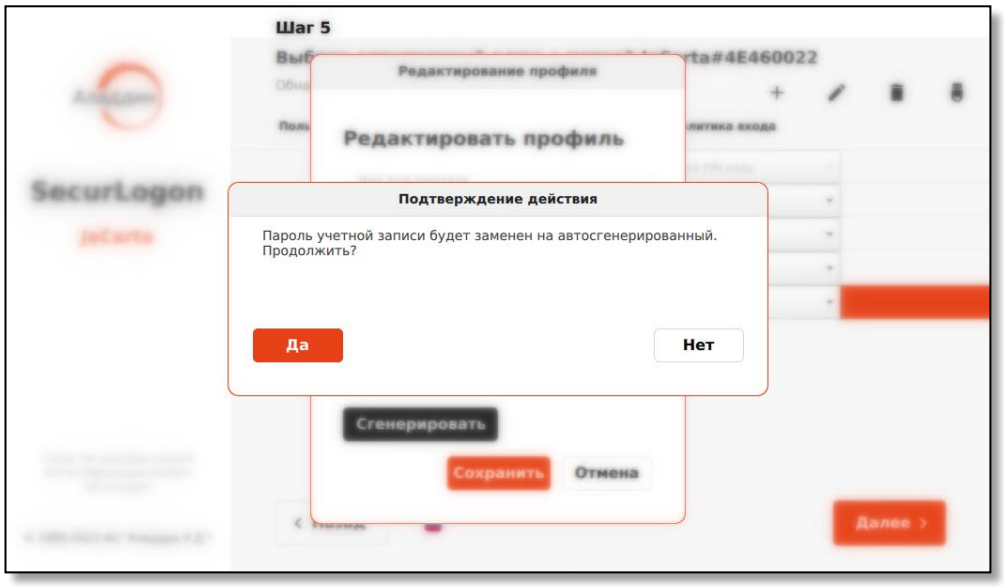

Рисунок 88 – Окно подтверждения смены пароля доменной учётной записи пользователя на автосгенерированный

После подтверждения действия в открывшемся окне введите учётные данные доменного пользователя, профиль которого создается, и нажмите кнопку <Ок> для изменения текущего пароля на сгенерированный (см. Рисунок 89).

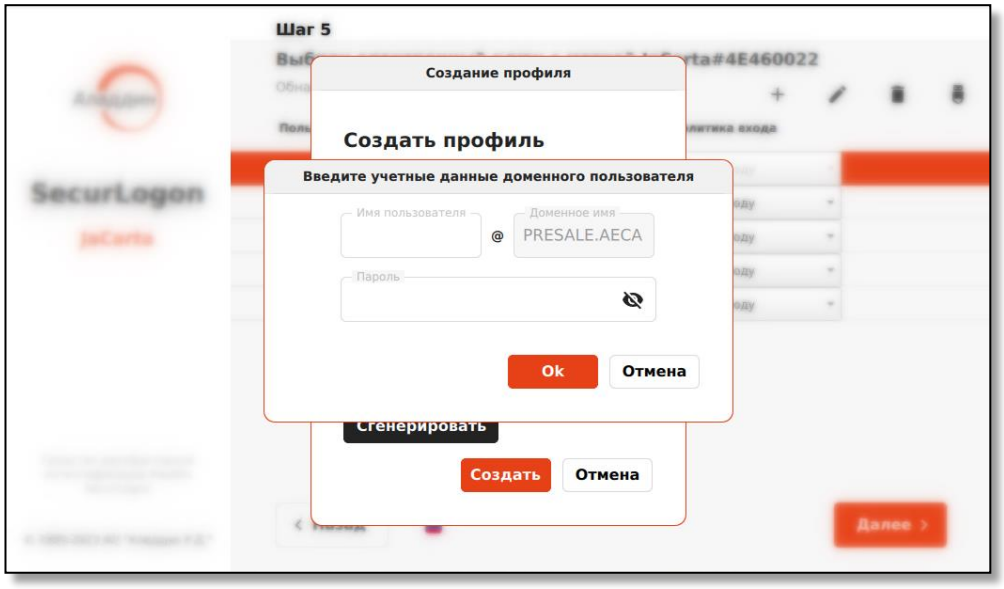

Рисунок 89 – Окно ввода учётных данных доменного пользователя

В случае неудачной попытки проверки учётных данных доменного пользователя уполномоченный пользователь будет уведомлён об ошибке (см. Рисунок 90).

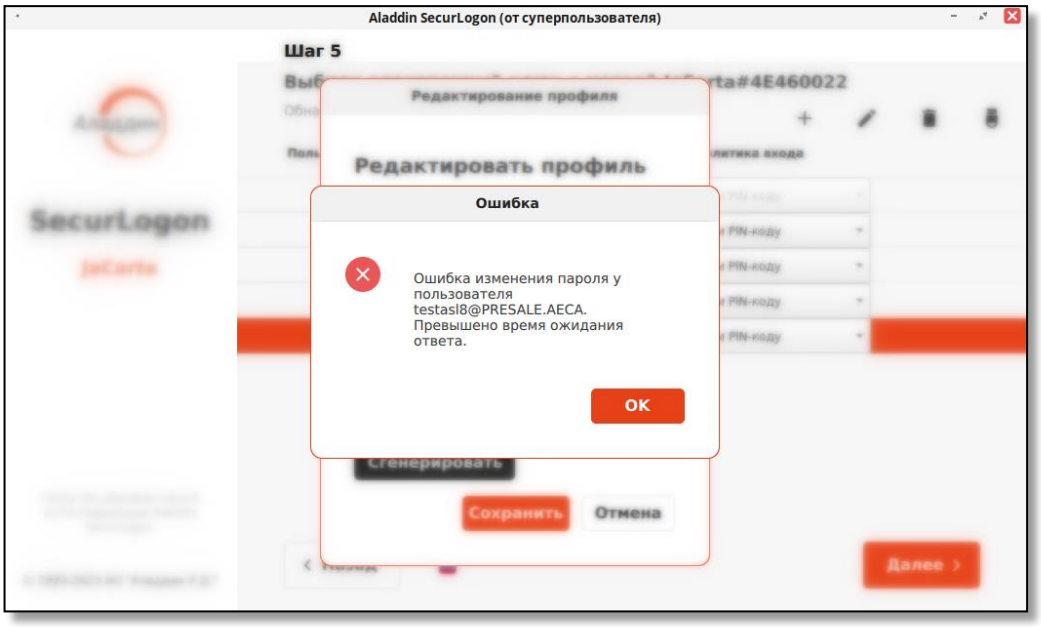

Рисунок 90 – Окно уведомления об ошибке ввода учётных данных доменного пользователя

В случае успешной проверки учётных данных доменного пользователя пароль в системе будет изменён на автосгенерированный и уполномоченный пользователь будет уведомлён об успехе операции (см. Рисунок 91).

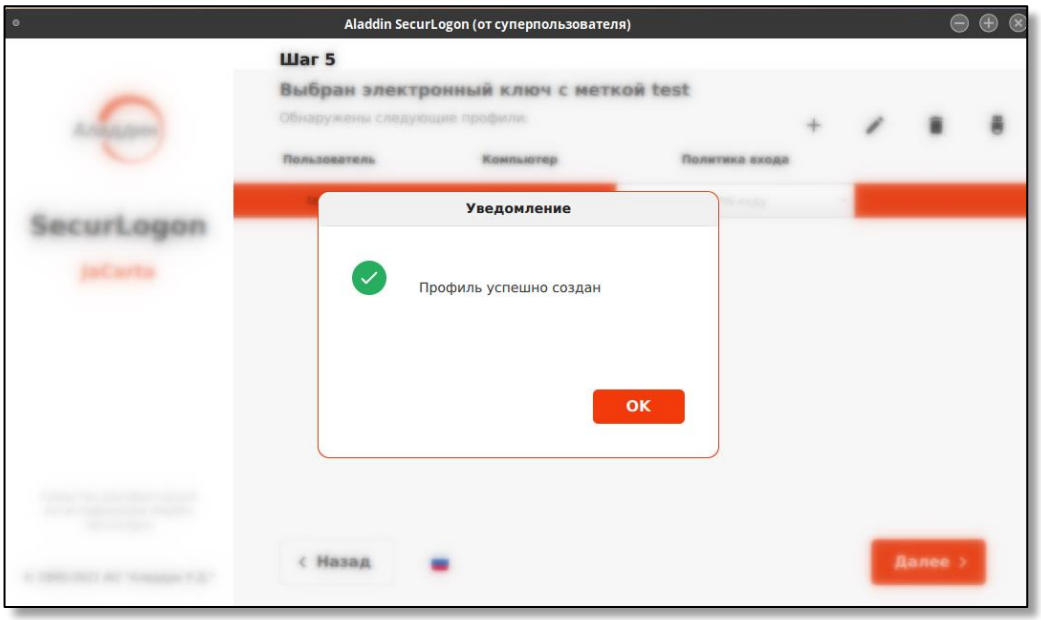

Рисунок 91 – Окно уведомления об успешном создании профиля

8.2.1.6.2 Редактирование выбранного профиля

Для редактирования выбранного профиля на экранной форме шага 5 (см. Рисунок 37) нажмите на кнопку  , после чего, если ранее не был введен PIN-код, появится окно «Аутентификация» (см. Рисунок 86), где необходимо ввести PIN-код, и, если PIN-код верен, далее вы увидите окно «Редактирование профиля» (см. Рисунок 92).

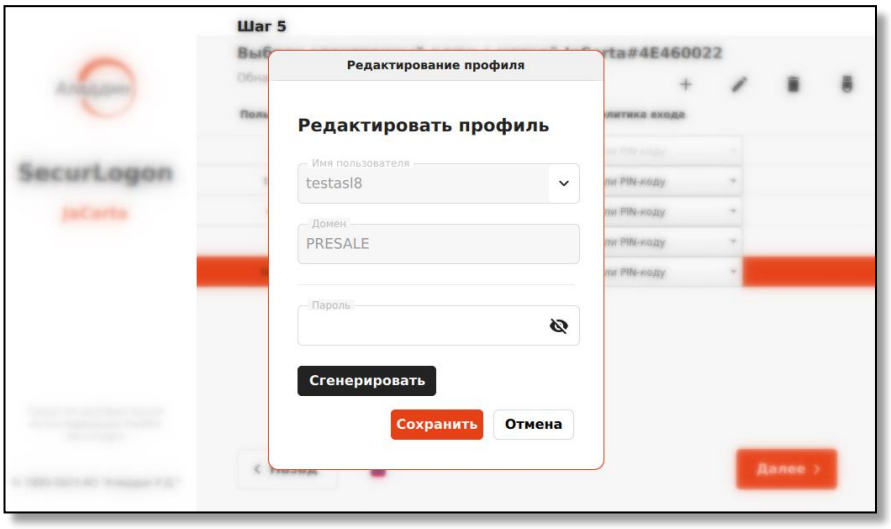

Рисунок 92 – Окно редактирования профиля

При редактировании профиля доступно:

- поле ввода пароля для задания пароля текущего профиля пользователя в соответствии с правилами, приведёнными в Приложении Б.
- автоматическая смена текущего пароля по кнопке <Сгенерировать>. При автоматической генерации пароля учётной записи доменного пользователя в появившемся окне необходимо ввести текущие учётные данные для замены пароля в системе на автосгенерированный (см. пункт «Создание нового профиля», подраздел 8.2.2.3 настоящего документа).

Нажмите кнопку <Сохранить>, профиль будет отредактирован.

Для выхода из режима редактирования профиля без сохранения изменений нажмите кнопку <Отмена>.

8.2.1.6.3 Удаление выбранного профиля

Для удаления выбранного профиля пользователя на экранной форме шага 5 (см. Рисунок 93) нажмите на кнопку  , после чего, если ранее не был введен PIN-код, появится окно «Аутентификация» (см. Рисунок 86), где необходимо ввести PIN-код, и, если PIN-код верен, далее:

- вы увидите окно подтверждения удаления профиля (см. Рисунок 93). При нажатии кнопки <Удалить> вы подтверждаете действие и профиль пользователя будет удален. Нажав кнопку <Нет> вы отменяете удаление профиля пользователя.

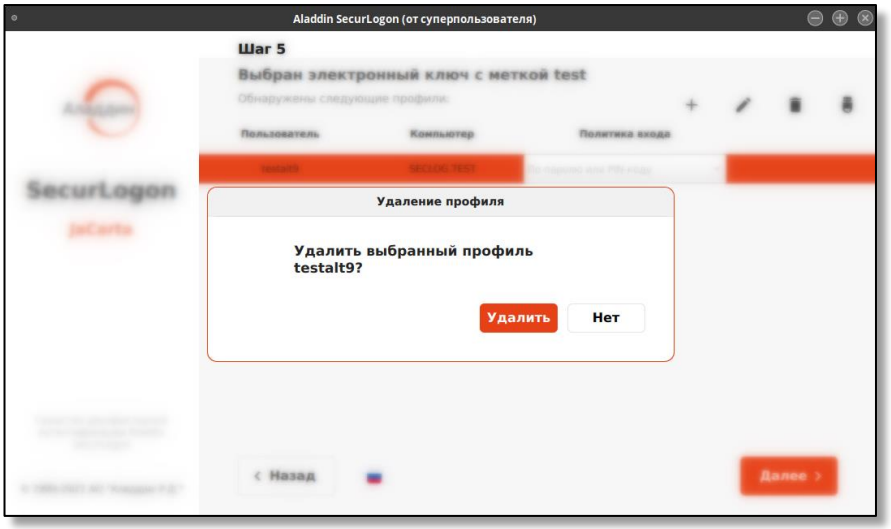

Рисунок 93 – Окно подтверждения удаления профиля пользователя при ручном вводе пароля

В случае успешного выполнения действия будет показано окно уведомления об успешной операции (см. Рисунок 94).

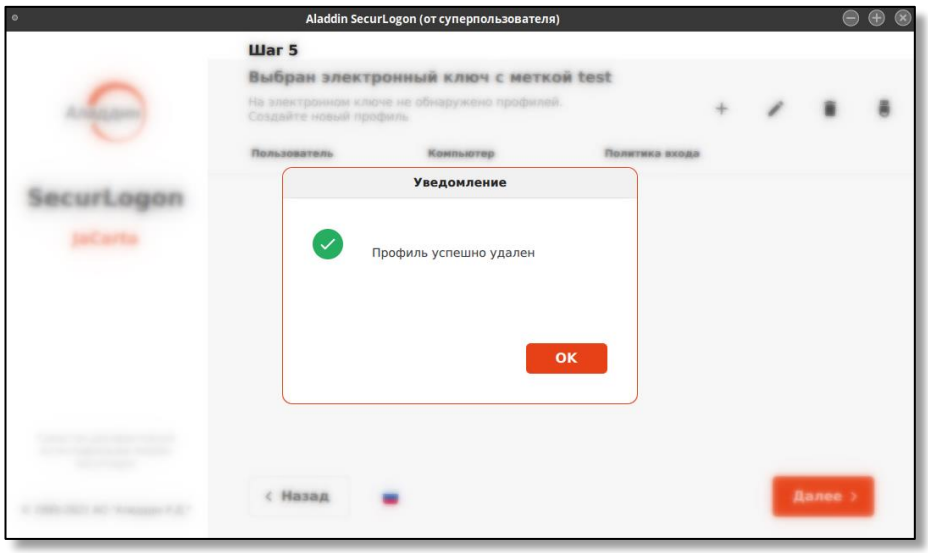

Рисунок 94 – Окно уведомления об успешном удалении профиля пользователя

8.2.1.6.4 Действия при извлечении электронного ключа

Для настройки действия при извлечении электронного ключа из разъёма нажмите кнопку на панели управления сертификатами (см. Рисунок 52) и выберете нужное действие:

- бездействие – при извлечении электронного ключа ничего не произойдет, текущий сеанс продолжается в штатном режиме;
- блокировать сессию пользователя – при извлечении электронного ключа активный сеанс пользователя будет заблокирован;
- выключить компьютер – при извлечении электронного ключа активный сеанс и все процессы будут завершены.

Если у пользователя настроена политика входа «Только по паролю», то двухфакторная аутентификация в этом случае не используется. Поэтому, вне зависимости от настроенного действия, при извлечении электронного ключа ничего не произойдет.

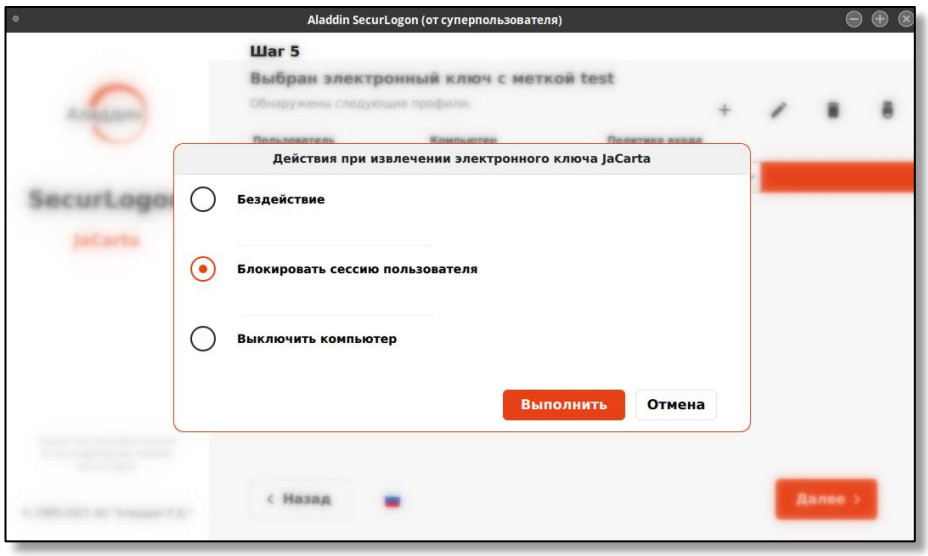

Рисунок 95 – Окно выбора действия при извлечении электронного ключа

Подтвердите действие, нажав кнопку <Выполнить>, при успешном сохранении выбора действия при извлечении электронного ключа вы увидите уведомление об успехе операции.

Также настройку действия при извлечении электронного ключа можно выполнить на финальном этапе настройки двухфакторной аутентификации.

После окончания работы с профилями пользователей нажмите на экранной форме шага 5 (см. Рисунок 82) кнопку <Далее>.

8.2.1.7 Настройка смены пароля и OTP аутентификации

Перед переходом на следующий шаг будет выведено окно с предложением установить автоматическую смену пароля пользователя домена, для профиля которого происходит настройка двухфакторной аутентификации (см. Рисунок 96).

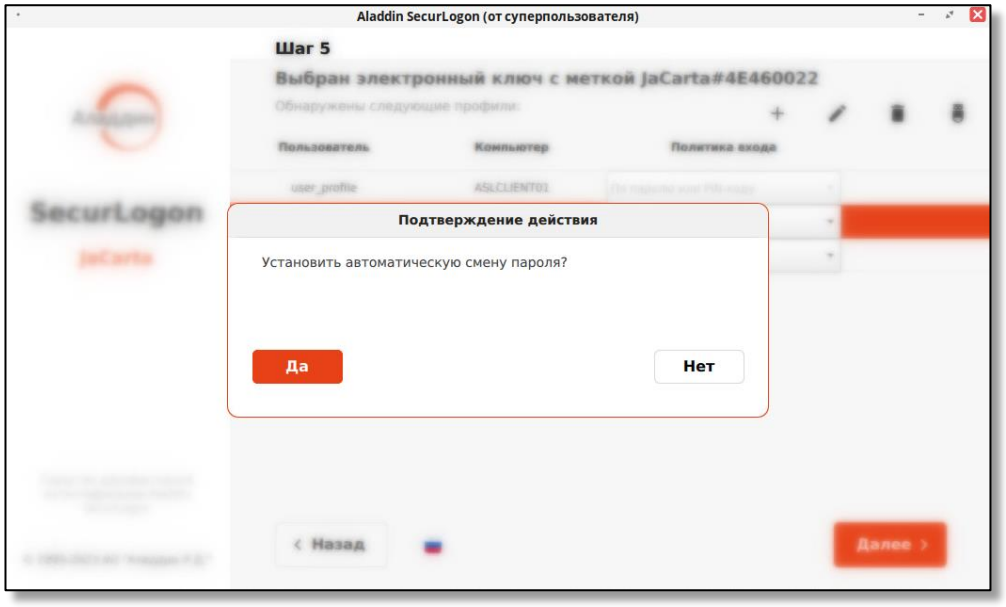

Рисунок 96 – Окно подтверждения действия по установке смены пароля

В случае выбора автоматической смены пароля пользователя домена, по нажатию на кнопку <Да>, необходимо ввести данные администратора домена в открывшемся окне (см. Рисунок 97).

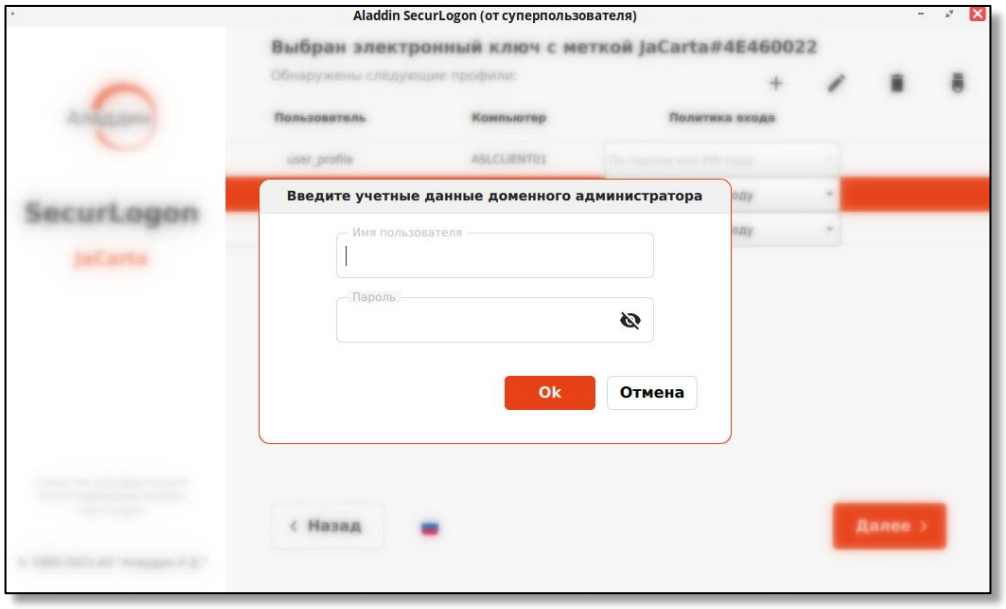

Рисунок 97 – Окно ввода данных администратора домена

В случае ввода некорректных данных администратора домена, пользователь будет уведомлён об этом и возвращён на 5 шаг.

При корректном вводе учётных данных администратора домена происходит установка автоматической смены пароля учётной записи доменного пользователя в соответствии с заданным интервалом в домене в фоновом режиме.

После успешной настройки автоматической смены пароля или отказа от неё по нажатию на кнопку <Нет> в следующем окне будет предложено дополнительно установить OTP-аутентификацию (см. Рисунок 98).

