Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice

Руководство по эксплуатации
Часть 1

Руководство администратора

Версия	1.0
Статус	Публичный
Дата	30.11.2021
Обозначение	АЛДЕ.467669.011РЭ1
Листов	92

Оглавление

1. О документе

1.1 Назначение документа

Документ АЛДЕ.467669.011РЭ1 "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice. Руководство по эксплуатации. Часть 1. Руководство администратора" предназначен для описания работы администратора со средством защиты информации "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice" (далее – средство, Aladdin LiveOffice, изделие) и включает в себя:

- сведения, описывающие конструкцию, характеристики, а также принципы работы средства;
- описание действий по приемке средства;
- описание действий по учёту СЗИ и СКЗИ из состава изделия;
- описание действий по безопасной установке программ, обеспечивающих функционирование средства на рабочем месте администратора;
- описание действий по настройке средств вычислительной техники и системного программного обеспечения на этих средствах, необходимых для корректного функционирования защищенного служебного носителя;
- инструкции, описывающие настройку, обслуживание, обновление, аудит и утилизацию Aladdin LiveToken из состава Aladdin LiveOffice.

В руководство администратора также включены описания, соответствующие *роли "администратор"* и сведения о работе *непривилегированных пользователей*:

- режимы работы средства;
- принципы безопасной работы средства;
- описание функций и интерфейсов функций средства доступных ролям «пользователь» и "администратор";
- описание настроек безопасности, доступных ролям "пользователь" и "администратор";
- типы событий безопасности изделия.

1.2 На кого ориентирован данный документ

Настоящий документ ориентирован на сотрудников организации, ответственных за приёмку, ввод в эксплуатацию, эксплуатацию и вывод из эксплуатации средств защиты информации.

Для подготовки ко вводу изделий в эксплуатацию указанные сотрудники должны обладать навыками администрирования системного программного обеспечения (операционных систем), необходимого для функционирования изделия.

Для обеспечения безопасной работы указанные сотрудники должны обладать навыками администрирования корпоративных сетей и средств защиты информации, предназначенных для шифрования траффика (VPN- или TLS-клиенты).

1.3 Документы, рекомендуемые для предварительного прочтения (изучения)

1. Формуляр на "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice" АЛДЕ.467669.011ФО.
2. Формуляр на доверенную операционную систему (зависит от установленной ОС в изделии).
3. Формуляр на VPN/TLS клиент (зависит от установленного VPN/TLS клиента).
4. Формуляр на "VPN/FW "ЗАСТАВА", версия 6". Клиент" МКЕЮ.00433-01 30 02 ФО.

Мы рекомендуем также ознакомиться с прочими эксплуатационными документами на составные части (далее – СЧ) изделия Aladdin LiveOffice.

1.4 Соглашения по оформлению

Таблица 1 – Элементы оформления

Выделение	Используется для выделения наименований полей, блоков, секций, кнопок, вкладок экранных форм
<**Кнопка**>	Используется для выделения кнопок/клавиш
`file.exe`	Используется для выделения имен файлов, каталогов, текстов программ
[1]	Ссылка на пункт в списке литературы (приведен в конце документа)
Гиперссылка	Используется для выделения внешних ссылок
Ссылка, [с. 6]	Используется для выделения перекрестных ссылок
Важно	Используется для выделения информации, на которую следует обратить внимание
	Совет
	Рекомендация
	Примечание