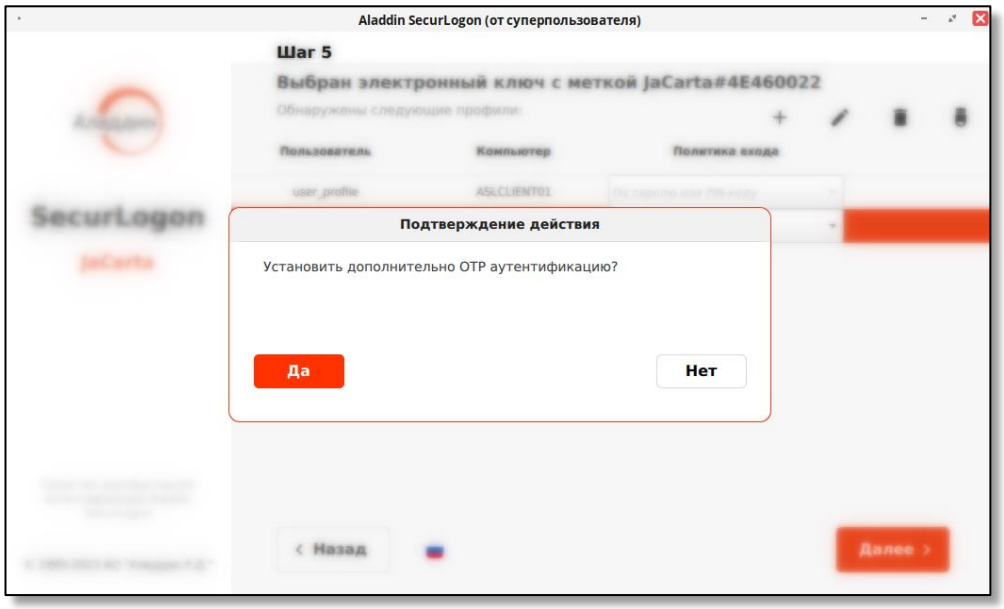

Рисунок 98 – Окно подтверждения действия при установке OTP-аутентификации

По нажатию на кнопку <Да> происходит переход к следующему шагу настройки OTP-аутентификации (описание полей окна см. в пункте 8.2.3) (см. Рисунок 99).

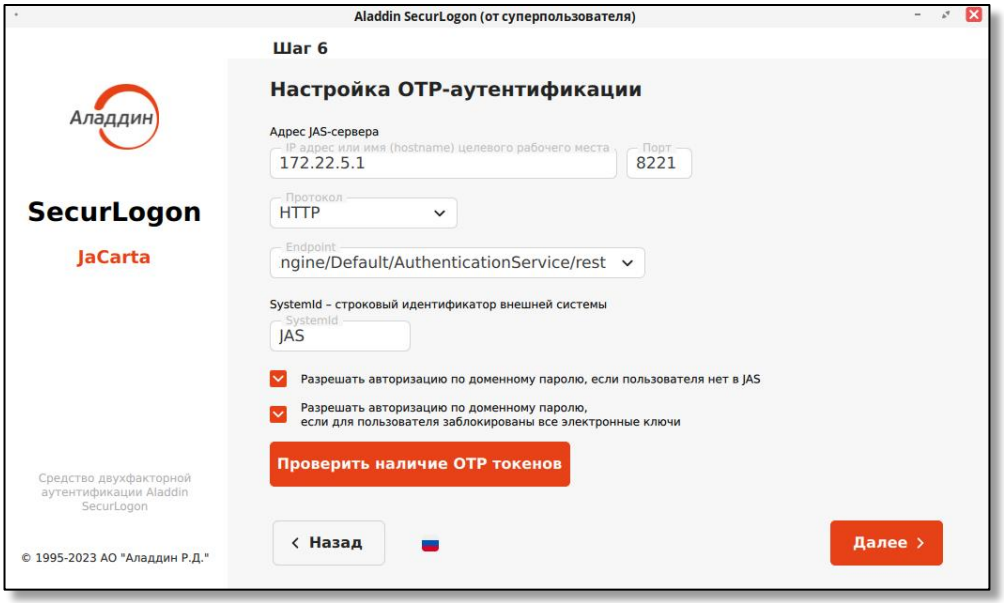

Рисунок 99 – Окно настройки OTP-аутентификации

8.2.1.8 Завершение настройки усиленной аутентификации

После завершения настройки OTP-аутентификации или в случае отказа от неё осуществляется переход на следующий шаг настройки локальной двухфакторной аутентификации (см. Рисунок 100).

На данном шаге возможно настроить действие при извлечении электронного ключа из разъема ПК, выбрав нужное значение на экранной форме шага 6.

Также можно применить тему SecurLogon (см. Приложение А) для входа пользователя в систему перед началом сеанса.

Все изменения будут применены по нажатию на кнопку <Завершить> и перезагрузке компьютера.

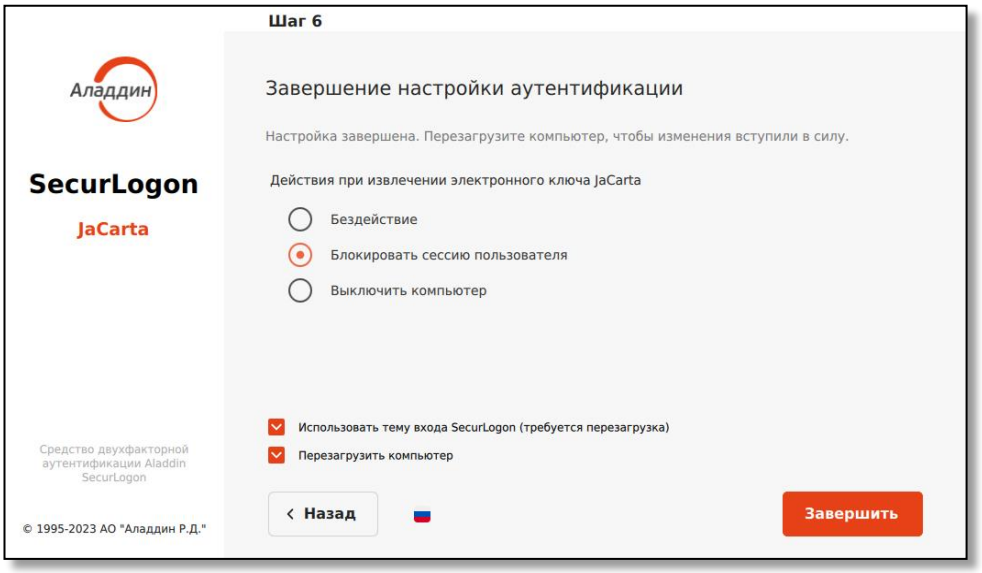

Рисунок 100 – Окно настройки сетевой аутентификации без использования PKI. Шаг 6

8.2.2 OTP

На данном шаге должен быть настроен JAS сервер, предоставляющий возможность аутентификации пользователей с помощью одноразовых паролей в организации.

На шаге 3 (см. Рисунок 101) выбираем способ входа в систему <OTP>. Для перехода к следующему шагу нажмите кнопку <Далее>.

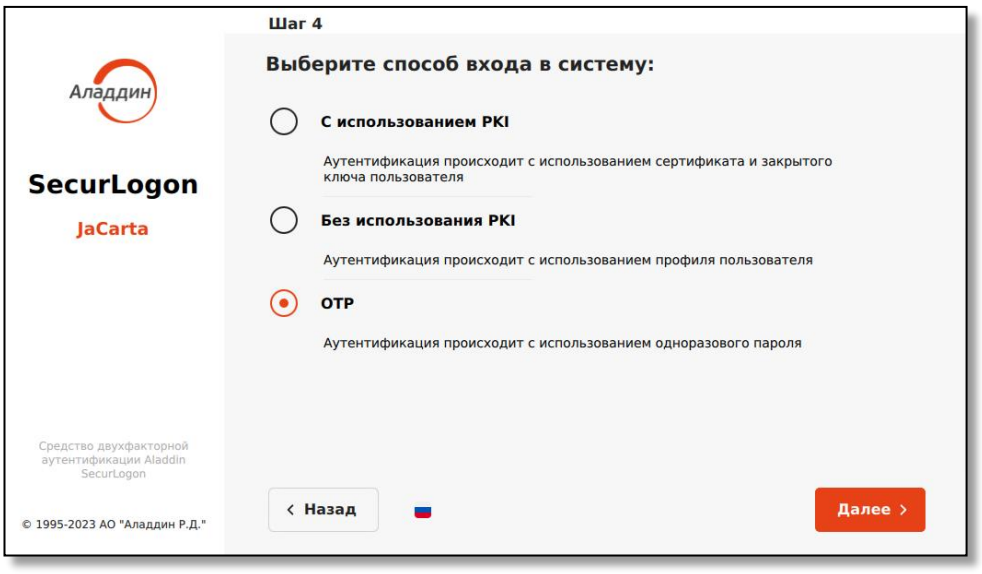

Рисунок 101 – Окно настройки сетевой аутентификации с использованием OTP. Шаг 3

8.2.2.1 Настройка аутентификации One Time Password

На следующем шаге в появившемся окне заполните поля (см. Рисунок 92):

- «адрес JAS-сервера» - по умолчанию заполняется адресом контроллера домена, если JAS-сервер расположен по другому адресу, то необходимо записать в данное поле ip-адрес JAS-сервера или полное имя сервера JAS, указанное в параметре «ServerUri»;
- «порт» – по умолчанию настроен 8221 порт;
- «протокол» - выберите тип протокола HTTP или HTTPS в зависимости от установленного по умолчанию протокола в адресе «ServerUri» JAS сервера;
- «endpoint» - точка подключения к интерфейсу аутентификации JAS;
- «System ID» - строковый идентификатор внешней системы, для которой осуществляется аутентификация пользователя посредством Messaging-токена. Один пользователь не может иметь более одного Messaging-токена для одной внешней системы. Если данный параметр не задан на сервере JAS, то оставляем заданное значение по умолчанию;
- чек-бокс «разрешать авторизацию по доменному паролю, если пользователя нет в JAS»;
- чек-бокс «разрешать авторизацию по доменному паролю, если для пользователя заблокированы все токены».

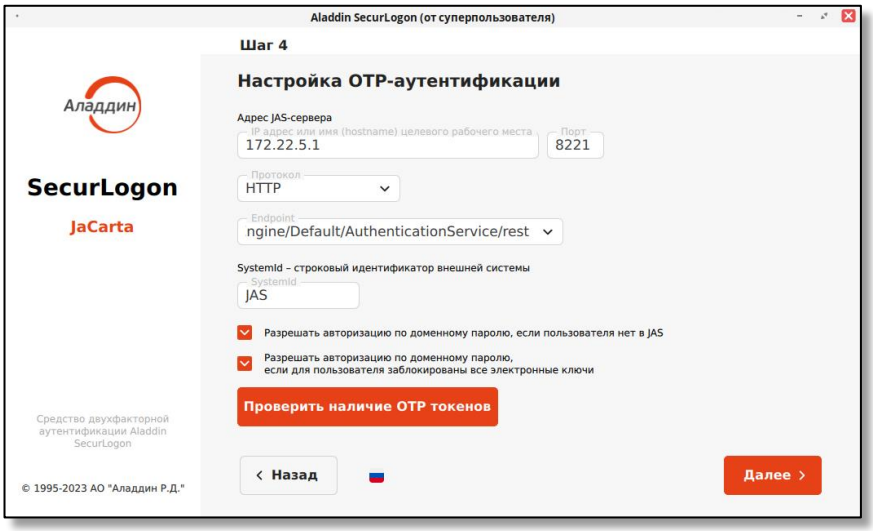

Рисунок 102 – Окно настройки сетевой аутентификации с использованием OTP. Шаг 4

По кнопке <Проверить наличие OTP токенов> в открывшемся окне введите имя пользователя и выберите тип OTP-токена, наличие которого необходимо проверить в настройках JAS-сервера для указанного пользователя (см. Рисунок 103). Перед началом проверки необходимо ввести верные адрес JAS-сервера и порт в соответствующих полях на текущем шаге.

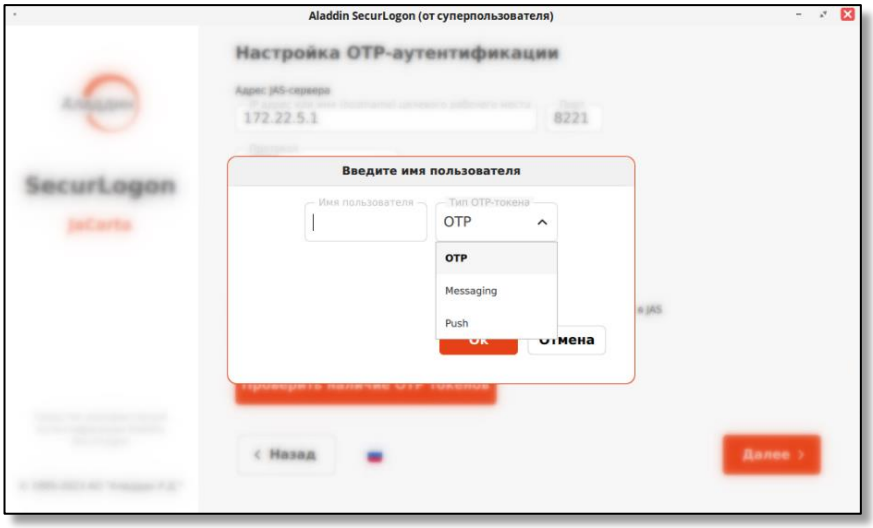

Рисунок 103 – Окно проверки наличия OTP для пользователя

Для настройки OTP-аутентификации и перехода к следующему шагу нажмите кнопку <Далее>.

8.2.2.2 Завершение настройки аутентификации

После окончания настройки сетевой аутентификации с OTP осуществляется переход на следующий шаг настройки сетевой двухфакторной аутентификации (см. Рисунок 93). Также можно применить тему SecurLogon (см. Приложение А) для входа пользователя в систему перед началом сеанса. Все изменения будут применены по нажатию на кнопку <Завершить> и перезагрузке компьютера.

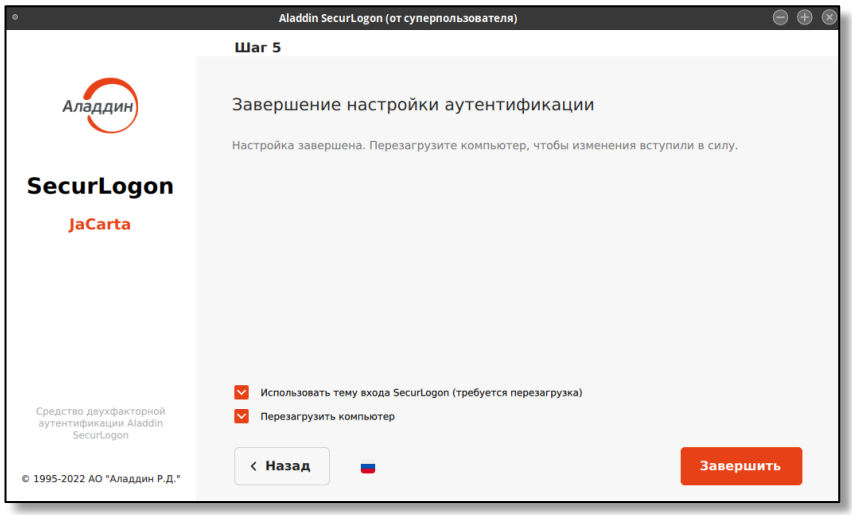

Рисунок 104 – Окно настройки сетевой аутентификации с использованием OTP. Шаг 5

8.2.3 Отключение сетевой аутентификации

Чтобы изменить ранее настроенную локальную двухфакторную аутентификацию:

- запустите программу;
- выполните аутентификацию путем ввода пароля администратора cbcntvs (см. Рисунок 8);
- в приветственном окне (см. Рисунок 9), нажмите кнопку <Далее>;
- в окне шага 1 выберите способ аутентификации «Сетевая», нажмите кнопку <Далее>;
- в окне шага 2 (см. Рисунок 70) выберите действие «Отключить вход в систему по электронному ключу», нажмите кнопку <Далее>, после чего на экране появится окно «Подтверждение действия» (см. Рисунок 95), в данном окне необходимо отклонить изменения, нажав кнопку <Нет> или подтвердить отключение аутентификации, нажав кнопку <Да>.

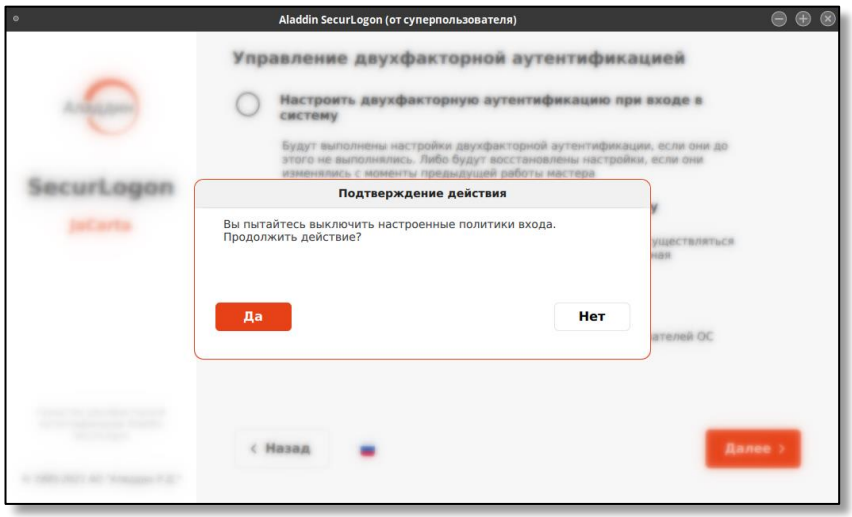

Рисунок 105 – Окно подтверждения отключения сетевой двухфакторной аутентификации

Далее осуществляется автоматический переход к завершению отключения аутентификации (см. Рисунок 106).

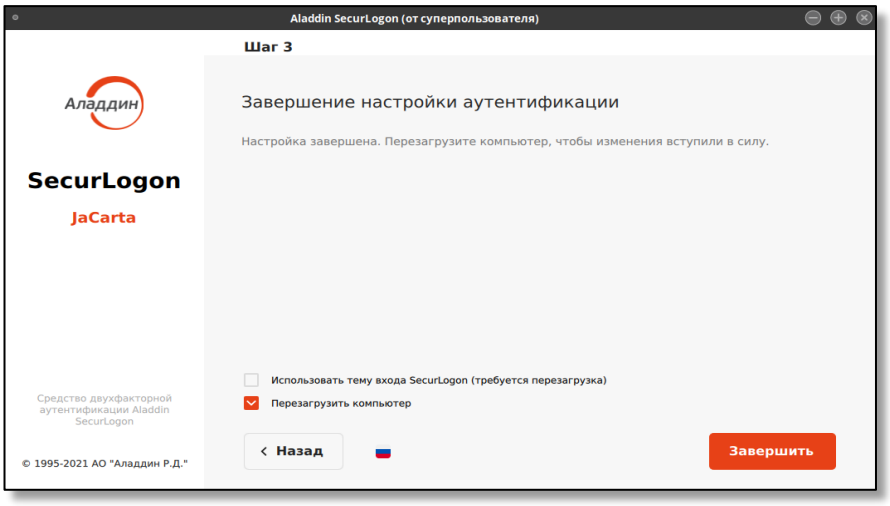

Рисунок 106 – Окно завершения отключения сетевой аутентификации

На форме «Завершение настройки аутентификации», чтобы завершить операцию нажмите кнопку <Завершить>.

8.2.4 Управление политиками входа

- Для настройки политики входа создайте на контроллере домена следующие группы:
  - jc_net_pin – группа пользователей, входящих в систему по pin-коду электронного ключа;
  - jc_net_pass – группа пользователей, входящая в систему по паролю.
- Для изменения ранее настроенных политик входа пользователей на шаге 2 (см. Рисунок 70) выбираем способ управления двухфакторной аутентификацией «Управление политиками входа». Для перехода к следующему шагу нажмите кнопку <Далее>.

8.2.4.1 Управление политиками сетевой аутентификации с PKI (с использованием электронного ключа)

В поле диалогового окна шага 3 (см. Рисунок 107) показаны все приложения, записанные на подсоединенном электронном ключе. Выберите нужное приложение и нажмите кнопку <Далее> для продолжения действий по изменению политики входа.

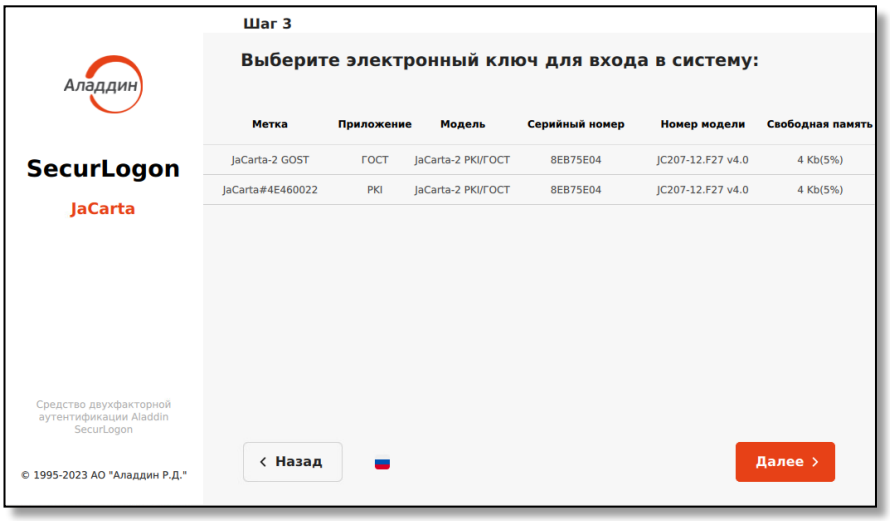

Рисунок 107 – Окно управления политиками входа учетных записей с использованием электронного ключа. Шаг 3

В диалоговом окне шага 4 (см. Рисунок 108) показаны все профили, которые записаны на электронном ключе. Дальнейшие действия по настройке политики входа повторяют действия, описанные в пункте 1.1.1 для сетевой аутентификации с использованием PKI.

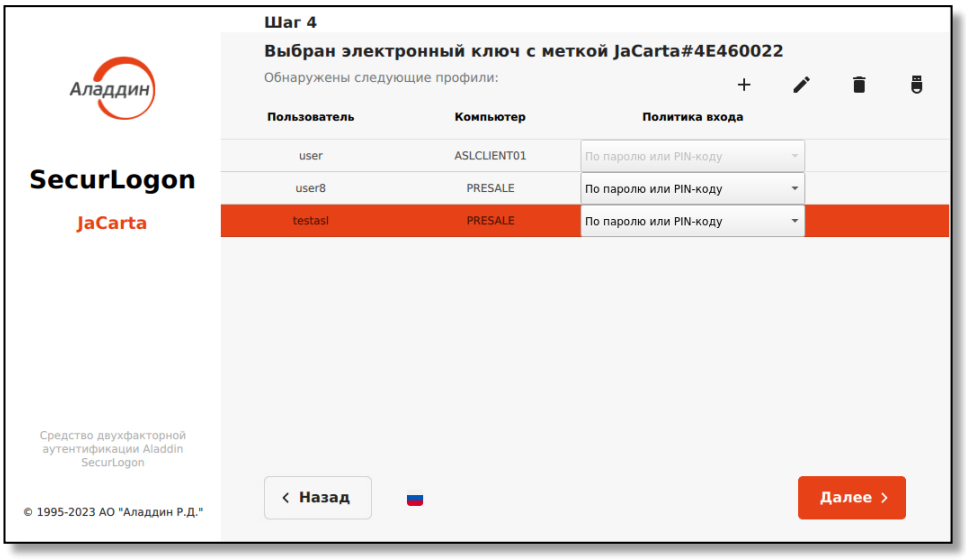

Рисунок 108 – Окно управления политиками входа учетных записей с использованием электронного ключа. Шаг 4

После настройки политики входа будет осуществлен переход к окну завершения настройки аутентификации. Все изменения будут применены после перезагрузки ПК.

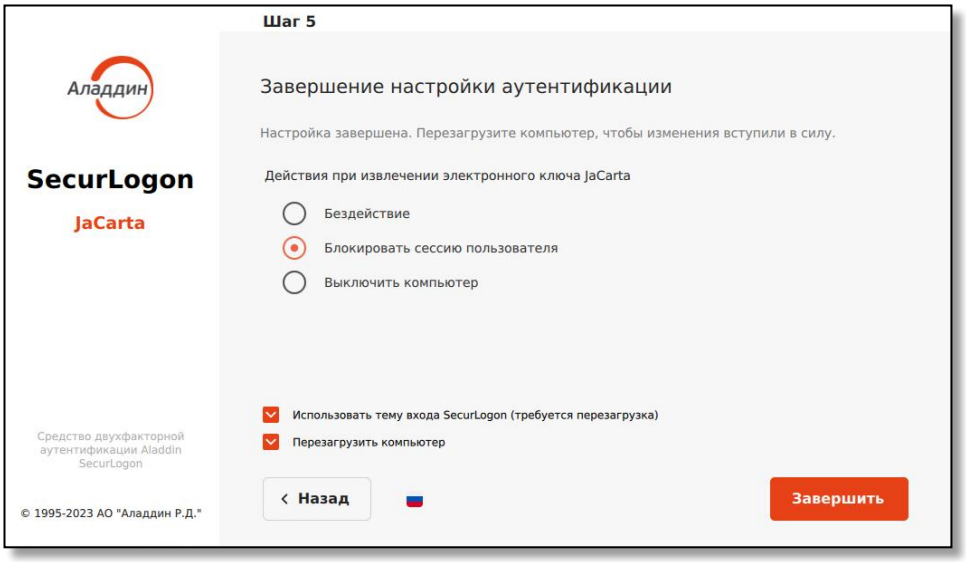

Рисунок 109 – Окно завершения управления политиками входа для сетевой аутентификации

8.3 Настройка удалённой аутентификации по протоколу RDP

Если на первом шаге настройки аутентификации (см. Рисунок 15) выбран способ «Удаленный доступ» по протоколу RDP, то осуществляется переход на второй шаг.

8.3.1 Строгая аутентификация

На данном шаге к настраиваемому ПК должен быть подсоединен электронный ключ.

В памяти электронного ключа может быть установлено одно или несколько приложений.

- На втором шаге в окне настройки удаленного доступа (см. Рисунок 110) выбираем способ входа в систему <С использованием PKI>. Для перехода к следующему шагу нажмите кнопку <Далее>.

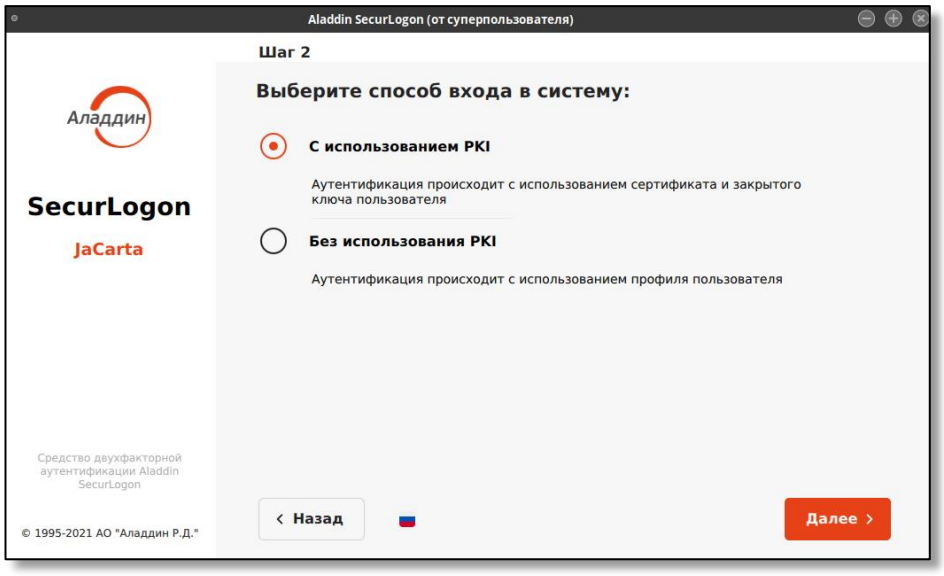

Рисунок 110 - Окно настройки удаленного доступа с использованием PKI. Шаг 2

8.3.1.1 Выбор электронного ключа

В поле диалогового окна шага 3 (см. Рисунок 111) показаны все записанные приложения на подключенном электронном ключе, в столбцах указана следующая информация для каждого приложения:

- в столбце «метка приложения» указано название электронного ключа (имя токена);
- в столбце «приложение» указано название приложения, установленного в память электронного ключа, определяющее функциональность модели электронного ключа;
- в столбце «модель» указана модель электронного ключа;
- в столбце «серийный номер» указан 8-значный серийный номер электронного ключа;
- в столбце «номер модели» указана модель электронного ключа;
- в столбце «свободная память» указано свободное место на электронном ключе в Кбайтах и % от общего объема электронного ключа.

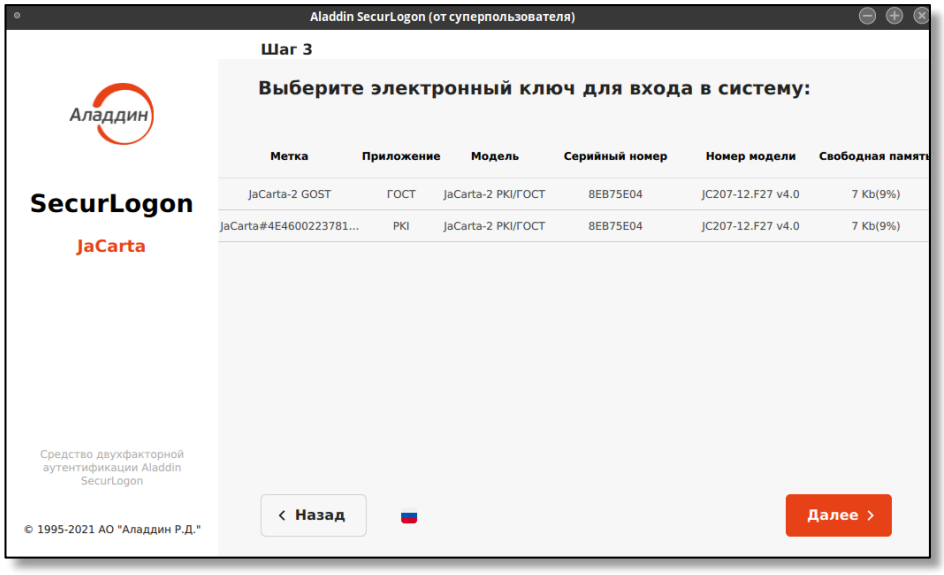

Рисунок 111 - Окно настройки удаленного доступа с использованием PKI. Шаг 3

Выберите нужное приложение и нажмите кнопку <Далее>.

8.3.1.2 Настройка удаленного доступа для аутентификации

В диалоговом окне шага 4 (см. Рисунок 112) отображены:

- поле ввода IP-адреса или имени ПК, к которому происходит подключение, с указанием номера порта для подключения по протоколу RDP, по умолчанию используется порт TCP 3389;
- поле для указания пути сохранения ярлыка. Возможен ввод пути с клавиатуры или, нажав кнопку <Обзор>, выбрать нужную папку для сохранения ярлыка запуска подключения по RDP к удаленному ПК;

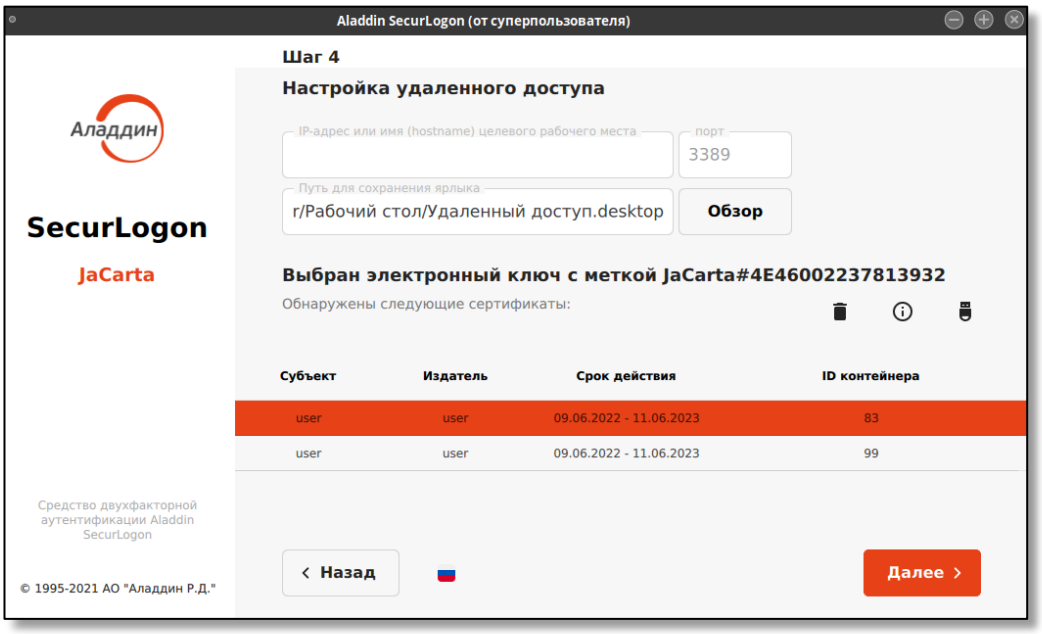

Рисунок 112 - Окно настройки удаленного доступа с использованием PKI. Шаг 4

- в табличной форме отображены все имеющиеся сертификаты для выбранного на предыдущем шаге приложения. В столбцах экранной формы для каждого сертификата отображена следующая информация:
  - имя субъекта;
  - издатель;
  - срок действия сертификата;
  - ID контейнера.
- На текущей экранной форме расположена панель управления сертификатами (см. Рисунок 113).

Рисунок 113 – Панель управления сертификатами при удаленном доступе с использованием PKI

На данной панели представлены следующие возможности:

 - просмотр данных выбранного сертификата;

 - удаление выбранного сертификата;

 - настройка действия при извлечении электронного ключа.

8.3.1.2.1 Просмотр данных сертификата

Для просмотра информации о сертификате пользователя на панели управления сертификатами (см. Рисунок 113) нажмите кнопку  , после чего появится окно <О сертификате> (см. Рисунок 114).

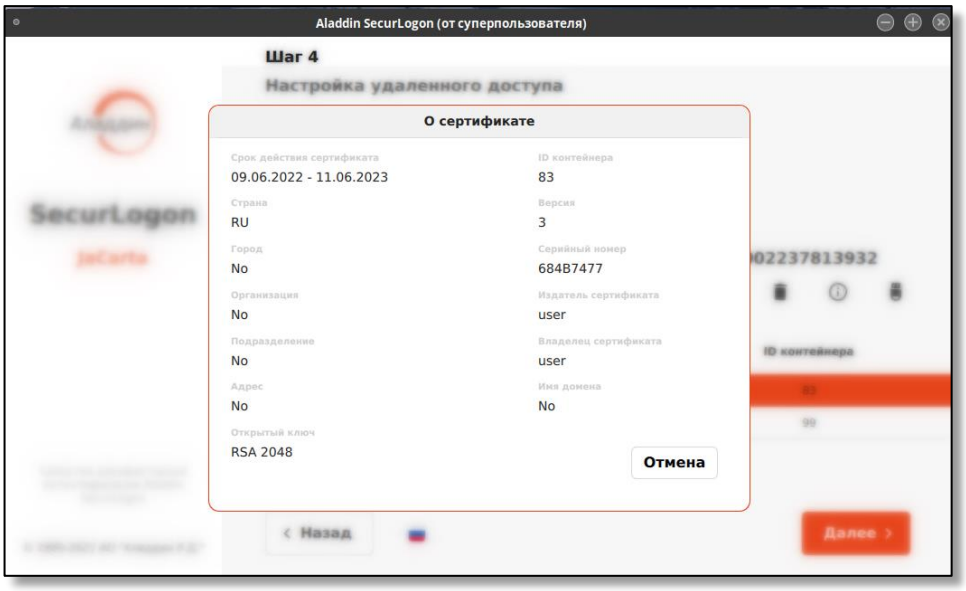

Рисунок 114 – Окно просмотра сведений о сертификате

Нажмите кнопку <Отмена>, для закрытия окна.

8.3.1.2.2 Удаление сертификата

Для удаления сертификата с электронного ключа, на панели управления сертификатами (см. Рисунок 113) нажмите на кнопку , после чего, если ранее не был введен PIN-код, появится окно <Аутентификация>, где необходимо ввести PIN-код электронного ключа, и, если PIN-код верен, то далее вы увидите окно подтверждения удаления сертификата (см. Рисунок 115).

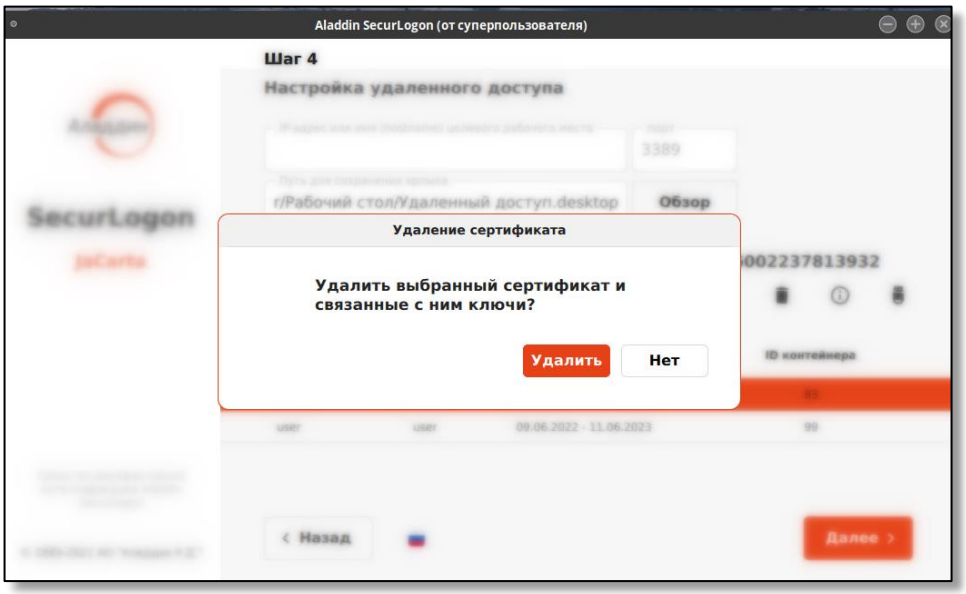

Рисунок 115 – Окно подтверждения удаления сертификата

Подтвердите удаление сертификата нажатием на кнопку <Удалить>, при успешном удалении сертификата вы увидите уведомление об успехе операции (см. Рисунок 116).

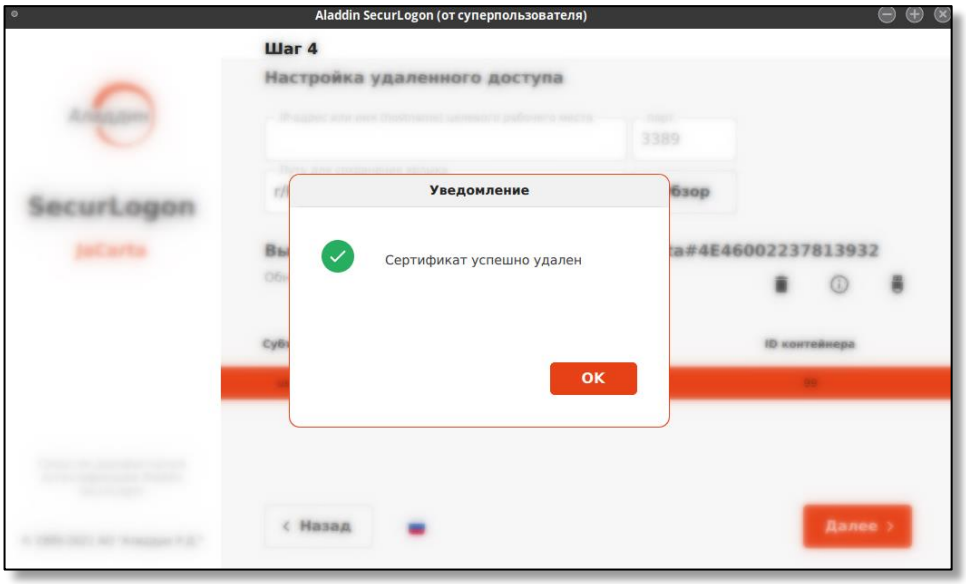

Рисунок 116 – Окно уведомления об успешном удалении сертификата

8.3.1.2.3 Действия при извлечении электронного ключа

Для настройки действия при извлечении электронного ключа из разъёма нажмите кнопку на панели управления сертификатами (см. Рисунок 113) и выберете нужное действие (см. Рисунок 117):

- бездействие – при извлечении электронного ключа ничего не произойдет, текущий сеанс продолжается в штатном режиме;
- закрывать удаленное подключение – при извлечении электронного ключа подключение к удаленному компьютеру будет закрыто.

Также настройку действия при извлечении электронного ключа можно выполнить на финальном этапе настройки двухфакторной аутентификации.

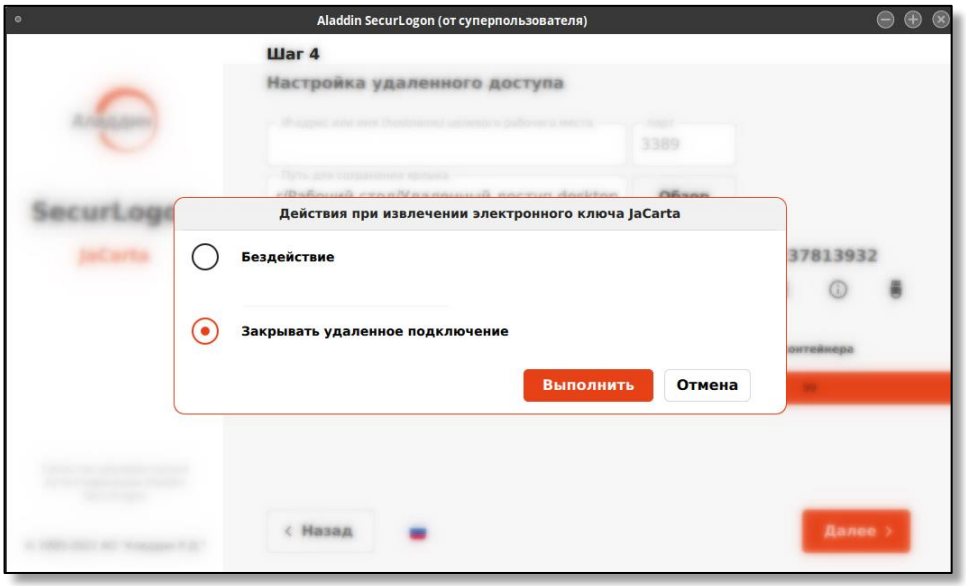

Рисунок 117 – Окно выбора действия при извлечении электронного ключа

Подтвердите действие, нажав кнопку <Выполнить>, при успешном сохранении выбора действия при извлечении электронного ключа вы увидите уведомление об успехе операции (см. Рисунок 118).

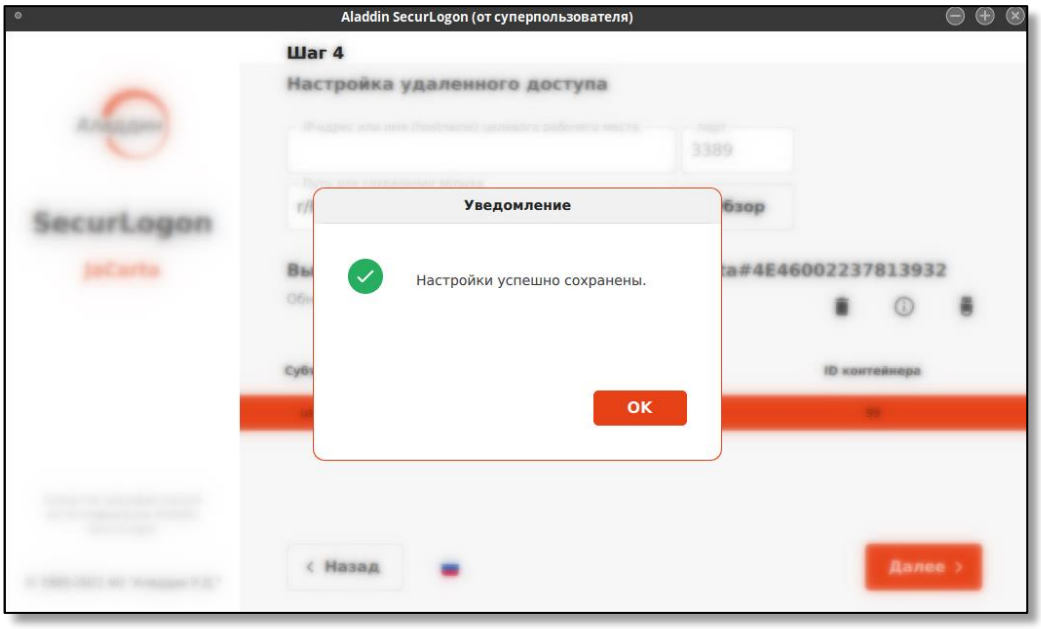

Рисунок 118 – Окно уведомления об успешном сохранении выбора действия при извлечении электронного ключа

После настройки полей шага 4 и выбора сертификата пользователя нажать кнопку <Далее> для перехода на следующий шаг. Администратор будет уведомлен о успешном создании ярлыка для запуска удаленной сессии (см. Рисунок 119).

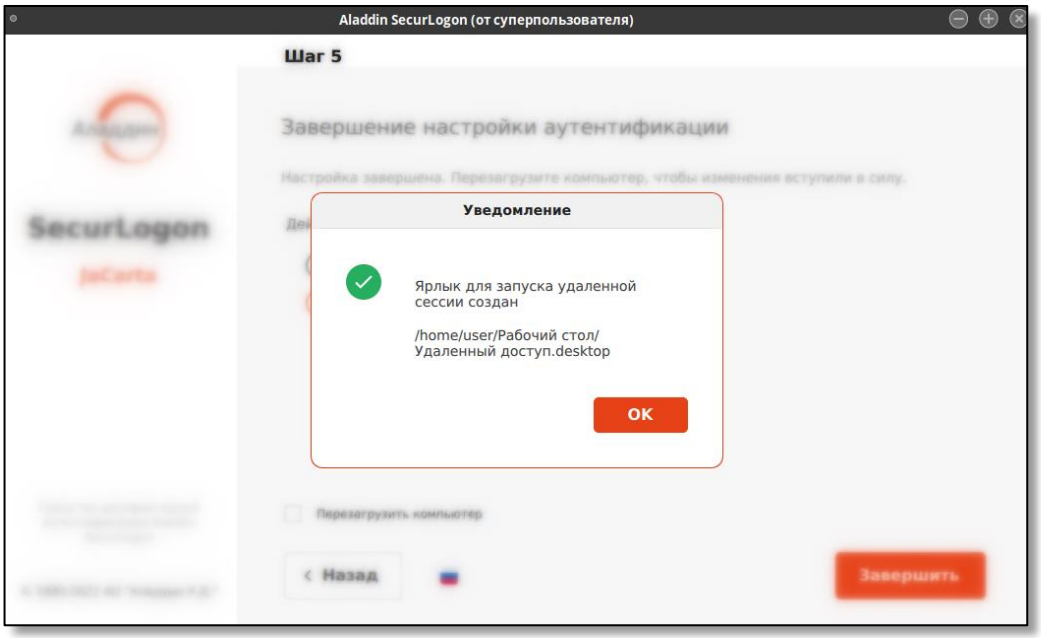

Рисунок 119 – Окно уведомления об успешном создании ярлыка для запуска удаленной сессии

8.3.1.3 Завершение настройки аутентификации при удаленном доступе

В диалоговом окне шага 5 для завершения настройки двухфакторной аутентификации необходимо выбрать действие при извлечении электронного ключа и перезагрузить компьютер для вступления изменений в силу, поставив галочку <Перезагрузить компьютер> и нажав кнопку <Завершить>.