1.5 Термины и определения

Таблица 2 – Термины и определения

Администратор	Уполномоченный пользователь, имеющий административную роль: "Администратор безопасности Aladdin LiveOffice".
Аутентификация	Действия по проверке подлинности идентификатора пользователя. В рамках использования Aladdin LiveOffice под аутентификацией понимается ввод конкретным пользователем данных, необходимых для аутентификации (пароль или PUK-код) и проверка этих данных изделием.
Внутренний канал связи СЗИ	Канал связи между разделёнными частями СЗИ: например, программой администратора безопасности и Aladdin LiveToken [с.13]. Каждая часть средства обеспечения безопасной дистанционной работы обеспечивает выполнение конкретного сервиса и взаимодействует с другими частями через внутренние каналы связи.
Данные пользователя, пользовательская информация	Данные (информация), содержащиеся в ресурсах, защищаемых функциями безопасности Aladdin LiveOffice. К подобным ресурсам относятся: разделы карты памяти (MicroSD-карты) изделия Aladdin LiveToken[1], ключевая и идентификационная информация Aladdin LiveOffice, а также содержимое баз данных, генерируемых программой администратора безопасности [с. 15].
Действительность аутентификационной информации	Соответствие (на момент предъявления) аутентификационной информации, предъявленной пользователем, той аутентификационной информации, которая по сведениям функции безопасности действительно ассоциирована с данным пользователем.
Данные функций безопасности	Данные, предназначенные специально для функций безопасности и используемые функциями безопасности для принятия решения в соответствии с функциональными требованиями безопасности.
Идентификатор	Представление сущности (например, строка символов), однозначно её идентифицирующее. Таким представлением может быть полное или сокращенное имя этого пользователя, псевдоним, численно-символьная последовательность и др. В программах (программных компонентах) из состава изделия идентификаторы пользователей обозначены как логины. Aladdin LiveOffice имеет следующие типы идентификаторов: идентификатор СВТ, идентификатор пользователя, идентификатор Aladdin LiveToken. Идентификатор СВТ создаётся на основе сведений об аппаратной составляющей рабочего места пользователя. В отдельную категорию идентификаторов попадают устанавливаемые администратором идентификаторы, применяемые для авторизации в ИС [с. 26].
Идентификация	Действия по присвоению субъектам и объектам доступа идентификаторов и (или) действия по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.
Инициализация	Под инициализацией понимается процесс записи на конкретный носитель начальных параметров (правил и ключа), заданных в настраиваемом шаблоне, созданном уполномоченным пользователем с ролью «администратор безопасности».

[1] Состав изделия представлен в пункте 2.2.1 на с. 17.

Компания	АО "Аладдин Р. Д."
Контрольная сумма	Некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении.
Логин	Индивидуальный идентификатор конкретного пользователя.
Мастер-ключ	Уникальный набор данных, используемый Aladdin LiveOffice при операциях, связанных с защитой данных. Мастер-ключ используется для создания уникальных наборов данных, предназначенных для разделения ролей и дифференциации контуров.
Обезличивание	Под обезличиванием (стиранием) информации понимается удаление всех персональных данных и параметров инициализации с Aladdin LiveToken.
Параметр безопасности	Под параметрами безопасности (или параметрами функций безопасности) понимаются выбираемые администратором параметры, тем или иным способом влияющие на выполнение изделием функций безопасности.
Пользователь	Физическое лицо (сотрудник, специалист), использующее «Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice».
Права доступа	Права доступа определяют набор возможных действий, которые субъекты доступа (пользователи и процессы) могут выполнять над объектами доступа (составными частями изделия) в конкретной среде функционирования.
Правила управления доступом (правила)	Правила, регламентирующие условия доступа пользователей к объектам на основе прав доступа.
Программа (программный компонент)	Представленная в объективной форме совокупность данных и команд, предназначенных для функционирования средств вычислительной техники и других компьютерных устройств с целью получения определённого результата, включая подготовительные материалы, полученные в ходе разработки программы для СВТ, и порождаемые ею аудиовизуальные отображения.
Программное средство	Программа, предназначенная для многократного применения на различных объектах, разработанная любым способом и снабжённая программной документацией.
Программное обеспечение	Совокупность программ (программных средств) системы обработки информации (средства вычислительной техники, средства защиты информации, объекта оценки и т.п.) и программных документов, необходимых для эксплуатации этих программ.
Политика безопасности	Одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.
Политика функций безопасности	Совокупность правил, описывающих конкретный режим безопасности, реализуемый функциями безопасности объекта оценки, и выраженных в виде совокупности функциональных требований безопасности.
Роль	Заранее определённая совокупность правил, устанавливающих допустимые взаимодействия субъекта доступа, действующего в данной "роли", и объекта доступа.
Системное программное средство	Управляющее программное средство, которое обеспечивает распределение ресурсов средства вычислительной техники, планирование выполнения задач (прикладных программ), ввод-вывод