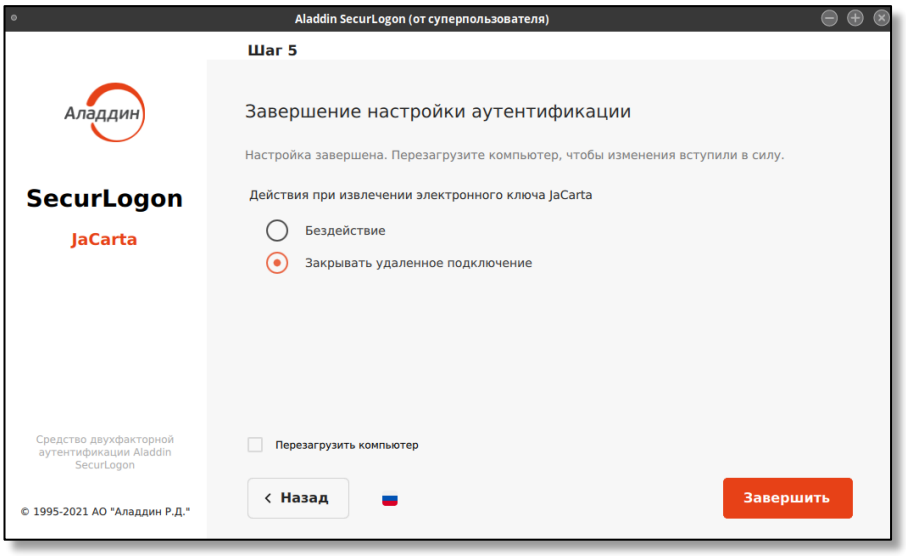

Рисунок 120 – Окно завершения настройки аутентификации при удаленном доступе

По завершению работы программы по указанному на шаге 4 пути появится ярлык запуска удаленного подключения (см. Рисунок 121).

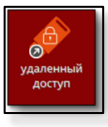

Рисунок 121 – Ярлык запуска удаленного подключения

Порядок действий пользователя при двухфакторной аутентификации на удаленном целевом компьютере приведен в «RU.АЛДЕ.03.12.010 34 01-1 Средство двухфакторной аутентификации Aladdin SecurLogon. Руководство оператора».

8.3.2 Усиленная аутентификация

На данном шаге к настраиваемому ПК должен быть подсоединен электронный ключ.

В памяти электронного ключа может быть установлено одно или несколько приложений.

- На втором шаге в окне настройки удаленного доступа (см. Рисунок 122) выбираем способ входа в систему <С использованием PKI>. Для перехода к следующему шагу нажмите кнопку <Далее>.

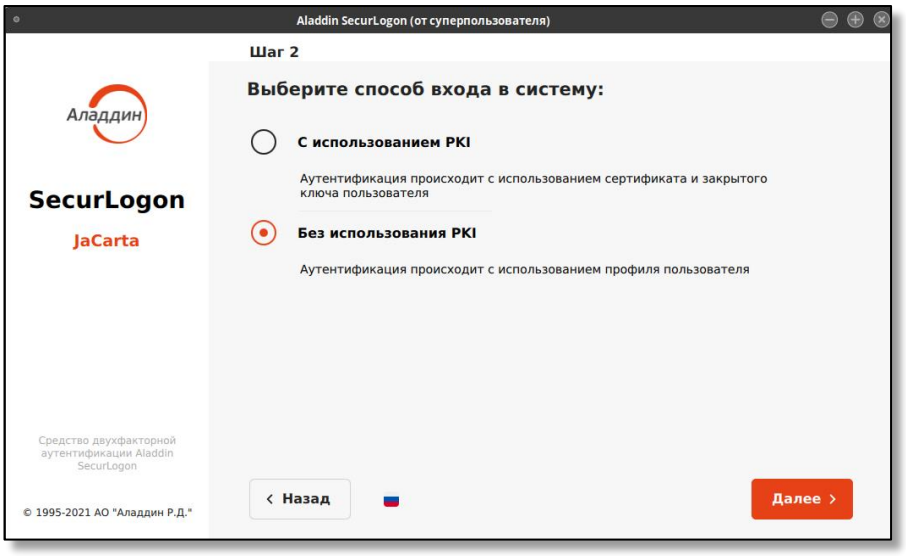

Рисунок 122 - Окно настройки удаленного доступа без использования PKI. Шаг 2

8.3.2.1 Выбор электронного ключа

В поле диалогового окна шага 3 (см. Рисунок 123) показаны все записанные приложения на подключенном электронном ключе, в столбцах указана следующая информация для каждого приложения:

- в столбце «метка приложения» указано название электронного ключа (имя токена);
- в столбце «приложение» указано название приложения, установленного в память электронного ключа, определяющее функциональность модели электронного ключа;
- в столбце «модель» указана модель электронного ключа;
- в столбце «серийный номер» указан 8-значный серийный номер электронного ключа;
- в столбце «номер модели» указана модель электронного ключа;
- в столбце «свободная память» указано свободное место на электронном ключе в Кбайтах и % от общего объема электронного ключа.

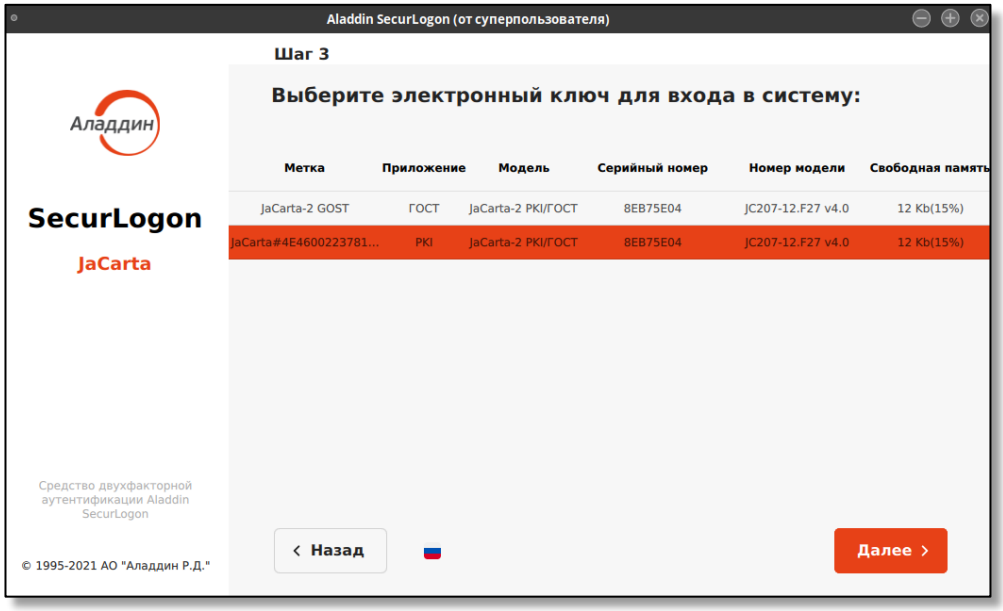

Рисунок 123 - Окно настройки удаленного доступа без использования PKI. Шаг 3

Выберите нужное приложение и нажмите кнопку <Далее>.

8.3.2.2 Настройка удаленного доступа для аутентификации

В диалоговом окне шага 4 (см. Рисунок 124) отображены:

- поле ввода IP-адреса или имени ПК, к которому происходит подключение, с указанием номера порта для подключения по протоколу RDP, по умолчанию используется порт TCP 3389;
- поле для указания пути сохранения ярлыка. Возможен ввод пути с клавиатуры или, нажав кнопку <Обзор>, выбрать нужную папку для сохранения ярлыка запуска подключения по RDP к удаленному ПК;

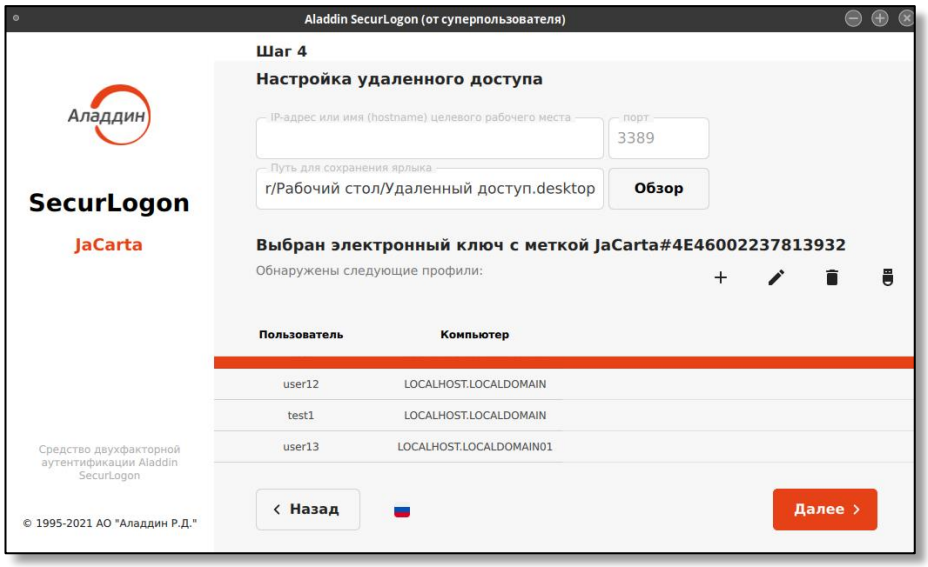

Рисунок 124 – Окно настройки удаленного доступа без использования PKI. Шаг 3

- в табличной форме отображены все имеющиеся профили для выбранного на предыдущем шаге приложения электронного ключа. В столбцах экранной формы для каждого профиля отображена следующая информация:
  - пользователь. В данном столбце отображены все профили пользователей, созданные на текущем электронном ключе;
  - компьютер. В этом столбце отображены имена компьютеров, для работы на которых настроены соответствующие профили пользователей;

На данном шаге 4 осуществляется выбор профиля пользователя и управление профилями пользователей посредством панели (см. Рисунок 125).

Рисунок 125 – Панель управления профилями

На данной панели представлены следующие возможности:

 - создание нового профиля;

 - редактирование данных выбранного профиля;

 - удаление выбранного профиля;

 - настройка действия при извлечении электронного ключа.

8.3.2.2.1 Создание нового профиля

Для создания нового профиля пользователя в панели управления профилями нажмите на кнопку  , после чего появится окно «Аутентификация» (см. Рисунок 126), в случае если ранее не была проведена аутентификация на выбранном электронном ключе.

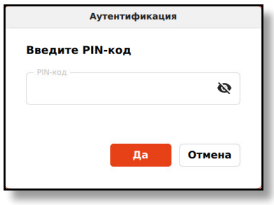

Рисунок 126 – Окно аутентификации для ввода ПИН-кода электронного ключа

Для авторизации на электронном ключе в окне “Аутентификация”, введите PIN-код пользователя. Количество попыток ввода PIN-кода пользователя определяется настройками электронного ключа.

После успешно введённого PIN-кода вы увидите окно “Создание нового профиля” (см. Рисунок 127).

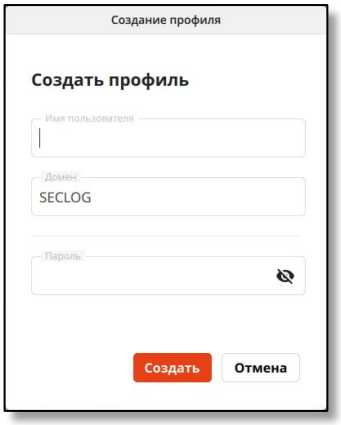

Рисунок 127 – Окно создания нового профиля

Заполните данные нового профиля, указав в соответствующих полях:

- имя пользователя – введите имя пользователя, совпадающее с учетной записью пользователя на ОС удаленного рабочего места;
- домен – домен, в котором находится удаленный ПК, к которому происходит подключение;
- пароль – пароль для текущего пользователя должен совпадать с паролем учетной записи удаленного ПК.

После ввода данных доменного пользователя, профиль которого создается, нажмите кнопку <Создать>. Уполномоченный пользователь будет уведомлён об успехе операции (см. Рисунок 128).

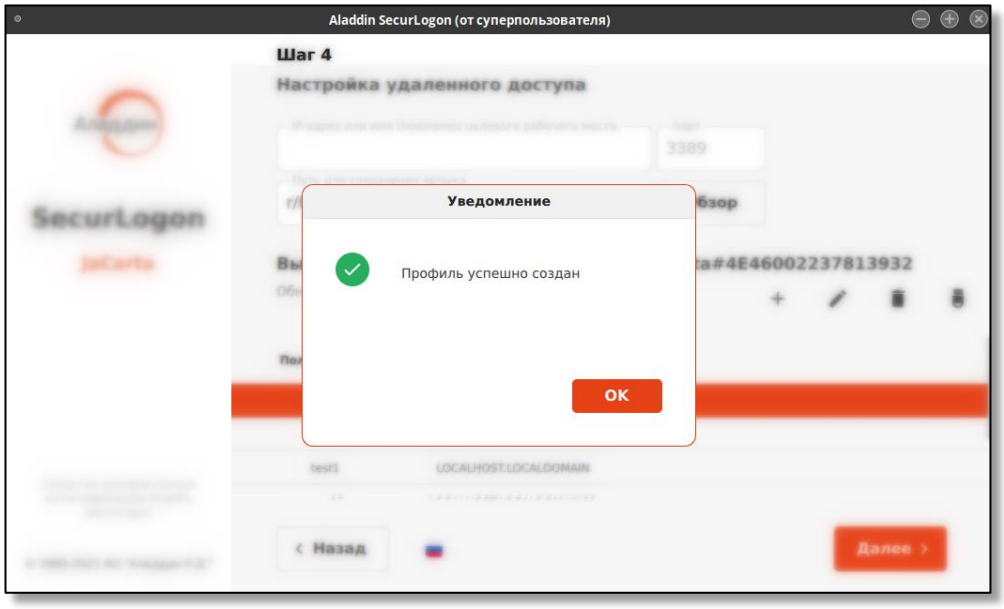

Рисунок 128 – Окно уведомления об успешном создании профиля

8.3.2.2.2 Редактирование выбранного профиля

Для редактирования выбранного профиля на экранной форме шага 4 (см. Рисунок 124) нажмите на кнопку  , после чего, если ранее не был введен PIN-код, появится окно “Аутентификация”, где необходимо ввести PIN-код, и, если PIN-код верен, далее вы увидите окно “Редактирование профиля” (см. Рисунок 129).

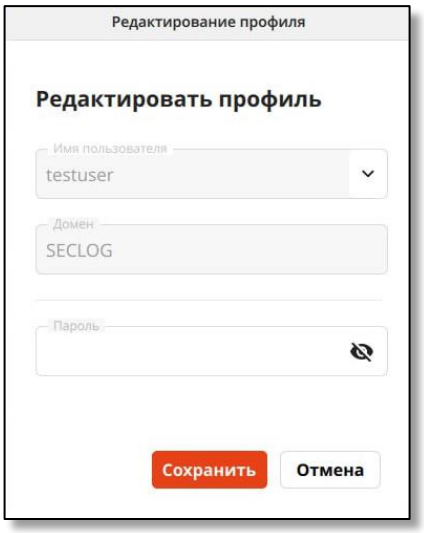

Рисунок 129 – Окно редактирования профиля

При редактировании профиля доступно поле:

- поле ввода пароля для смены текущего пароля профиля пользователя в соответствии с правилами, приведёнными в Приложении Б.

Нажмите кнопку <Сохранить>, профиль будет отредактирован. Для выхода из режима редактирования профиля без сохранения изменений нажмите кнопку <Отмена>.

8.3.2.2.3 Удаление выбранного профиля

Для удаления выбранного профиля пользователя на экранной форме шага 4 (см. Рисунок 124) нажмите на кнопку , после чего, если ранее не был введен PIN-код, появится окно «Аутентификация», где необходимо ввести PIN-код, и, если PIN-код верен далее вы увидите окно “Подтверждения удаления профиля” (см. Рисунок 130).

Далее, в окне подтверждения удаления профиля (см. Рисунок 130) нажмите кнопку <Удалить> для подтверждения действия и профиль пользователя будет удален, или нажмите кнопку <Нет> для отмены удаления профиля пользователя.

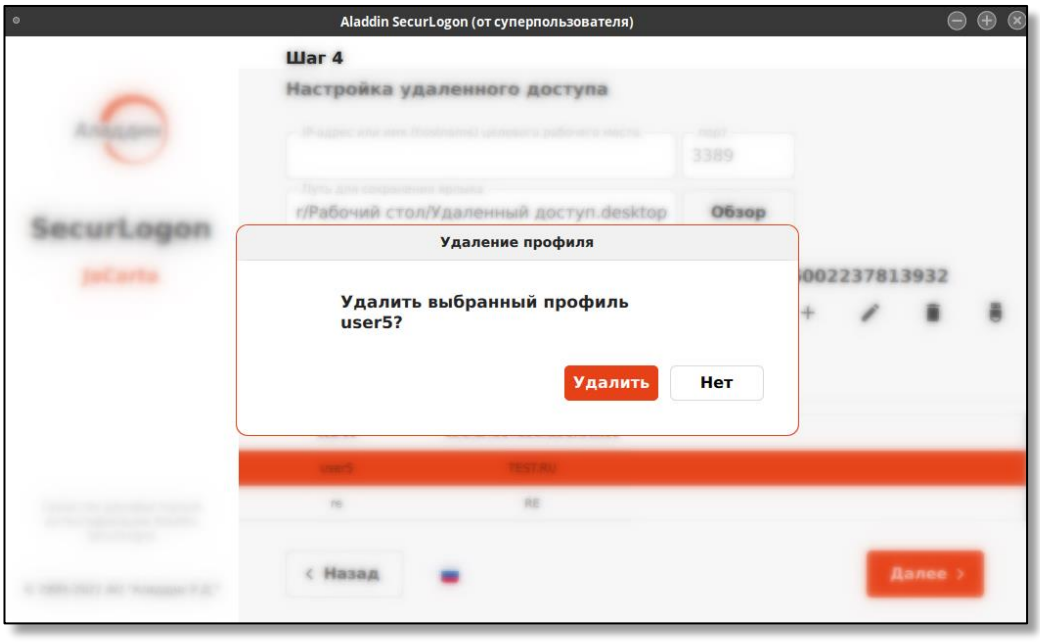

Рисунок 130 – Окно подтверждения удаления профиля пользователя

В случае успешного выполнения действия будет показано окно уведомления об успешной операции (см. Рисунок 51).

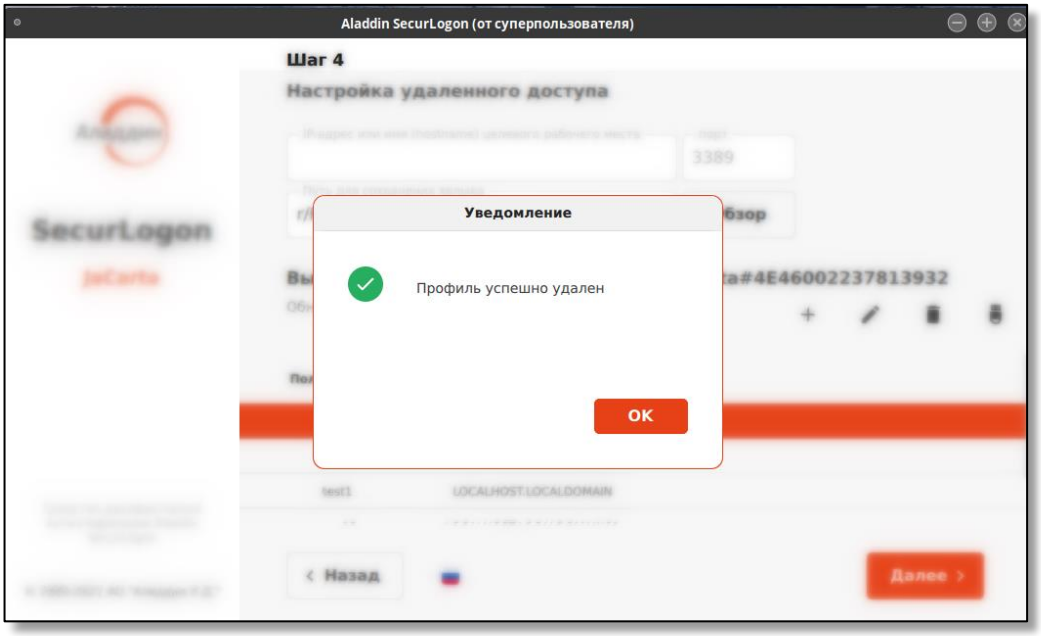

Рисунок 131 – Окно уведомления об успешном создании ярлыка для запуска удаленной сессии

8.3.2.2.4 Действия при извлечении электронного ключа

Для настройки действия при извлечении электронного ключа из разъёма нажмите кнопку  на панели управления сертификатами (см. Рисунок 125) и выберете нужное действие (см. Рисунок 132).

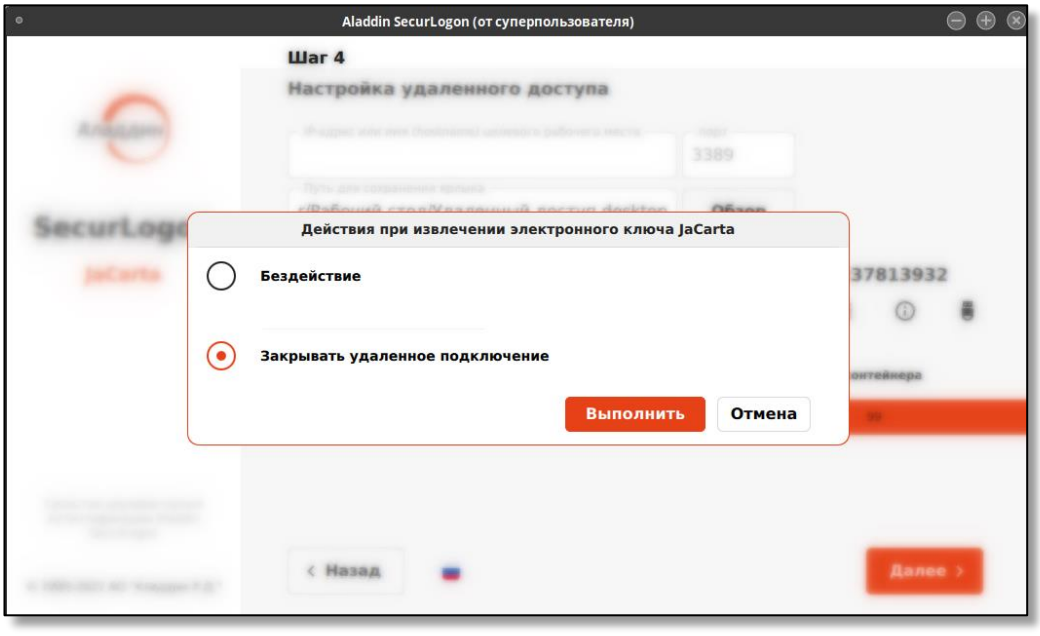

Рисунок 132 – Окно выбора действия при извлечении электронного ключа

Подтвердите действие, нажав кнопку <Выполнить>, при успешном сохранении выбора действия при извлечении электронного ключа вы увидите уведомление об успехе операции (см. Рисунок 133).

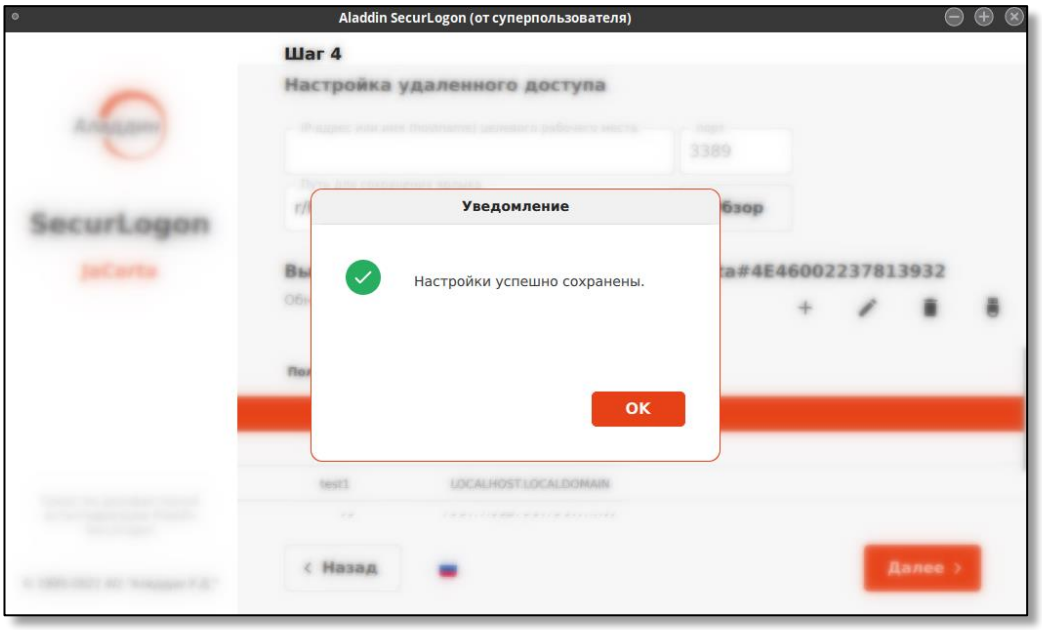

Рисунок 133 – Окно уведомления об успешном сохранении выбора действия при извлечении электронного ключа

После настройки полей шага 4 и выбора профиля пользователя нажмите кнопку <Далее> для перехода на следующий шаг. Администратор будет уведомлен о успешном создании ярлыка для запуска удаленной сессии (см. Рисунок 134).

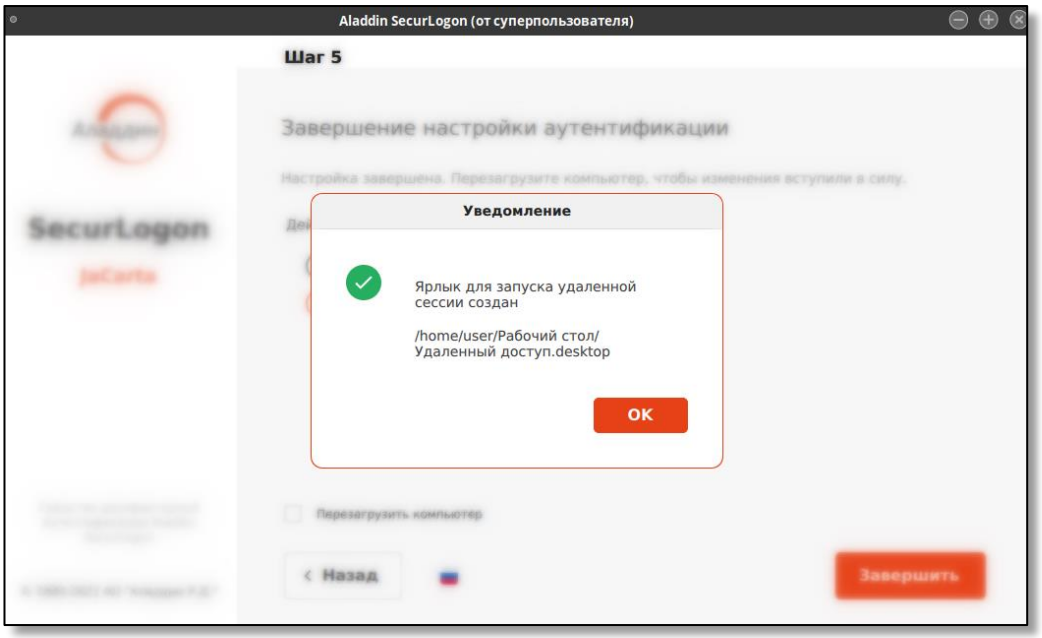

Рисунок 134 – Окно уведомления об успешном создании ярлыка для запуска удаленной сессии

8.3.2.3 Завершение настройки аутентификации при удаленном доступе

В диалоговом окне шага 5 для завершения настройки двухфакторной аутентификации необходимо выбрать действие при извлечении электронного ключа и перезагрузить компьютер для вступления изменений в силу, поставив галочку <Перезагрузить компьютер> и нажав кнопку <Завершить>.

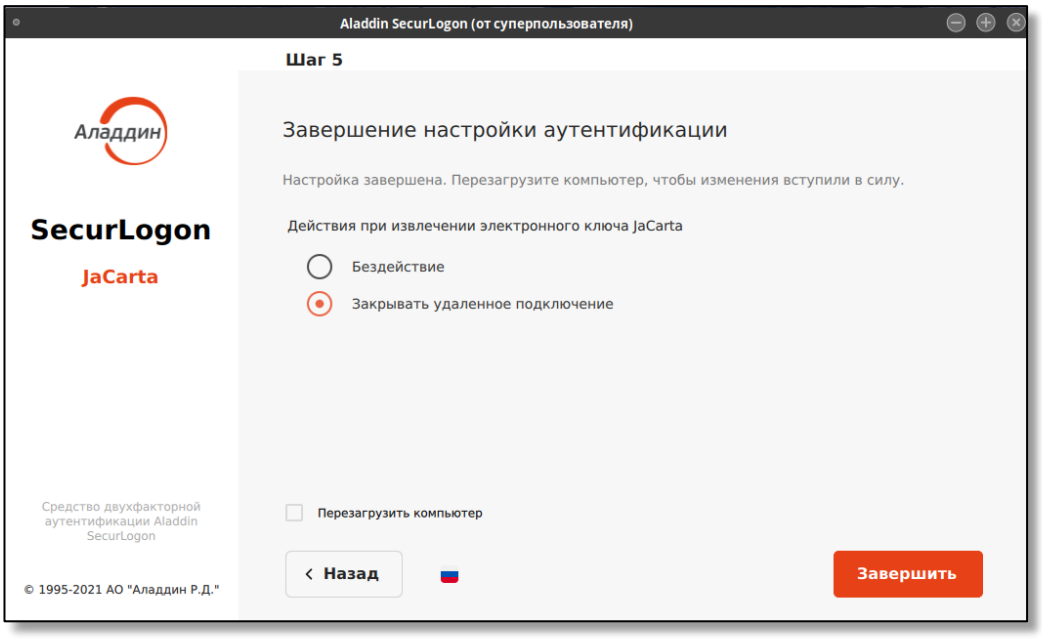

Рисунок 135 – - Окно настройки аутентификации при удаленном доступе без использования PKI. Шаг 7

По завершению работы программы по указанному на шаге 4 пути появится ярлык запуска удаленного подключения (см. Рисунок 136).

Рисунок 136 – Ярлык запуска удаленного подключения

Порядок действий пользователя при двухфакторной аутентификации на удаленном целевом компьютере приведен в «RU.АЛДЕ.03.12.010 34 01-1 Средство двухфакторной аутентификации Aladdin SecurLogon. Руководство оператора».

9. Обновление программного средства

9.1 Назначение обновлений

Обновление базы данных и модулей программы обеспечивает актуальность версии программного средства.

Выполняемые обновлениями задачи:

- исправление обнаруженных за время существования программного средства недочетов и ошибок;
- устранение выявленных уязвимостей;
- изменение или улучшение работы существующих функций;
- добавление новых функций и возможностей.

9.2 Информирование потребителей о выпуске обновлений

- Компания ведет учет покупателей «Средства двухфакторной аутентификации Aladdin SecurLogon«. Выполняется регистрация следующей информации:
  - наименование организации;
  - адрес организации;
  - контактная информация (содержит электронный почтовый адрес лица, обеспечивающего администрирование Aladdin SecurLogon).
- Уведомление пользователей о выпуске обновлений «Средства двухфакторной аутентификации Aladdin SecurLogon« выполняется путем публикации информации на официальном сайте Компании (https://www.aladdin-rd.ru/company/pressroom/news) и (или) с использованием рассылки электронных почтовых сообщений на электронные адреса потребителей. Рассылка может происходить за счет применения средств, обеспечивающих доведение уведомлений до потребителя автоматически. Вместе с файлом обновлений может предоставляться обновленная документация для использования программного средства.

9.3 Процедура установки обновлений

Для обновления продукта:

- Перенесите дистрибутив с обновленной версией программного средства на АРМ с установленным Aladdin SecurLogon любым удобным способом.
- Проверьте целостность дистрибутива путем подсчёта контрольной суммы (см. подраздел 3.2 настоящего документа).
- Выполните распаковку дистрибутива, для этого:
  - в эмуляторе терминала прейдите в папку, в которую скачан архив, выполнив команду:

```
cd <путь к папке размещения архива>
```

  - произведите распаковку архива, выполнив команду:

```
tar -xf {имя файла} -C /<путь распаковки архива>/
```

Архив будет распакован в указанную в пути папку.

- Запустите установку продукта в режиме обновления из папки с распакованным архивом, выполнив переход в папку:

```
cd /<путь распаковки архива>/
```

и запустив скрипт установки:

```
sudo bash ./install.sh
```

Установщик обнаружит установленную версию программного средства и выполнит обновление установленной версии до актуальной версии программного средства. В процессе обновления программного средства «Средство двухфакторной аутентификации Aladdin SecurLogon« будет произведено:

- обновление из репозитория операционной системы следующих пакетов:
  - pcre2-utf16;
  - pcsc-lite-libs;
  - pcsc-lite;
  - pcsc-lite-ccid;
  - opensc;
  - qt-settings;
  - qt5-qtbase;
  - qt5-qtbase-gui;
  - xcb-util-image;
  - xcb-util-keysyms;
  - xcb-util-renderutil;
  - xcb-util-wm;
  - qt5-qtbase-common;
  - openssl-pkcs11;
  - openssl-gost-engine;
  - qt5-qtdeclarative;
  - qt5-qtxmlpatterns;
  - qt5-qt5graphicaleffects;
  - qt5-qtquickcontrols;
  - qt5-qtquickcontrols2;
  - openh264-libs;
  - freerdp-libs;
  - libwinpr;
  - freerdp;
  - xfreerdp;
  - brotli;
  - krb5-pkinit;
  - lightdm-qt5;
  - libcurl;
  - jsoncpp;
  - xwininfo;
  - adcli;
- удаление предыдущей версии пакета jcsecurlogond;
- установка новой версиия пакета jcsecurlogond;
- обновление версии пакета securlogon и jc_lightdm_greeter.

- Перезагрузите АРМ.

9.4 Критерий успешности установки обновления

Критерием правильности установки обновления продукта является отображение информации о новой версии программного средства.

Для вывода версии установленного программного средства, выполните команду:

```
sudo jcsecurlogon -v
```

10. Продление лицензии программы

10.1 Уведомления об окончание срока действия лицензии

- В период 30 дней и менее перед окончанием срока действия лицензии пользователь будет уведомлён в процессе аутентификации в системе сообщением с указанием оставшихся дней действия лицензии (см. Рисунок 137).

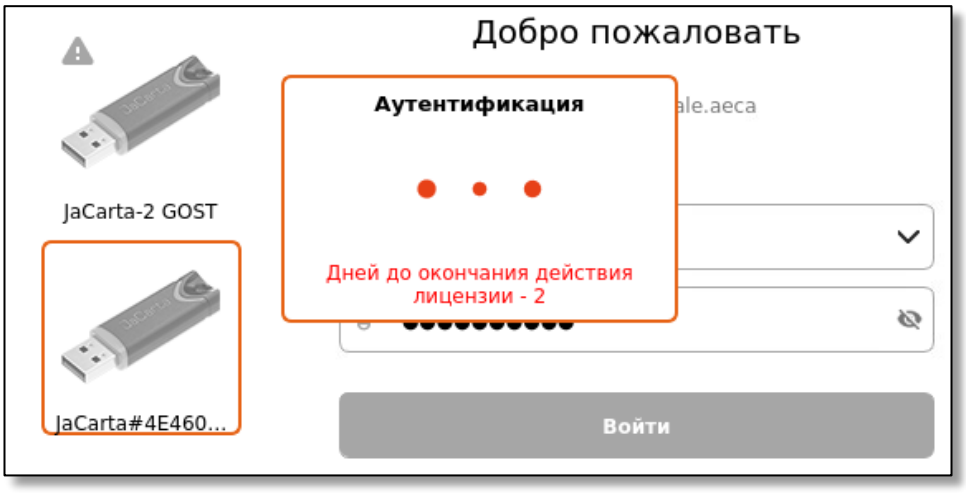

Рисунок 137 – Окно SecurLogon входа в систему с уведомлением о количестве оставшихся дней действия лицензии

- После окончания срока действия лицензии программы, пользователь будет уведомлен соответствующим сообщением при первом запуске операционной системы в окне аутентификации сообщением об истечении срока действия лицензии SecurLogon и перезагрузке системы (см. Рисунок 138).

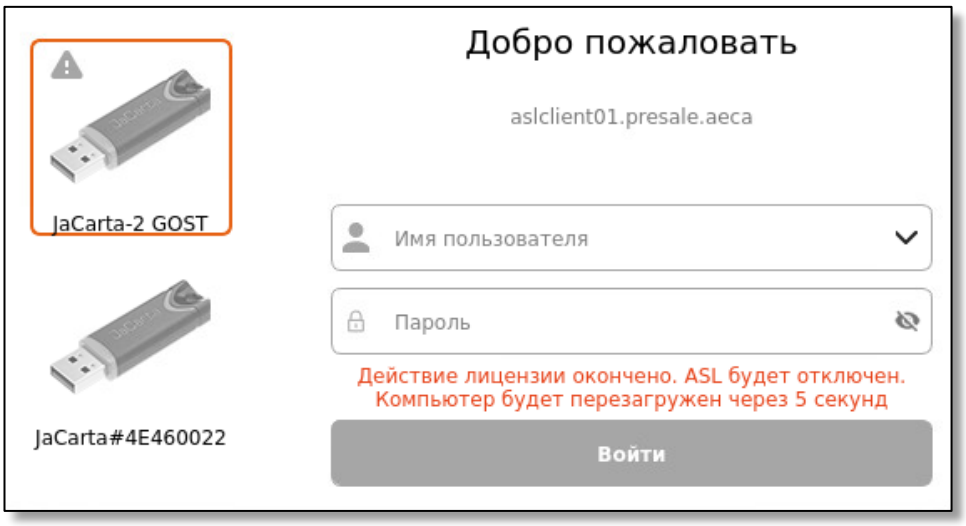

Рисунок 138 – Окно SecurLogon входа в систему с уведомлением об окончании действия лицензии

- Далее после перезагрузки системы и авторизации с использованием штатного окна операционной системы следует однократное уведомление об истечении действия лицензии программы (см. Рисунок 139):

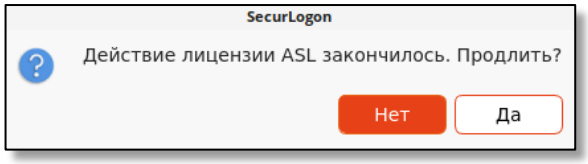

Рисунок 139 – Окно оповещения об окончании срока действия лицензии

– при нажатии кнопки <Нет> окно уведомления закрывается;
– при нажатии кнопки <Да>, запускается программа SecurLogon для дальнейшей установки лицензии.

- При запуске программы с истекшем сроком действия лицензии администратор попадает на страницу принятия лицензионного соглашения и далее, после принятия соглашения, на окно активации программного средства с уведомлением об истечении срока действия ключа активации (см. Рисунок 140).

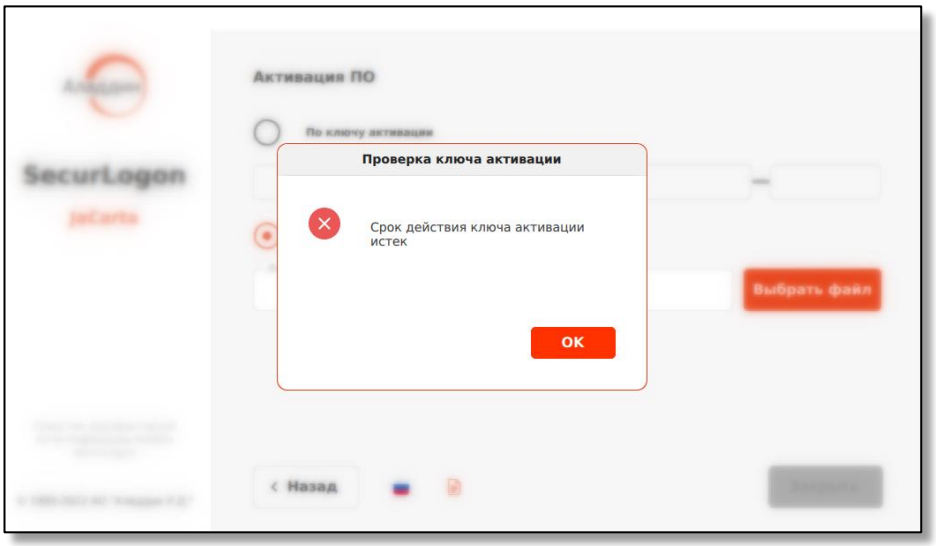

Рисунок 140 – Окно активации ПО после истечения срока действия лицензии

10.2 Продление срока действия лицензии

10.2.1 Активация программного средства после истечения срока действия лицензии

- После окончания срока действия лицензии продукта необходимо запустить программу SecurLogon и выполнить активацию ПО согласно п.5.4, 5.5 настоящего руководства.

10.2.2 Установка новой лицензии до истечения срока действия текущей

- Также возможна установка новой лицензии до истечения срока текущей. Для этого после запуска программы на шаге приветствия нажмите кнопку  <Активация ПО> (см. Рисунок 141).

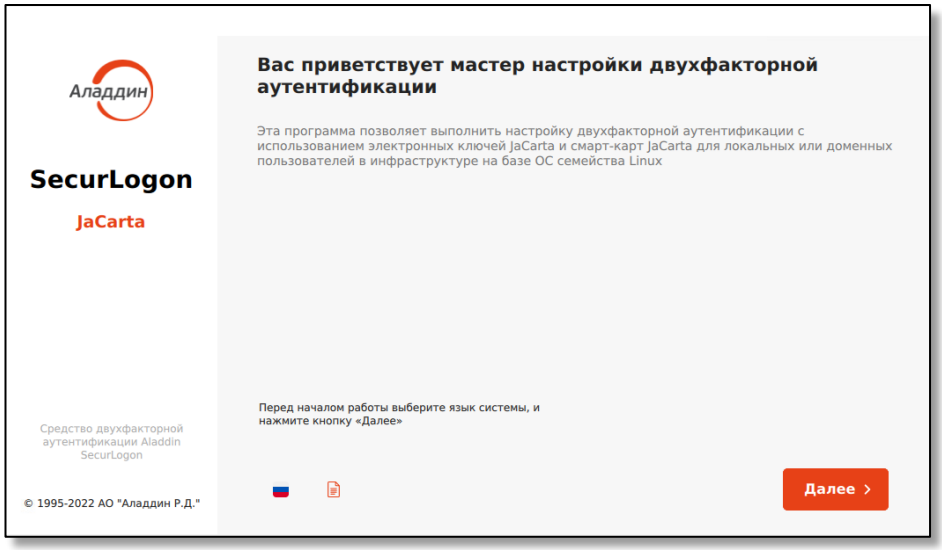

Рисунок 141 – Окно приветствия программы

- В открывшемся окне активации ПО отображены все загруженные лицензии. Для установки новой лицензии нажмите кнопку <Новая Лицензия> (см. Рисунок 142).

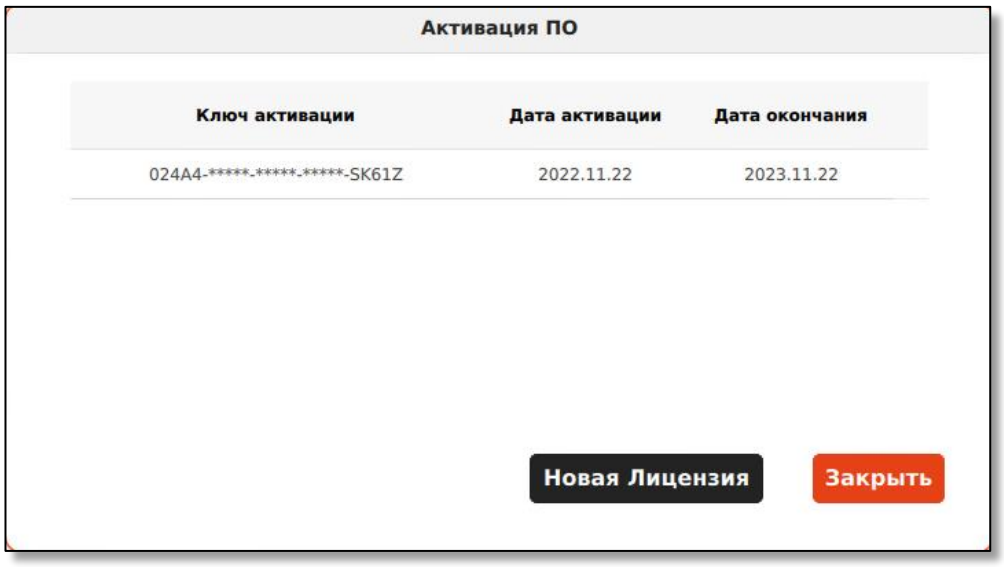

Рисунок 142 – Окно активации ПО (установка новой лицензии при действительной текущей)

- В открывшемся окне введите ключ активации или укажите путь к файлу лицензии (см. Рисунок 143) и нажмите, ставшую активной кнопку <Закрыть>.

Рисунок 143 – Окно активации ПО

11. Сообщения программы

11.1 Сбор диагностической информации

В процессе работы ПО SecurLogon системные службы и приложения записывают все производимые действия. Программа SecurLogon оснащена функцией сбора диагностической информации, которая получает необходимые системные журналы, конфигурационные файлы и аккумулирует их в одном месте, определённом пользователем, для последующего анализа. В процессе сбора формируется архив, который включает в себя:

- системный журнал;
- информацию о конфигурации подсистемы SELinux;
- информацию о подключённых электронных ключах JaCarta и объектах на них;
- информацию о настройках PAM-модулей;
- информацию об установленных пакетах;
- информацию о домене;
- конфигурацию и журналы служб SSSD;
- прочую диагностическую информацию.