	данных, управление данными и прикладными программными средствами, взаимодействие с пользователем. К системным программным средствам в настоящем документе относятся операционные системы, установленные на конкретных средствах вычислительной техники.
Среда функционирования	Среда, в которой функционирует изделие. В качестве среды функционирования для "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice" выступает средство вычислительной техники. Подробнее о средах функционирования различных составных частей изделия в разделе "Особенности реализации" [с.15].
Средство вычислительной техники (СВТ)	Комплекс технических (аппаратных) и программных средств, предназначенный для автоматической обработки информации в процессе решения вычислительных и информационных задач. Наиболее часто – персональный компьютер (ПК или ноутбук).
События безопасности	Событие информационной безопасности: идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер или возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.
Субъект доступа	Активные сущности, которые выполняют операции над объектами.
Сущность	Человек, группа, устройство или процесс, принимающая участие в работе изделия "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice".
Уполномоченный пользователь	Пользователь, который обладает правами и/или привилегиями, необходимыми для выполнения операций. Уполномоченному пользователю разрешается выполнять конкретную операцию или совокупность операций в соответствии с функциональными требованиями безопасности и его ролью.
Функция безопасности	Совокупность функциональных возможностей аппаратного, программного и программно-аппаратного обеспечения, на которые как непосредственно, так и косвенно возложено обеспечение безопасности, и которые необходимо для корректной реализации функциональных требований безопасности.
Функциональные требования безопасности	Перечень требований безопасности к функциям безопасности, определяющий правила, по которым "Aladdin LiveOffice" или СВТ взаимодействуют с информацией и сервисами из их состава.
Целостность	Свойство, отражающее наличие и неизменность объекта при выполнении операций над ним.

1.6 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.

1.7 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 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.

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

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 ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

2. Описание и работа изделия

Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice – это программно-аппаратный комплекс на базе специализированного защищённого USB-устройства с набором предустановленного системного и прикладного ПО.

ПАК предназначен для загрузки доверенной операционной системы на рабочем месте пользователя и создания защищённого соединения между этим рабочим местом и удалённым компьютером: рабочим СВТ, расположенным в корпоративной сети или имеющим подключение, например, к ГИС.

2.1 Общее описание изделия

2.1.1 Наименование и обозначение

Полное наименование изделия: Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice.

Краткое наименование изделия: Aladdin LiveOffice.

Обозначение изделия: АЛДЕ.467669.011.

Тип устройства: программно-техническое средство защиты информации (средство обеспечения безопасной дистанционной работы).

2.1.2 Назначение изделия

Основным назначением Aladdin LiveOffice является организация безопасной дистанционной работы пользователей с вычислительными и информационными ресурсами автоматизированной (информационной) системы посредством использования вычислительных ресурсов локального средства вычислительной техники[2]

В рамках выполнения своей основной функции изделие обеспечивает:

- идентификацию и аутентификацию пользователей и устройств;
- защиту функций безопасности;
- защиту данных пользователя;
- управление работой и параметрами, а также разграничение доступа к управлению функциями безопасности (управление работой и параметрами);
- аудит событий безопасности;
- загрузку доверенной операционной системы;
- подключение к удалённому рабочему столу;
- сигнализация о работоспособности USB-носителя;
- запись и хранение информации;
- поддержку выполнения требований к АС, ГИС, ИСПДн и др. ИС, в которых хранится и обрабатывается информация, не содержащая сведений, составляющих государственную тайну.

[2] В качестве локального средства вычислительной техники рассматриваются средства вычислительной техники (персональный компьютер, портативный переносной персональный компьютер (ноутбук), планшетный переносной персональный компьютер (планшет), ультрапортативные переносной персональный компьютер (нетбук) на базе архитектуры x64) находящиеся в личном пользовании физического лица, которое является уполномоченным пользователем автоматизированной (информационной) системы. Требования к данным средства вычислительной техники приведены в разделе 3 "Требования к среде функционирования составных частей Aladdin LiveOffice".

При использовании на СВТ, входящих в ИС, компонентов Aladdin LiveOffice ПК "Единый клиент JaCarta", Aladdin SecurLogon, а также реализации доверенных цифровых сертификатов, обеспечивается:

- реализация строгой или усиленной двухфакторной аутентификации в информационной системе.

Aladdin LiveOffice применимо для подключения к удалённым рабочим местам находящимся под управлением ОС семейств Windows и Linux.