- Собрать диагностическую информацию можно на любом шаге работы SecurLogon. Для этого щёлкните на пиктограмме Аладдин в левой части окна приложения, появится кнопка <Диагностика> (см. Рисунок 144).

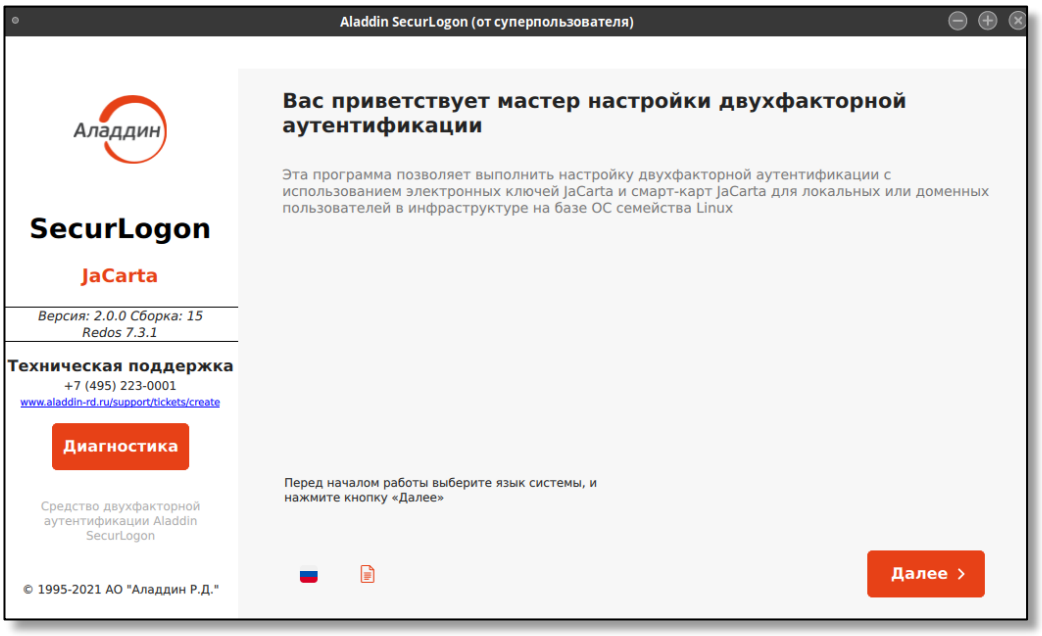

Рисунок 144 – Панель сбора диагностической информации

- Для сбора диагностической информации щёлкните на кнопке <Диагностика> и в появившемся окне (см. Рисунок 145), нажав кнопку <Открыть>, выберите необходимый каталог в файловой системе, в котором будет создан архив с журналами, или введите путь до папки в поле «Директория сбора логов» с помощью клавиатуры.

  По умолчанию архив создаётся в каталоге `/tmp`.

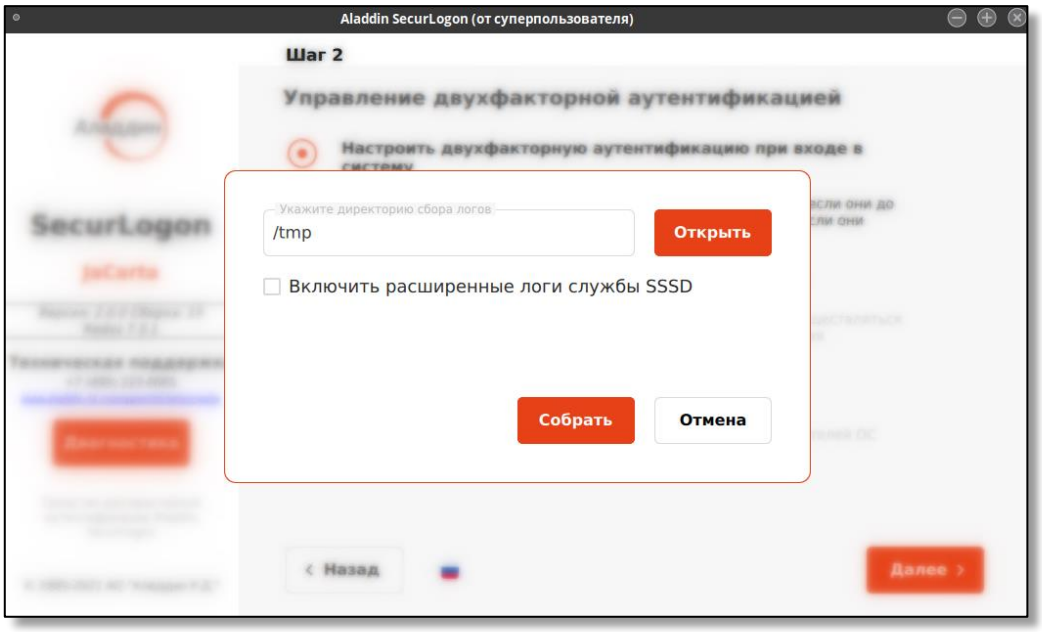

Рисунок 145 – Выбор каталога сбора диагностической информации

Для включения расширенных логов службы SSSD поставьте галочку в соответствующее поле, программа уведомит об успешном включении расширенных логов служб SSSD (см. Рисунок 146), при этом отобразится уведомление о необходимости провести повторную попытку двухфакторной аутентификации для того, чтобы соответствующие диагностические записи попали в журналы службы SSSD. В результате будут отредактированы соответствующие конфигурационные файлы службы SSSD и произведён её перезапуск.

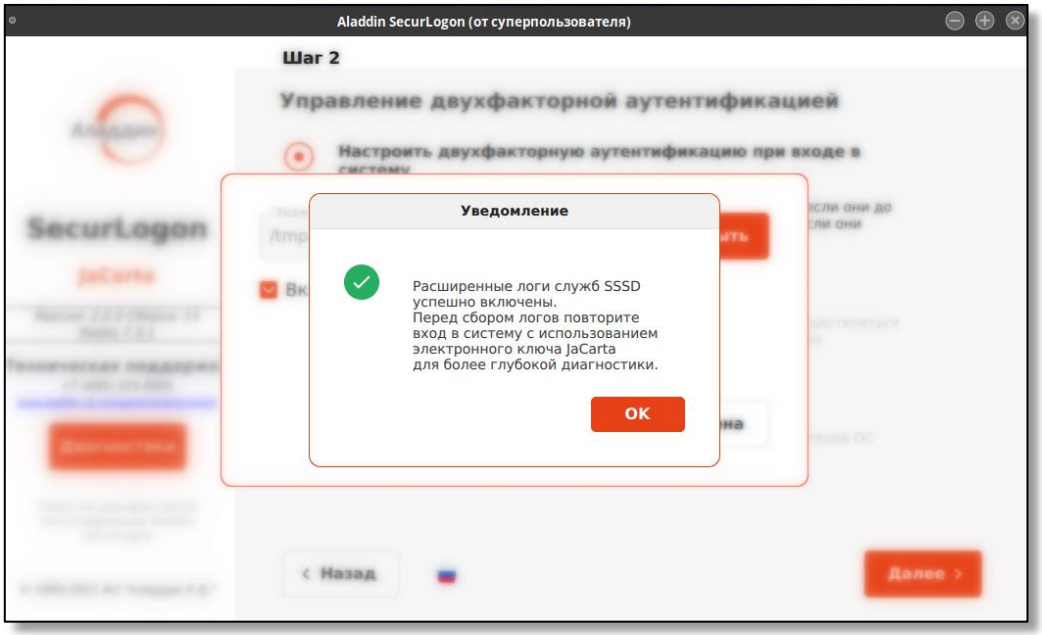

Рисунок 146 – Окно уведомления об успешном включении расширенных логов служб SSSD

- Далее по нажатию кнопки <Собрать> в выбранном каталоге будет создан архив с журналами. Имя архива генерируется автоматически и имеет вид: `SL_LOGS_год_месяц_число_часы_минуты_секунды.tgz`.После сбора журналов появится уведомление об успешном завершении операции (см. Рисунок 147).

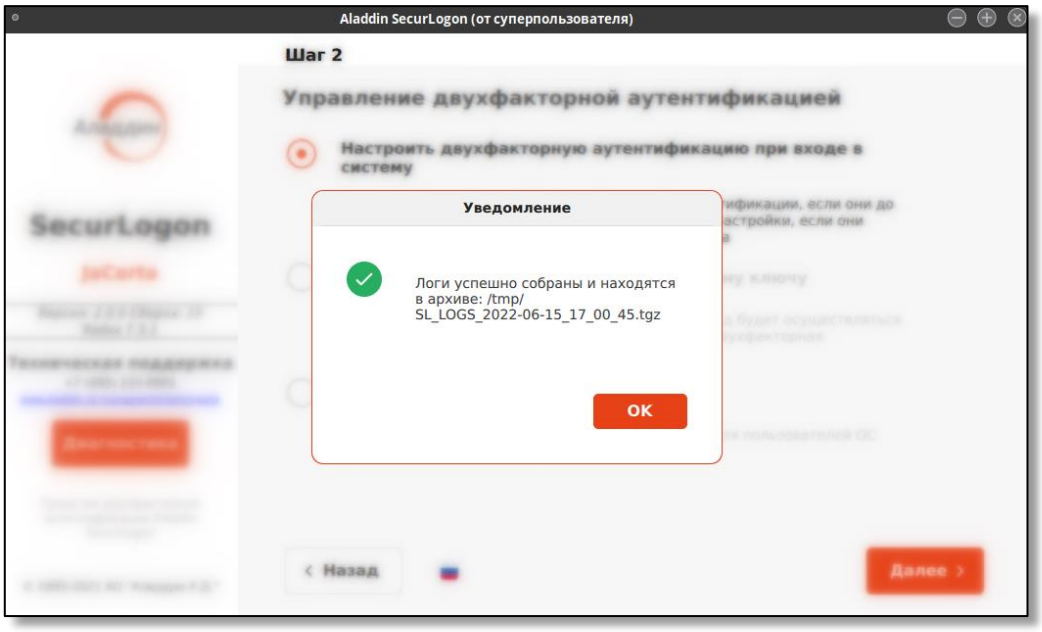

Рисунок 147 – Окно уведомления об успешном создании архива с журналами

11.2 Механизм оповещений

В программе предусмотрен механизм оповещений для информирования уполномоченного пользователя о том, что в программе что-то произошло и требует внимания. Оповещение представляет собой модальное окно, которое появляется, как правило, по центру текущего диалогового окна программы и сообщает об ошибке программы или обязательном действии, которое не выполнено. Дальнейшие действия в программе возможны только после обработки этого окна.

11.3 Сообщения об ошибках

Возможные сообщения об ошибках и необходимые действия по их устранению приведены в Таблица 9.

Таблица 9 – Сообщения об ошибках в журнале событий

№ п/п	Ошибка	Описание	Действие оператора

1	Запуск процесса обновления Ошибка	Ошибка возникает, когда процесс `/usr/sbin/jcsecurlogonupdater check` или `/usr/sbin/jcsecurlogonupdater install` завершился с кодом ошибки `-1`.	1) Попробовать вручную запустить процесс
			`/usr/sbin/jcsecurlogon updater check:`
			`root#: /usr/sbin/jcsecurlogon updater check`
			2) Проверьте соединение с сервером обновлений:
			`root#: ping $(IP-адрес сервера или url-адрес сервера)`

№ п/п	Ошибка	Описание	Действие оператора

2	Перезапуск службы `sssd` Ошибка	Ошибка возникает, когда перезапуск службы `sssd` завершился с ошибкой.	1) Проверьте существование конфигурационного файла /etc/sssd.conf
			`root#: ls /etc/ | grep sssd.conf`
			2) Проверьте наличие пакета `sssd` в системе:
			Astra Linux:
			`root#: dpkg -l | grep sssd`
			RedOS и Alt:
			`root#: yum list installed sssd`
			3) Перезапустите `sssd`:
			`root#: systemctl restart sssd`
			4) Переустановите SecurLogon

3	Невозможно открыть `/etc/pam.d/common-auth`
	Невозможно открыть `/etc/pam.d/system-auth`
	Невозможно открыть `/etc/pam.d/common-password`
	Невозможно открыть `/etc/pam.d/password-auth`
		Ошибка возникает, когда невозможно открыть файлы конфигурации:
		1) `/etc/pam.d/common-auth`;
		2) `/etc/pam.d/system-auth`;
		3) `/etc/pam.d/common-password`;
		4) `/etc/pam.d/password-auth.`
			1) Проверьте существование конфигурационных файлов в системе:
			`root#: ls /etc/pam.d/ | grep common-auth`
			`root#: ls /etc/pam.d/ | grep common-password`
			`root#: ls /etc/pam.d/ | grep system-auth`
			`root#: ls /etc/pam.d/ | grep password-auth`
			2) Проверьте права доступа к конфигурационным файлам:
			`root#: chmod 600 /etc/pam.d/common-auth`
			`root#: chmod 600 /etc/pam.d/common-password`
			`root#: chmod 600 /etc/pam.d/system-auth`
			`root#: chmod 600 /etc/pam.d/password-auth`

№ п/п	Ошибка	Описание	Действие оператора
			3) Переустановите SecurLogon.
4	Данная версия Ред ОС не поддерживается!	Ошибка возникает, когда SecurLogon установлен на версию РЕД ОС, которая не поддерживается.	Переустановите SecurLogon на поддерживаемую версию РЕД ОС.
5	Текущая платформа не поддерживается!	Ошибка возникает, когда SecurLogon установлен на версию РЕД ОС, которая не поддерживается.	Переустановить SecurLogon на поддерживаемую операционную систему.

6	Ошибка файла конфигурации	Ошибка возникает, когда:
		1) не удалось открыть конфигурационный файл /usr/local/etc/jcsecurlogon/jcsecurlogon.conf
		2) возникла ошибка в ходе чтения конфигурационного файла /usr/local/etc/jcsecurlogon/jcsecurlogon.conf
			1) Проверьте существование конфигурационных файлов в системе:
			`root#: ls /usr/local/etc/jcsecurlogon`
			2) Проверьте права доступа к конфигурационным файлам:
			`root#: chmod 600 /usr/local/etc/jcsecurlogon/jcsecurlogon.conf`
			3) Переустановите SecurLogon.

7	Не удалось открыть `sssd.conf`
	
	Не удалось открыть `krb5.conf`
		Ошибка возникает, когда не удалось открыть конфигурационный файл:
		1) `/etc/sssd.conf`
		2) `/etc/krb5.conf`
			1) Дублирует ошибку №2.
			2.1) Проверить существование конфигурационного файла /etc/krb5.conf
			`root#: ls /etc/ | grep krb5.conf`
			2.2) Проверить наличие пакета krb5 в системе:
			Astra Linux:
			`root#: dpkg -l | grep krb5`
			RedOS и Alt:
			`root#: yum list installed krb5`
			2.3) Перезапустите krb5:
			`root#: systemctl restart krb5`
			2.4) Переустановите SecurLogon.

8	Не удалось открыть `common-auth` (ОС Astra 1.6)	Ошибка возникает, когда не удалось открыть конфигурационный файл `/etc/pam.d/common-auth` на системе Astra1.6	Дублирует ошибку №3

№ п/п	Ошибка	Описание	Действие оператора

9	Не удалось открыть jc-tf-net-auth_nopki	Ошибка возникает, когда не удалось открыть конфигурационный файл `/etc/pam.d/jc-tf-net-auth_nopki`	1) Проверьте существование конфигурационных файлов в системе:
			`root#: ls /etc/pam.d/ | grep jc-tf-net-auth_nopki`
			2) Проверьте права доступа к конфигурационным файлам:
			`root#: chmod 600 /etc/pam.d/jc-tf-net-auth_nopki`
			3) Переустановите SecurLogon

10	Включение двухфакторной аутентификации: неизвестный тип ОС	Ошибка возникает, когда происходит установка двухфакторной аутентификации на неизвестную ОС	Переустановите SecurLogon на поддерживаемую систему
11	Включение двухфакторной аутентификации noPKI: неизвестный тип ОС	Ошибка возникает, когда происходит установка двухфакторной усиленной (noPKI) аутентификации на неизвестную ОС	Дублирует ошибку №10
12	Отключение двухфакторной аутентификации: неизвестный тип ОС	Ошибка возникает, когда происходит отключение двухфакторной усиленной (noPKI) аутентификации на неизвестную ОС	Дублирует ошибку №10
13	Не удалось назначить политику входа для пользователя	Ошибка возникает, когда смена политики входа произошла неудачно	1) Удостоверьтесь, что имя профиля соответствует имени системного пользователя, для которого происходит настройка политики входа. 2) Попробуйте вручную сменить пароль для заданного системного пользователя: `root#: gpasswd $(пользователь) $(группа политики входа)`
14	Ошибка в ходе установки политики для пользователя	Ошибка возникает, когда установка политики входа произошла неудачно	Дублирует ошибку №13
15	Невозможно создать профиль	Ошибка возникает, когда профиль уже создан в памяти электронного ключ JaCarta	1) Создайте профиль с другим именем. 2) Пересоздайте электронный ключ JaCarta с заданным именем

№ п/п	Ошибка	Описание	Действие оператора
16	Не удалось открыть файл сертификата	Ошибка возникает, когда нельзя открыть файл сертификата, хранящегося в памяти электронного ключа JaCarta	1) Проверьте, что электронный ключ JaCarta подсоединён к компьютеру. 2) Удостоверьтесь, что электронный ключ JaCarta правильно определился в системе средствами Единого Клиента JaCarta. 3) Проверьте наличие сертификата в памяти электронного ключа JaCarta. 4) Перезапустите SecurLogon. 5) Переустановите SecurLogon
17	Не удалось сохранить файл сертификата	Ошибка возникает, когда нельзя сохранить файл сертификата в памяти электронного ключа JaCarta	1) Проверьте, что электронный ключ JaCarta подсоединён к компьютеру. 2) Удостоверьтесь, что электронный ключ JaCarta правильно определился в системе средствами Единого Клиента JaCarta. 3) Попытайтесь создать сертификат в памяти электронного ключ JaCarta. 4) Перезапустите SecurLogon. 5) Переустановите SecurLogon
18	Не удалось открыть файл конфигурации	Дублирует ошибку №6	Дублирует ошибку №6
19	Не найден файл конфигурации	Дублирует ошибку №6	Дублирует ошибку №6

20	Ошибка поиска профиля	Ошибка возникает, когда невозможно проинициализировать поиск объектов средствами «Единой Библиотеки».
		Код возврата:
		`CKR_ARGUMENTS_BAD` – недопустимые аргументы.
		`CKR_ATTRIBUTE_READ_ONLY` – невозможно установить значение атрибута, т.к. он поддерживает только чтение.
		`CKR_ATTRIBUTE_TYPE_INVALID` – недопустимый тип атрибута.
		`CKR_ATTRIBUTE_VALUE_INVALID` – недопустимое значение атрибута.
		`CKR_CRYPTOKI_NOT_INITIALIZED` – функция не может быть выполнена, т.к. библиотека еще не была инициализирована
		`CKR_DEVICE_ERROR` – возникла проблема с электронным ключом JaCarta и/или слотом.
		`CKR_DEVICE_MEMORY` – памяти электронный ключ JaCarta недостаточно для данной операции.
		`CKR_DEVICE_REMOVED` – электронный ключ JaCarta был изъят из слота.
		`CKR_DOMAIN_PARAMS_INVALID` – недопустимые или неподдерживаемые параметры домена.
			1) Проверить наличие «Единой Библиотеки»:
			Astra Linux:
			`root#: dpkg -l | grep jcPKCS`
			RedOS и Alt:
			`root#: yum list installed jcPKCS`
			2) Переустановите SecurLogon

№ п/п	Ошибка	Описание	Действие оператора
		CKR_FUNCTION_FAILED – выполнение функции было прервано или она не может быть выполнена. CKR_GENERAL_ERROR – общий сбой при работе с библиотекой. CKR_HOST_MEMORY – компьютер, на котором запущена библиотека, не имеет достаточно памяти для выполнения функции. CKR_OK – функция выполнена успешно. CKR_PIN_EXPIRED – срок действия указанного PIN-кода истек. CKR_SESSION_CLOSED – сеанс был закрыт в момент выполнения функции. CKR_SESSION_HANDLE_INVALID – недопустимый дескриптор сеанса. CKR_SESSION_READ_ONLY – сеанс открыт только на чтение. CKR_TEMPLATE_INCOMPLETE – шаблон, указанный для создания объекта, неполон. CKR_TEMPLATE_INCONSISTENT – шаблон, указанный для создания объекта, содержит конфликтующие атрибуты. CKR_TOKEN_WRITE_PROTECTED – данный электронный ключ JaCarta защищен от записи. CKR_USER_NOT_LOGGED_IN – действие не может быть выполнено, т.к. пользователь не авторизован.	
21	Ошибка поиска атрибута	Ошибка возникает, когда невозможно получить атрибут со слота электронный ключ JaCarta средствами «Единой Библиотеки». Код возврата: CKR_ARGUMENTS_BAD – недопустимые аргументы. CKR_ATTRIBUTE_SENSITIVE – запрашиваемый атрибут недоступен для чтения. CKR_ATTRIBUTE_TYPE_INVALID – недопустимый тип атрибута. CKR_BUFFER_TOO_SMALL – вывод функции слишком велик для предоставленного буфера. CKR_CRYPTOKI_NOT_INITIALIZED – функция не может быть выполнена, т. к. библиотека ещё не была инициализирована CKR_DEVICE_ERROR – возникла проблема с электронным ключом JaCarta и/или слотом.. CKR_DEVICE_MEMORY – памяти электронный ключ JaCarta недостаточно для данной операции. CKR_DEVICE_REMOVED – электронный ключ JaCarta был изъят из слота. CKR_FUNCTION_FAILED – выполнение функции было прервано или она не может быть выполнена. CKR_GENERAL_ERROR – общий сбой при работе с библиотекой. CKR_HOST_MEMORY – компьютер, на котором запущена библиотека, не имеет достаточно памяти для выполнения функции. CKR_OBJECT_HANDLE_INVALID – недопустимый дескриптор объекта. CKR_OK – функция выполнена успешно.	Дублирует ошибку №20

№ п/п	Ошибка	Описание	Действие оператора
		CKR_SESSION_CLOSED – сеанс был закрыт в момент выполнения функции. CKR_SESSION_HANDLE_INVALID – недопустимый дескриптор сеанса.	
22	Ошибка установки атрибута на электронном ключе JaCarta	Ошибка возникает, когда невозможно установить атрибут на слот электронный ключ JaCarta средствами «Единой Библиотеки». Код возврата: CKR_ARGUMENTS_BAD – недопустимые аргументы. CKR_ATTRIBUTE_READ_ONLY – невозможно установить значение атрибута, т.к. он поддерживает только чтение. CKR_ATTRIBUTE_TYPE_INVALID – недопустимый тип атрибута. CKR_ATTRIBUTE_VALUE_INVALID – недопустимое значение атрибута. CKR_CRYPTOKI_NOT_INITIALIZED – функция не может быть выполнена, т.к. библиотека ещё не была инициализирована CKR_DEVICE_ERROR – возникла проблема с электронный ключ JaCartaом и/или слотом. CKR_DEVICE_MEMORY – памяти электронный ключ JaCarta недостаточно для данной операции. CKR_DEVICE_REMOVED – электронный ключ JaCarta был изъят из слота. CKR_FUNCTION_FAILED – выполнение функции было прервано или она не может быть выполнена. CKR_GENERAL_ERROR – общий сбой при работе с библиотекой. CKR_HOST_MEMORY – компьютер, на котором запущена библиотека, не имеет достаточно памяти для выполнения функции. CKR_OBJECT_HANDLE_INVALID – недопустимый дескриптор объекта. CKR_OK – функция выполнена успешно. CKR_SESSION_CLOSED – сеанс был закрыт в момент выполнения функции. CKR_SESSION_HANDLE_INVALID – недопустимый дескриптор сеанса. CKR_SESSION_READ_ONLY – сеанс открыт только на чтение. CKR_TEMPLATE_INCONSISTENT – шаблон, указанный для создания объекта, содержит конфликтующие атрибуты. CKR_TOKEN_WRITE_PROTECTED – данный электронный ключ JaCarta защищён от записи. CKR_USER_NOT_LOGGED_IN – действие не может быть выполнено, т.к. пользователь не авторизован.	Дублирует ошибку №20

№ п/п	Ошибка	Описание	Действие оператора
23	Ошибка открытия сессии обмена с токеном	Ошибка возникает, когда невозможно открыть сессию средствами «Единой Библиотек». Код возврата: `CKR_ARGUMENTS_BAD` – недопустимые аргументы. `CKR_CRYPTOKI_NOT_INITIALIZED` – функция не может быть выполнена, т.к. библиотека ещё не была инициализирована `CKR_DEVICE_ERROR` – возникла проблема с электронным ключом JaCartaом и/или слотом. `CKR_DEVICE_REMOVED` – электронный ключ JaCarta был изъят из слота. `CKR_DEVICE_MEMORY` – памяти электронный ключ JaCarta недостаточно для данной операции. `CKR_FUNCTION_FAILED` – выполнение функции было прервано или она не может быть выполнена. `CKR_GENERAL_ERROR` – общий сбой при работе с библиотекой. `CKR_HOST_MEMORY` – компьютер, на котором запущена библиотека, не имеет достаточно памяти для выполнения функции. `CKR_OK` – функция выполнена успешно. `CKR_SESSION_COUNT` – открыто слишком большое количество сеансов. `CKR_SESSION_PARALLEL_NOT_SUPPORTED` – данный электронный ключ JaCarta не поддерживает параллельные сеансы `CKR_SESSION_READ_WRITE_SO_EXISTS` – сеанс чтения/записи уже открыт, администратор не имеет возможности авторизоваться. `CKR_SLOT_ID_INVALID` – недопустимый идентификатор слота. `CKR_TOKEN_NOT_PRESENT` – в слоте отсутствует электронный ключ JaCarta. `CKR_TOKEN_NOT_RECOGNIZED` – электронный ключ JaCarta не поддерживается. `CKR_TOKEN_WRITE_PROTECTED` – данный электронный ключ JaCarta защищён от записи.	Дублирует ошибку №20.
24	Ошибка авторизации на токене	Ошибка возникает, когда корректно не вызвалась функция для ввода PIN-кода и перехода в режим администратора или пользователя сессию «Единой Библиотеки». Код возврата: `CKR_ARGUMENTS_BAD` – недопустимые аргументы. `CKR_CRYPTOKI_NOT_INITIALIZED` – функция не может быть выполнена, т.к. библиотека ещё не была инициализирована `CKR_DEVICE_ERROR` – возникла проблема с электронным ключом JaCartaом и/или слотом. `CKR_DEVICE_MEMORY` – памяти электронный ключ JaCarta недостаточно для данной операции. `CKR_DEVICE_REMOVED` – электронный ключ JaCarta был изъят из слота. `CKR_FUNCTION_CANCELED` – функция была отменена в момент исполнения.	Дублирует ошибку №20.

№ п/п	Ошибка	Описание	Действие оператора
		`CKR_FUNCTION_FAILED` – выполнение функции было прервано или она не может быть выполнена. `CKR_GENERAL_ERROR` – общий сбой при работе с библиотекой. `CKR_HOST_MEMORY` – компьютер, на котором запущена библиотека, не имеет достаточно памяти для выполнения функции. `CKR_OK` – функция выполнена успешно. `CKR_OPERATION_NOT_INITIALIZED` – в указанном сеансе нет активной операции данного типа. `CKR_PIN_INCORRECT` – неверный PIN-код. `CKR_SESSION_CLOSED` – сеанс был закрыт в момент выполнения функции. `CKR_PIN_LOCKED` – указанный PIN-код заблокирован и не может быть использован. `CKR_SESSION_HANDLE_INVALID` – недопустимый дескриптор сеанса. `CKR_SESSION_READ_ONLY_EXISTS` – сеанс на чтение уже открыт и администратор не может быть авторизован. `CKR_USER_ALREADY_LOGGED_IN` – пользователь уже авторизован. `CKR_USER_ANOTHER_ALREADY_LOGGED_IN` – указанный пользователь не может быть авторизован в данном сеансе, так как другой пользователь уже авторизован в нем. `CKR_USER_PIN_NOT_INITIALIZED` – PIN-код-пользователя не инициализирован `CKR_USER_TOO_MANY_TYPES` – невозможно авторизоваться больше пользователей, чем позволяет электронный ключ JaCarta/библиотека. `CKR_USER_TYPE_INVALID` – недопустимый тип пользователя	
25	Профиль пользователя не найден на электронном ключе JaCarta	Ошибка возникает, когда на электронном ключе JaCarta не был найден профиль.	1) Создайте профиль с другим именем. 2) Пересоздайте электронный ключ JaCarta с заданным именем
26	Не задан пароль пользователя	Ошибка возникает, когда на созданном профиле не задан пароль	Создайте профиль и задайте пароль в соответствии с требованиями безопасности

27	Ошибка в процессе запуска сессии удалённого доступа	Ошибка возникает, когда невозможно запустить процесс удалённого доступа `xfreerdp`	1) Проверьте наличие пакета `sssd` в системе:
			Astra Linux:
			`root#: dpkg -l | grep xfreerdp`
			RedOS и Alt:
			`root#: yum list installed xfreerdp`
			2) Перезапустите `xfreerdp`:

№ п/п	Ошибка	Описание	Действие оператора
			`root#: systemctl restart xfreerdp` 3) Переустановить SecurLogon
28	Ошибка в процессе завершения сессии удалённого доступа	Ошибка возникает, когда невозможно корректно завершить процесс удалённого доступа `xfreerdp`	Перезапустить `xfreerdp`: `root#: systemctl restart xfreerdp`

29	Не удалось получить ticket kerberos, проверьте доступность контроллера домена	Ошибка возникает, когда не получилось получить ticket Kerberos на контроллере домена	1) Попробуйте вручную подключиться к контроллеру домена:
			`root#: kinit $(администратор)@$(домен)`
			2) Проверить, что компьютер пользователя видит компьютер контроллера домена:
			`root#: ping $(администратор)@$(домен)`
			`root#: ping $(IP-адрес контроллера домена)`

30	Ошибка загрузки сертификата	Ошибка возникает, когда не получилось получить сертификат на контроллере домена	1) Дублирует ошибку №29
			2) Проверить наличие пакета `curl` в системе:
			Astra Linux:
			`root#: dpkg -l | grep curl`
			RedOS и Alt:
			`root#: yum list installed curl`

31	Ошибка доступа к файлу	Дублирует ошибку №7	Дублирует ошибку №7
32	Ошибка, превышено время ожидания ответа	Ошибка возникает, когда превышено время на выполнение операции	Перегрузите систему
33	Не удалось отредактировать файл конфигурации	Дублирует ошибку №7	Дублирует ошибку №7
34	Файл не найден	Дублирует ошибку №30	Дублирует ошибку №30

№ п/п	Ошибка	Описание	Действие оператора
35	Неизвестная операционная система	Дублирует ошибку №12	Дублирует ошибку №12
36	Не введён PIN-код	Ошибка возникает, когда не был введён PIN-код в процессе удаления сертификата	Введите PIN-код
37	Введён неправильный PIN-код	Ошибка возникает, когда не был введён корректный PIN-код в процессе удаления сертификата	Введите корректный PIN-код
38	Некорректный формат файла конфигурации	Ошибка возникает в процессе чтения файла конфигурации `/usr/local/etc/jcsecurlogon/jcsecurlogon.conf`	Переустановите SecurLogon
39	Не получен список слотов.	Ошибка возникает, когда корректно не вызвалась функция для получения списка слотов средствами “Единой Библиотеки”. Код возврата: `CKR_ARGUMENTS_BAD` – недопустимые аргументы. `CKR_BUFFER_TOO_SMALL` – вывод функции слишком велик для предоставленного буфера. `CKR_CRYPTOKI_NOT_INITIALIZED` – функция не может быть выполнена, т.к. библиотека еще не была инициализирована `CKR_FUNCTION_FAILED` – выполнение функции было прервано или она не может быть выполнена. `CKR_GENERAL_ERROR` – общий сбой при работе с библиотекой. `CKR_HOST_MEMORY` – компьютер, на котором запущена библиотека, не имеет достаточно памяти для выполнения функции. `CKR_OK` – функция выполнена успешно	Дублирует ошибку №20
40	Неверный слот!	Ошибка возникает, когда номер слота больше, чем количество слотов на электронном ключе JaCarta	1) Перезапустите SecurLogon. 2) Перегрузите систему.
41	Не получен идентификатор слота.	Дублирует ошибку №39	Дублирует ошибку №39.
42	Не удалось получить информацию по электронный ключ JaCarta	Ошибка возникает, когда корректно не вызвалась функция для получения информации о слоте средствами «Единой Библиотеки». Код возврата: `CKR_ARGUMENTS_BAD` – недопустимые аргументы. `CKR_CRYPTOKI_NOT_INITIALIZED` – функция не может быть выполнена, т.к. библиотека еще не была инициализирована `CKR_DEVICE_ERROR` – возникла проблема с электронным ключом JaCarta и/или слотом. `CKR_FUNCTION_FAILED` – выполнение функции было прервано или она не может быть выполнена. `CKR_GENERAL_ERROR` – общий сбой при работе с библиотекой. `CKR_HOST_MEMORY` – компьютер, на котором запущена библиотека, не имеет достаточно памяти	Дублирует ошибку №20.

№ п/п	Ошибка	Описание	Действие оператора
		для выполнения функции. CKR_OK – функция выполнена успешно	
43	Некорректный тип электронный ключ JaCarta	Ошибка возникает, когда не удалось распознать модель слота электронного ключа JaCarta	Дублирует ошибку №40
44	Ошибка доступа к электронному ключу токену	Дублирует ошибку №23	Дублирует ошибку №23
45	Ошибка создания профиля	Ошибка возникает, когда корректно не получилось создать объект на слоте электронного ключа JaCarta средствами «Единой Библиотеки». Код возврата: CKR_ARGUMENTS_BAD – недопустимые аргументы. CKR_ATTRIBUTE_READ_ONLY – невозможно установить значение атрибута, т.к. он поддерживает только чтение. CKR_ATTRIBUTE_TYPE_INVALID – недопустимый тип атрибута. CKR_ATTRIBUTE_VALUE_INVALID – недопустимое значение атрибута. CKR_CRYPTOKI_NOT_INITIALIZED – функция не может быть выполнена, т.к. библиотека ещё не была инициализирована CKR_DEVICE_ERROR – возникла проблема с электронным ключом JaCarta и/или слотом. CKR_DEVICE_MEMORY – памяти электронный ключ JaCarta недостаточно для данной операции. CKR_DEVICE_REMOVED – электронный ключ JaCarta был изъят из слота. CKR_DOMAIN_PARAMS_INVALID – недопустимые или неподдерживаемые параметры домена. CKR_FUNCTION_FAILED – выполнение функции было прервано или она не может быть выполнена. CKR_GENERAL_ERROR – общий сбой при работе с библиотекой. CKR_HOST_MEMORY – компьютер, на котором запущена библиотека, не имеет достаточно памяти для выполнения функции. CKR_OK – функция выполнена успешно. CKR_PIN_EXPIRED – срок действия указанного PIN-кода истёк. CKR_SESSION_CLOSED – сеанс был закрыт в момент выполнения функции. CKR_SESSION_HANDLE_INVALID – недопустимый дескриптор сеанса. CKR_SESSION_READ_ONLY – сеанс открыт только на чтение. CKR_TEMPLATE_INCOMPLETE – шаблон, указанный для создания объекта, неполон. CKR_TEMPLATE_INCONSISTENT – шаблон, указанный для создания объекта, содержит конфликтующие атрибуты.	Дублирует ошибку №20

№ п/п	Ошибка	Описание	Действие оператора
		`CKR_TOKEN_WRITE_PROTECTED` – данный электронный ключ JaCarta защищён от записи. `CKR_USER_NOT_LOGGED_IN` – действие не может быть выполнено, т.к. пользователь не авторизован	

1.2 Сообщения информационные

В Таблица 10 приведены возможные информационные сообщения механизма оповещения.

Таблица 10 – Оповещения программы

№ п/п	Ошибка	Описание	Действие оператора
1	Непредвиденная ошибка в процессе установки политик входа	Ошибка возникает, когда смена политики входа произошла неудачно	1) Убедитесь, что имя профиля соответствует имени системного пользователя, для которого происходит настройка политики входа. 2) Попробуйте вручную сменить пароль для заданного системного пользователя: `root#: gpasswd $(пользователь) $(группа политики входа)`
2	Пользователь не выбран	Пользователь не был выбран из таблицы пользователей	Убедитесь, что выбран пользователь из таблицы пользователей.
3	Сертификат не привязан	Ошибка возникает в ходе привязки сертификата к пользователю	1) Убедитесь, что пользователь, к которому происходит привязка сертификата существует. 2) Проверьте, что электронный ключ JaCarta вставлен. 3) Убедитесь, что электронный ключ JaCarta правильно определился в системе средствами Единого Клиента JaCarta. 4) Проверьте наличие сертификата на слоте электронного ключа JaCarta. 5) Перезапустите SecurLogon. 6) Переустановите SecurLogon
4	Не удалось отвязать сертификаты	Ошибка возникает в ходе отвязки сертификатов от пользователя	Дублирует ошибку №3
5	Непредвиденная ошибка в процессе выключения автогенерации пароля	Ошибка возникает в ходе установки автоматического типа пароля на профиль пользователя	Посмотрите файлы журнала для подробной информации
6	Непредвиденная ошибка в процессе изменения пароля	Ошибка возникает в ходе смены или установки пароля на профиль	1) Создайте профиль с другим именем. 2) Пересоздайте электронный ключ JaCarta с заданным именем
7	Сертификат не выбран	Ошибка возникает, когда сертификат не был выбран из таблицы сертификатов	Удостовериться, что сертификат выбран из таблицы сертификатов
8	Непредвиденная ошибка в процессе	Обобщённая ошибка, которая выводится в случае наличия других ошибок в ходе установки	Посмотрите файлы журнала для подробной информации

№ п/п	Ошибка	Описание	Действие оператора
	включения аутентификации	двухфакторной аутентификации на профиле	
9	На выбранном токене профили для аутентификации отсутствуют	Ошибка выводится в случае, когда отсутствуют профили на электронном ключе JaCarta	1) Проверьте наличие профилей на электронном ключе JaCarta. 2) В случае отсутствия создайте профиль
10	Непредвиденная ошибка в процессе синхронизации профиля	Ошибка возникает в процессе синхронизации операций, которые ввёл оператор на профиль, находящийся на слоте электронный ключ JaCarta	1) Проверьте, что электронный ключ JaCarta подсоединён к компьютеру. 2) Удостоверьтесь, что электронный ключ JaCarta правильно определился в системе средствами Единого Клиента JaCarta. 3) Проверьте наличие профиля в памяти электронного ключа JaCarta. 4) Перезапустите SecurLogon. 5) Переустановите SecurLogon
11	Не выбран профиль	Ошибка возникает, когда оператор пытается перейти на форму, при этом не выбрав профиль	Удостоверьтесь, что выбран профиль из таблицы профилей
12	Сертификат не создан	Ошибка возникает, когда не получилось создать сертификат на электронном ключе JaCarta	1) Проверьте, что электронный ключ JaCarta подсоединён к компьютеру. 2) Удостоверьтесь, что электронный ключ JaCarta правильно определился в системе средствами Единого Клиента JaCarta. 3) Проверьте наличие сертификата в памяти электронного ключа JaCarta. 4) Перезапустите SecurLogon. 5) Переустановите SecurLogon
13	Профиль не создан	Ошибка возникает, когда не получилось создать профиль на электронном ключе JaCarta	1) Проверьте, что электронный ключ JaCarta подсоединён к компьютеру. 2) Удостоверьтесь, что электронный ключ JaCarta правильно определился в системе средствами Единого Клиента JaCarta. 3) Проверьте наличие профиля в памяти электронного ключа JaCarta. 4) Перезапустите SecurLogon. 5) Переустановите SecurLogon
14	Пароль меньше 14 символов!	Ошибка возникает, когда пароль не удовлетворяет требованиям безопасности	1) Введите пароль, который удовлетворяет требованиям безопасности. Длина пароля, должна быть не меньше 14 символов, должны присутствовать строчные буквы и все буквы должны быть латинскими.
15	Имя пользователя не может быть пустым Имя хоста не может быть пустым	Ошибка возникает, когда не были введены имя пользователя или имя хоста в процессе: - создания ярлыка для удалённого доступа; - создания профиля; - создания сертификата	Заполнить поля «Имя пользователя» или «Имя хоста»
16	Профиль с указанным именем уже существует	Ошибка возникает в процессе, когда профиль с указанным именем	1) Создайте профиль с другим именем.

№ п/п	Ошибка	Описание	Действие оператора
		уже создан в памяти электронного ключа JaCarta	2) Удалите профиль с заданным именем и создайте новый.
17	Сертификат не удален	Ошибка возникает, когда не получилось удалить сертификат на электронном ключе JaCarta	Дублирует ошибку №10
18	Профиль не удален	Ошибка возникает, когда не получилось удалить профиль на электронном ключе JaCarta	Дублирует ошибку №11
19	Профиль не отредактирован	Ошибка возникает, когда не получилось загрузить изменения профиля на электронный ключ JaCarta	1) Проверьте, что электронный ключ JaCarta подсоединён к компьютеру. 2) Удостоверьтесь, что электронный ключ JaCarta правильно определился в системе средствами Единого Клиента JaCarta. 3) Пересоздайте профиль в памяти электронного ключа JaCarta. 4) Перезапустите SecurLogon. 5) Переустановите SecurLogon
20	Не удалось синхронизировать пароли на электронном ключе JaCarta и в системе	Ошибка возникает, когда не получилось изменить пароль системного пользователя на пароль профиля	Дублирует ошибку №17.

21	Непредвиденная ошибка в процессе проверки	Ошибка возникает, когда не получилось получить тикет Kerberos на контроллере домена	1) Попробуйте вручную подключиться к контроллеру домена:
			`root#: kinit $(администратор)@$(домен)`
			2) Проверьте, что компьютер пользователя видит компьютер контроллера домена:
			`root#: ping $(администратор)@$(домен)`
			`root#: ping $(ip-адрес контроллера домена)`

22	IP-адрес введён некорректно	Ошибка возникает, когда IP-адрес введён некорректно	Ввести корректный IP-адрес по шаблону: x.x.x.x, где x – это число от 1до 255.
23	Ярлык для запуска удаленной сессии не создан	Ошибка возникает, когда не получилось создать ярлык удалённого доступа в указанном месте	1) Выясните права доступа к указанному месту: `root#: l $(место, куда будет сохранен ярылк)` 2) Укажите другое место, где можно создать ярлык
24	Непредвиденная ошибка в процессе форматирования электронный ключ JaCarta	Ошибка возникает, когда не получилось отформатировать указанный электронный ключ JaCarta	1) Проверьте, что электронный ключ JaCarta подсоединён к компьютеру. 2) Переустановите SecurLogon

№ п/п	Ошибка	Описание	Действие оператора
25	Поля «Новый PIN-код пользователя» и «Подтверждение PIN-кода» не совпадают	Ошибка возникает, когда введенные PIN-коды пользователя не совпадают	Проверьте идентичность PIN-кодов в полях «Новый PIN-код пользователя» и «Подтверждение PIN-кода»
26	Непредвиденная ошибка в процессе сохранения конфигурации	Ошибка возникает, когда не получилось сохранить изменения в файле `/usr/local/etc/jcsecurlogon/jcsecurlogond.conf`	1) Проверьте существование конфигурационного файла командой: `root#: ls usr/local/etc/jcsecurlogon/`
			2) Измените права доступа к файлу: `root#: chmod 600 usr/local/etc/jcsecurlogon/jcsecurlogond.conf` 3) Переустановите SecurLogon
27	Введен некорректный PIN-код	Ошибка возникает, когда введенный PIN-код не соответствует PIN-коду на слоте электронного ключа JaCarta	Введите верный PIN-код
28	Ошибка доступа к электронному ключу JaCarta. Код возврата: 244 (в слоте отсутствует электронный ключ JaCarta)	Ошибка возникает, когда пользователь пытается подключиться к удалённому рабочему столу без электронного ключа JaCarta. Код возврата: `CKR_TOKEN_NOT_PRESENT` - в слоте отсутствует электронный ключ JaCarta	Подключите электронный ключ JaCarta и повторите вход
29	Сертификат на электронном ключе не соответствует пользователю, для которого создан сертификат	Ошибка возникает, когда не получается верифицировать сертификат на электронном ключе JaCarta	Проверьте валидность сертификата на электронном ключе JaCarta
30	Ошибка в процессе проверки сессии удаленного доступа. Возможно, указанный сервер отсутствует в сети	Ошибка возникает, когда невозможно найти указанный сервер в сети или профиль на электронном ключе JaCarta не соответствует нужному пользователю	1) Проверьте адрес сервера. 2) Проверьте данные профиля на электронном ключе JaCarta
31	Дней до окончания действия лицензии - XX	Ошибка возникает, когда осталось = <30 дней до окончания действия лицензии	Рекомендуется обновить лицензию согласно разделу 7 настоящего руководства
32	Действие лицензии окончено. ASL будет отключен. Компьютер будет перезагружен через 5 секунд	Ошибка возникает, когда действие лицензии закончено	Рекомендуется загрузить новую лицензию согласно разделу 7 настоящего руководства
33	Обнаружена ошибка с лицензией! ASL будет отключен.	Ошибка возникает, когда обнаружена ошибка с файлом лицензии	Рекомендуется загрузить новую лицензию согласно разделу 7 настоящего руководства

№ п/п	Ошибка	Описание	Действие оператора
	Компьютер будет перезагружен через 5 секунд		

11.4 Журнал событий

Произошедшие события записываются в журнал событий, который представляет собой файл с расширением `.log`, расположенный в папке `var/log/jcsecurlogon`. Доступ к папке осуществляется от имени администратора ОС.

Файл регистрации событий в текстовом формате содержит записи об определенных событиях программы с указанием времени их наступления и дополнительных сведений – имени хоста, названия сервиса, инициировавшего запись сообщения в log-файл, и категории сообщений (WARNING, INFO, Успех). Для просмотра LOG-файла можно воспользоваться простым текстовым редактором, таким как »Блокнот«.

12. Удаление программы

Удалить программу SecurLogon можно с помощью скрипта ПО SecurLogon из терминала.

Для удаления ПО SecurLogon выполните команду из папки, в которую ранее была произведена распаковка архива:

```
sudo ./uninstall.sh
```

Удаление программы с помощью скрипта позволяет полностью очистить систему от остатков программы. После завершения удаления рекомендуется перезагрузить компьютер, чтобы убедиться, что все файлы были удалены.