2.1.2.1 Область применения

Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice применяется при обработке информации, не содержащей сведения, составляющие государственную тайну, и может использоваться при реализации требований по защите информации от несанкционированного доступа для автоматизированных систем классов защищенности 1Г, 1Д, 2Б, 3Б.

Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice может применяться:

- при реализации мер защиты в государственных информационных системах до 1-го класса защищенности включительно;
- при обеспечении до 1-го уровня защищенности персональных данных, включительно, при их обработке в информационных системах персональных данных;
- при реализации мер защиты в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до 1-го класса защищенности включительно;
- в значимых объектах критической информационной инфраструктуры до 1-ой категории включительно;
- в информационных системах общего пользования II класса.

Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice применяется при обработке информации, содержащей следующие сведения конфиденциального характера, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами в том числе, но не ограничиваясь:

- налоговая тайна;
- банковская тайна;
- врачебная тайна;
- нотариальная тайна;
- адвокатская тайна;
- аудиторская тайна;
- тайна страхования;
- тайна связи;
- тайна следствия;
- отдельные сведения при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд;
- информация о новых решениях и технических знаниях (результаты интеллектуальной деятельности);
- секрет производства (ноу-хау);
- сведения о должнике;
- информация о получателе социальных услуг;
- информация в профилях и индикаторах рисков, применяемых таможенными органами.

2.2 Особенности реализации

2.2.1 Состав изделия

Каждое из исполнений изделия включает в свой состав:

- Флеш-накопитель Aladdin LiveToken.
- Доверенная операционная система (сертифицирована не менее чем по 4 уровню доверия).
- Средство криптографической защиты информации, передаваемой в канале связи (VPN/TLS клиент, прошедший процедуру оценки соответствия требованиям ФСБ России).
- Программа Aladdin SecurLogon.
- Программа Aladdin SecureAdmin.
- Программный комплекс "Единый Клиент JaCarta", применяемый для работы с дополнительными компонентами флеш-накопителя Aladdin LiveToken.
- Средство криптографической защиты информации "Криптотокен 2 ЭП".

Изделие Aladdin LiveToken – внешнее запоминающее устройство, предназначенное для хранения программ, служебной информации и информации пользователя, а также их обработки. В состав Aladdin LiveToken входят:

1. Аппаратная платформа JaCarta-2.
2. Встроенное программное обеспечение LiveEOS.
3. Специальное программное обеспечение LiveBoot.

2.2.2 Варианты поставки изделия

Aladdin LiveOffice может поставляться в различных вариантах, отличающихся: комплектностью, назначением, перечнем действующих сертификатов.

При поставке изделия Aladdin LiveOffice делятся на носители пользователей и носители администраторов (Aladdin LiveAdmin). Для администрирования носителей пользователей нужен как минимум один носитель администратора Aladdin LiveAdmin.

Обозначения и назначение программных, аппаратных и программно-аппаратных составных частей изделия, на которые распространяется данное руководство администратора, представлены в таблице 3.

Совместно с изделием поставляются следующие комплекты:

- комплект эксплуатационной документации;
- комплект сертификатов на изделие и его составные части.

Таблица 3 – Состав изделия в разных исполнениях (в зависимости от выбранной ОС и VPN/TLS клиента)

Наименование компонента	Обозначение компонента	Назначение компонента
Программно-аппаратный комплекс LiveTSM. Исп. 1	АЛДЕ.467669.013-01	Средство загрузки доверенной операционной системы с носителя (изделия) Aladdin LiveToken
Изделие Aladdin LiveToken (совокупность изделий LiveToken называется «(машинные) носители информации»)	АЛДЕ.467669.012-01 Изделие Aladdin LiveToken	Внешнее запоминающее устройство, предназначенное для хранения программных компонент, служебной информации и информации пользователя, а также их обработки (передачи между составными частями Aladdin LiveOffice), в том числе хранения и запуска предустановленной безопасной ОС на личном СВТ пользователя
Аппаратная платформа JaCarta-2	АЛДЕ.467359.001-02 Аппаратная платформа JaCarta-2. Исполнение 2.	Аппаратная платформа, включающая следующие основные компоненты: микроконтроллер общего назначения, микроконтроллер смарт-карты, карта памяти (microSD)
Встроенное программное обеспечение LiveEOS	