Приложение А. Тема SecurLogon

А.1 Окно входа пользователя в операционную систему

Тема SecurLogon входа пользователя в ОС перед началом сеанса, представлена в виде графического окна на весь экран (см. Рисунок 148) для аутентификации в ОС с использованием средств двухфакторной аутентификации JaCarta или с использованием комбинации логина и пароля. Экран входа в систему отображает текущий механизм входа в зависимости от настроенного администратором метода, определенным в процессе настройки ПО SecurLogon.

Фоновое изображение графического окна темы SecurLogon отображается в формате .png или .jpg и может быть кастомизировано путем задания пути до устанавливаемого фонового изображения в конфигурационном файле /etc/xdg/AladdinRD/jcpkcs11.conf или путем добавления фонового изображения в папку /etc/xdg/AladdinRD/. Новое фоновое изображение будет применено при перезагрузке ОС.

Рисунок 148 – Общий вид графического окна темы входа SecurLogon

- В верхней части экрана расположена панель со следующими элементами:
  - текущая дата;
  - текущее время;
  - 

выбранный язык ввода, который можно изменить на английский или русский язык одним нажатием левой кнопки мыши на иконку;
  -  индикация сети с возможностью выбора сетевого подключения (см. Рисунок 149);

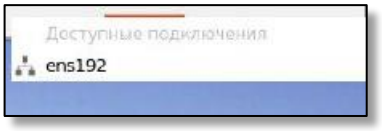

Рисунок 149 – Выбор сетевого подключения

  - для появления скрытой кнопки  <Настройка> на панели в верхней части экрана необходимо пять или более раз нажать на иконку 

в левом верхнем углу экрана. Кнопка <Настройка> появится в верхней панели (см. Рисунок 150).

Рисунок 150 – Окно входа SecurLogon с дополнительной кнопкой <Настройка>

- По нажатию на кнопку <Настройка> в появившемся подменю возможно (см. Рисунок 151):
  - выбрать графическую оболочку;

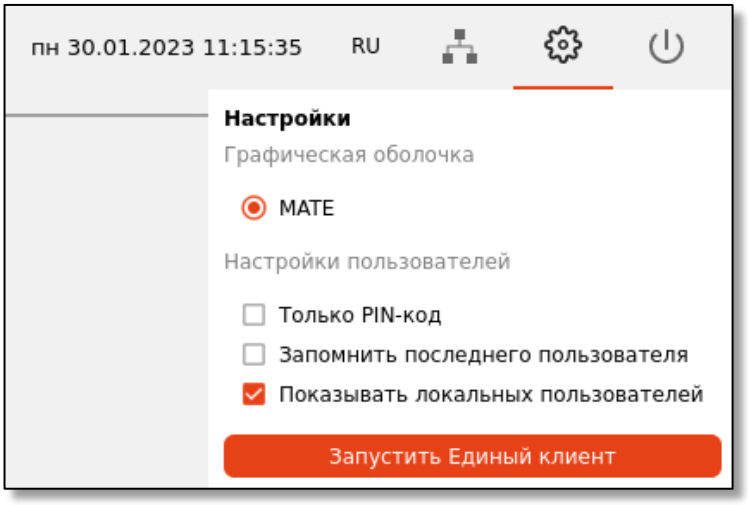

Рисунок 151 – Меню настройки

  - произвести настройку политики входа пользователя. После проставления флага в поле «Только PIN-код» для входа в ОС будет требоваться электронный ключ и ввод PIN-кода на экране входа в систему в поле «PIN-код». При снятии флага вход осуществляется в соответствии с настроенной политикой входа;
  - произвести настройку сохранения последнего успешно аутентифицированного пользователя. После проставления флага в поле «Запомнить последнего пользователя» при следующем включении компьютера на экране входа пользователя в ОС в поле «Имя пользователя» будет отображено имя пользователя, последним заходившего в систему;
  - расширить выбор учётных записей пользователей на экранной форме. После проставления флага в поле «Показывать локальных пользователей» появляются доступные для выбора учетные записи локальных пользователей в поле «Имя пользователя»;
  - запуск «Единого клиента». По нажатию на кнопку <Запустить единый клиент> происходит запуск одноимённого ПО поверх окна входа в систему.
- управление питанием – выключение или перезагрузка компьютера (см. Рисунок 152).

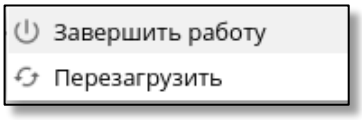

Рисунок 152 – Меню действий с электропитанием

- В центре экрана располагается панель ввода параметров входа в систему (см. Рисунок 153).

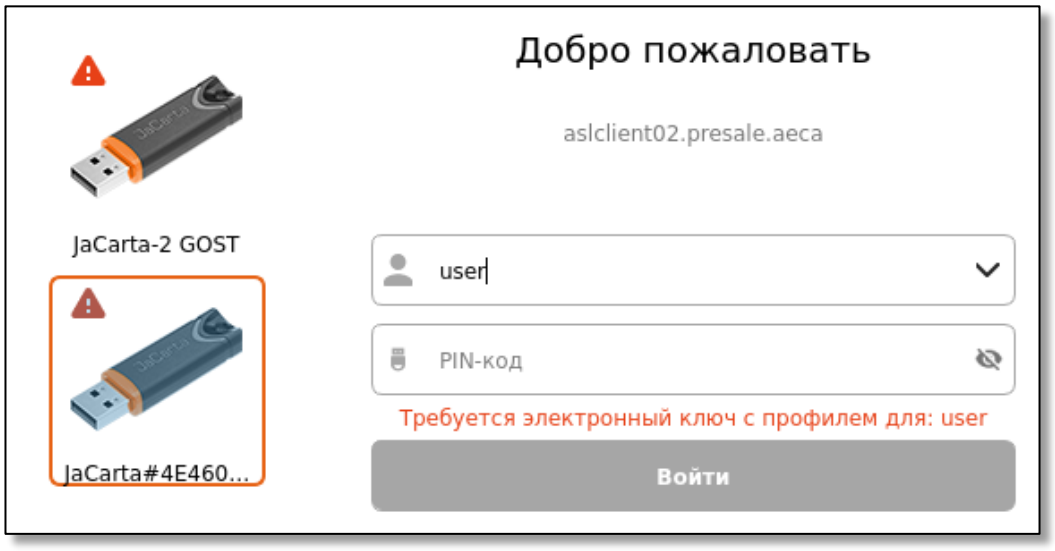

Рисунок 153 – Панель ввода аутентификационных данных

В левой части экранной панели отображены приложения подключенного электронного ключа. Электронный ключ, на котором выбран сертификат, подсвечивается. восклицательный знак возле ключа свидетельствует о том, что присоединенный электронный ключ не содержит аутентификационных данных. При отсутствии подключенных электронных ключей ожидается вход в ОС с использование пароля пользователя.

В правой части экранной панели отображены:

- поле для выбора пользователя из выпадающего списка – имя пользователя считывается из поля «CN» выбранного сертификата с указанием домена текущего ПК при сетевой аутентификации или имени ПК при локальной аутентификации. Также доступен ввод имени пользователя с клавиатуры;
- поле ввода пароля или PIN-кода, в соответствии с назначенной политикой входа, для выбранного пользователя. Максимальное количество неверных последовательных попыток ввода PIN-кода пользователя, после которого возможность использования PIN-кода пользователя будет заблокирована, определяется при настройке параметров токена в ПО «Единый Клиент JaCarta». Количество попыток ввода пароля пользователя не ограничено.
- поле вывода уведомлений об ошибках аутентификации. Возможны следующие уведомления:
  - Отсутствует подключение к контроллеру домена! Пожалуйста, проверьте подключение к сети или доступность домена (ошибка сети);
  - Пользователь не найден в домене (неверное имя пользователя);
  - Неправильно введен PIN-код пользователя (введен не верный PIN-код);
  - Ошибка аутентификации (введен не верный пароль);
  - Пользователь User заблокирован!
  - Электронный ключ заблокирован!

A.2 Вход в ОС после применения настройки сетевой аутентификации с использованием OTP

После применения выбранных настроек для входа в ОС необходимо:

- ввести доменное имя пользователя в поле «Имя пользователя»;
- ввести доменный пароль пользователя в поле «Пароль»;
- выбрать способ OTP аутентификации (в зависимости от настройки JAS-сервера может быть доступна аутентификация по одноразовому коду PUSH, OTP числовому паролю или коду из sms-сообщения) (см. Рисунок 154);

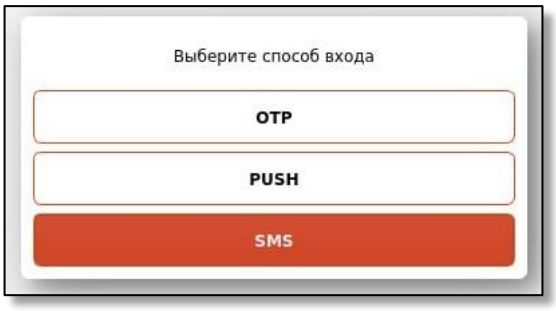

Рисунок 154 – Окно входа в ОС. Выбор способа аутентификации

- при выборе аутентификации по OTP-токену необходимо ввести одноразовый пароль, генерируемый программным токеном Aladdin 2FA или google authenticator для смартфонов под управлением iOS, Android, Windows (см. Рисунок 94);

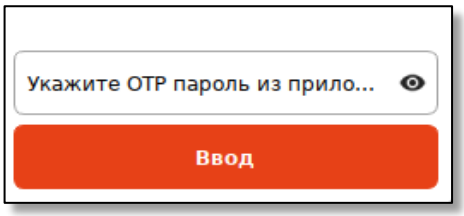

Рисунок 155 – Окно входа в ОС. Ввод OTP пароля

- при выборе аутентификации по Push-токену необходимо ввести одноразовый пароль, генерируемый программным токеном Aladdin 2FA или google authenticator для смартфонов под управлением iOS, Android, Windows, и подтвердить запрос на вход в программном токене;
- при выборе аутентификации по sms-сообщению необходимо ввести одноразовый пароль из полученного смс-сообщения.

А.3 Окно блокировки открытого сеанса пользователя

В случаях извлечения электронного ключа в процессе открытого пользовательского сеанса или бездействия пользователя в течение заданного в системе времени в процессе открытого пользовательского сеанса, клиентская ОС будет автоматически заблокирована. Это позволяет пользователям покидать рабочее место, забрав электронный ключ с собой, но оставляя открытым защищенный сеанс.

Для возобновления сеанса без необходимости входить снова в систему в зависимости от настроенной политики безопасности нужно:

- вставить электронный ключ и ввести PIN-код в окне блокировки экрана (см. Рисунок 156);

Рисунок 156 – Окно блокировки открытого сеанса пользователя

- или ввести пароль для учетной записи текущего пользователя, предварительно вызвав скрытую кнопку <Настройка>, кликнув 5 или более раз по иконке в левом верхнем углу экрана блокировки и сняв отметку с поля «Только PIN-код» (см. Рисунок 157).

Рисунок 157 – Окно блокировки открытого сеанса пользователя. Кнопка «Настройка»

- В верхней части экрана расположена панель со следующими элементами:
  - текущая дата;
  - текущее время;
  - EN выбранный язык ввода, который можно изменить на английский или русский язык одним нажатием левой кнопки мыши на иконку;
  - переход на экран входа для смены пользователя. Текущий сеанс пользователя не завершается. По нажатию на кнопку происходит переход в «Окно входа».
  - управление питанием – выключение или перезагрузка компьютера (см. Рисунок 158).

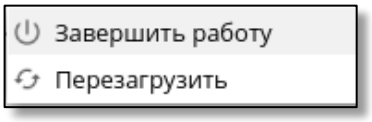

Рисунок 158 – Меню действий с электропитанием на экране блокировки

- Фоновое изображение графического окна блокировки отображается в формате .png или .jpg и может быть настроено путем задания пути до устанавливаемого фонового изображения в конфигурационном файле /etc/xdg/AladdinRD/jcpkcs11.conf или путем добавления фонового изображения в папку /etc/xdg/AladdinRD/. Новое фоновое изображение будет применено после перезагрузки ОС.

А.4 Двухфакторная аутентификация пользователя при заблокированном электронном ключе

В случае, если при аутентификации используется ранее заблокированный токен или электронный ключ был заблокирован в результате многократного неверного введения PIN-кода в панели аутентификационных данных, происходит автоматическое открытие ПК «Единый клиент JaCarta» для настройки и работы с токеном (см. Рисунок 159).

Пользователю доступно только окно ПК «Единый клиент JaCarta» разблокировки и смены PIN-кода электронного ключа с уведомлением о необходимости обратиться к администратору.

Выход из окна ПК «Единый клиент JaCarta» осуществляется по нажатию на кнопку Выход

Рисунок 159 – Окно входа SecurLogon с использованием заблокированного электронного ключа

Для разблокировки электронного ключа необходимо обратиться к администратору, который в окне «Единого клиента JaCarta» может разблокировать электронный ключ, выполнив корректный ввод пароля администратора и задав новый PIN-код пользователя (см. Рисунок 160).

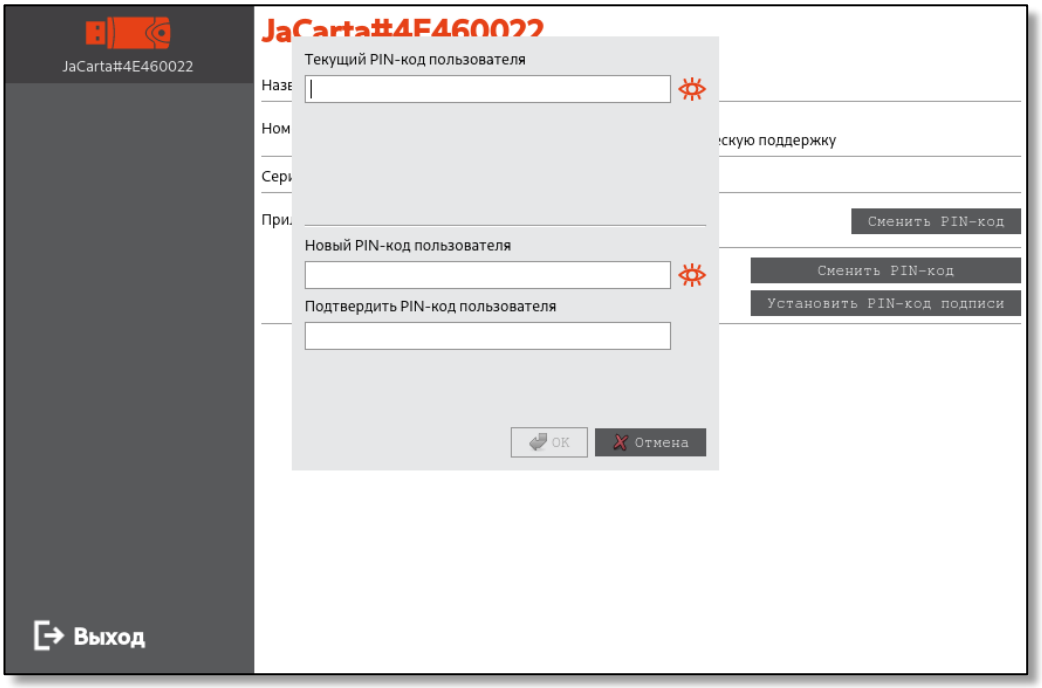

Рисунок 160 – Окно «Единого клиента JaCarta» для ввода PIN-кода

В результате успешной разблокировки PIN-кода администратор будет уведомлен сообщением (см. Рисунок 161).

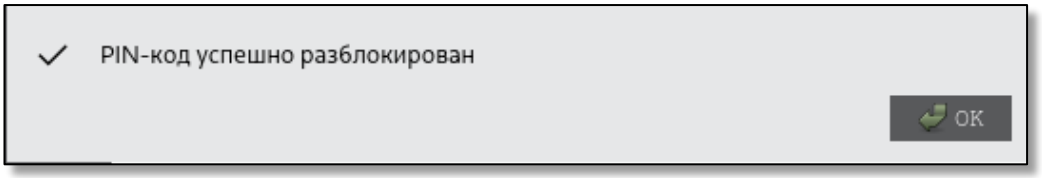

Рисунок 161 – Окно уведомления об успешной разблокировке токена

После разблокировки электронного ключа выполните корректный ввод аутентификационных данных.

А.5 Двухфакторная аутентификация пользователя при подключении к удаленному компьютеру

Для подключения к удалённому компьютеру с использованием двухфакторной аутентификации пользователь должен подсоединить электронный ключ JaCarta и запустить ранее созданный ярлык на рабочем столе (см. Рисунок 162).

Рисунок 162 – Ярлык запуска удаленного подключения

Затем в открывшемся окне ввести PIN-код пользователя (см. Рисунок 163). Значение PIN-кода по умолчанию при поставке приведены в таблице 3, раздела 3.2 RU.АЛДЕ.03.01.013-01 32 01-2 «Единый Клиент JaCarta. Руководства администратора «Аладдин Р.Д. « [1] в зависимости от используемого апплета. Настройка PIN-кода электронного ключа осуществляется при помощи ПО «Единый Клиент JaCarta» и подробно описано в разделе 10 RU.АЛДЕ.03.01.013-01 32 01-2 «Единый Клиент JaCarta. Руководства администратора «Аладдин Р.Д. « [1].

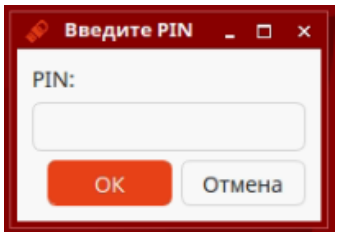

Рисунок 163 – Окно запроса PIN-кода для удаленного подключения

Далее откроется окно, предоставляющее удалённый доступ к целевому рабочему месту.

Если при подключении к удалённому компьютеру с использованием двухфакторной усиленной аутентификации (без PKI) выяснится, что пароль на профиле не совпадает с паролем доменного пользователя, пользователю будет предложено заменить пароль (см. Рисунок 164).

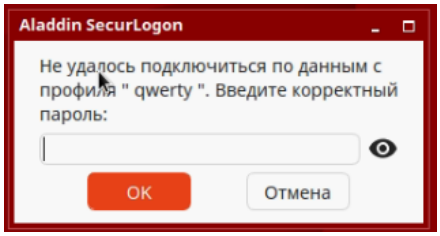

Рисунок 164 – Смена пароля

После ввода пароля и нажатия кнопки <OK> появится сообщение «Пароль успешно изменен! « (см. Рисунок 165) и произойдёт повторное подключение к удалённому компьютеру с новым паролем.

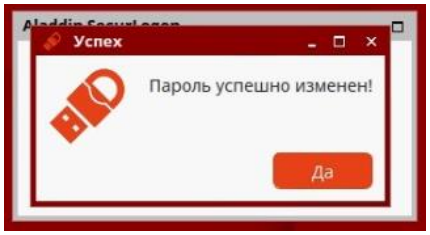

Рисунок 165 – Сообщение «Пароль успешно изменён! «

Если при подключении к удалённому компьютеру с использованием двухфакторной усиленной аутентификации (без PKI) выяснится, что на электроном ключе JaCarta отсутствует нужный профиль, то пользователю будет предложено создать его (см. Рисунок 166).

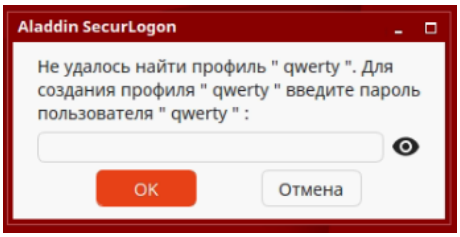

Рисунок 166 – Создание профиля

После ввода пароля профиля и нажатия кнопки <OK>, появится сообщение «Профиль успешно создан» (см. Рисунок 167) и произойдёт повторное подключение к удалённому компьютеру.

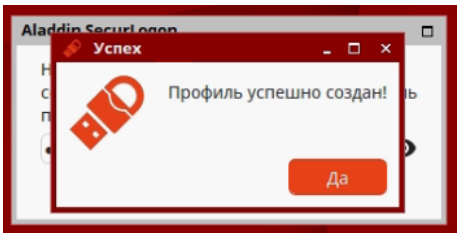

Рисунок 167 – Сообщение «Профиль успешно создан»

Приложение Б. Правила формирования пароля

Правила формирования пароля при вводе с клавиатуры или формирования пароля по кнопке <Сгенерировать> приведены в Таблица 11.

Таблица 11 – Правила формирования паролей

Характеристика	Метод генерации пароля	
	ввод с клавиатуры	автоматическая генерация
длина	от 8 до 63 символов	- от 14 до 63 символов; - 63 символа в случае генерации без возможности задания длины
допустимые символы	все печатные символы ASCII (кроме символов псевдографики), определенные международным стандартом ISO/IEC10646 (Блок «C0 Controls and Basic Latin»).	
сложность	обязательно должен содержать цифры, строчные и прописные буквы	требований нет, формируется случайным выбором допустимых символов

Термины и определения

Аутентификация: Действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации.

Вторичная идентификация: Действия по проверке существования (наличия) идентификатора, предъявленного субъектом доступа при доступе, в перечне идентификаторов доступа, которые были присвоены субъектам доступа и объектам доступа при первичной идентификации.

Идентификация: Действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Интерфейс: Взаимосвязь между двумя или более объектами (типа ЭКПО/ЭКПО, ЭКПО/ЭКА, ЭКПО/пользователь или между модулями ПО), которые совместно используют и обеспечивают данные или обмениваются ими.

Одноразовый пароль: Однократно используемый пароль.

Пароль: Конфиденциальная аутентификационная информация, обычно состоящая из строки знаков.

Программа: Данные, предназначенные для управления конкретными компонентами системы обработки информации в целях реализации определенного алгоритма.

Пользователь (программного средства): Физическое лицо, первичная идентификация которого выполнена в конкретной среде функционирования.

Простая аутентификация: Аутентификация с применением метода однофакторной односторонней аутентификации и соответствующих данному методу протоколов аутентификации.

Протокол аутентификации: Протокол, позволяющий участникам процесса аутентификации осуществлять аутентификацию.

Профиль пользователя: Совокупность имени и пароля пользователя, сохранённая в защищённом разделе устройства аутентификации.

Среда функционирования: Среда с предопределенными (установленными) граничными условиями, в которой существуют (функционируют) и взаимодействуют субъекты и объекты доступа.

Строгая аутентификация: Аутентификация с применением только метода многофакторной взаимной аутентификации с использованием криптографических протоколов аутентификации.

Усиленная аутентификация: Аутентификация с применением метода многофакторной односторонней или взаимной аутентификации и соответствующих данному методу протоколов аутентификации.

Устройство аутентификации (электронный ключ, токен): аппаратное средство, предназначенное для защиты программного обеспечения и данных от копирования, нелегального использования и несанкционированного распространения.

Обозначения и сокращения

АРМ	–	Автоматизированное рабочее место
ОС	–	Операционная система
ПК	–	Персональный компьютер
ПО	–	Программное обеспечение
AD	–	Active Directory (служба каталогов корпорации Microsoft для операционных систем семейства Windows Server)
OTP	–	One Time Password (одноразовый пароль)
PIN	–	Personal Identification Number (персональный идентификационный номер)
RDP	–	Remote Desktop Protocol (протокол удалённого рабочего стола)

Перечень ссылочных документов

1. RU.АЛДЕ.03.01.013-01 32 01-2 «Единый Клиент JaCarta». Руководством администратора для операционных систем семейства Linux.

2. «Операционная система «РЕД ОС». Руководство администратора» RU.29926343.02.01-01 32 1-1.

3. «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора» РУСБ.10015-01 95 01-2.

4. «Операционная система «Альт 8 СП». Руководство администратора» ЛКНВ.11100-01 90 01.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					

Тел.: +7 (495) 223-00-01 E-mail: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru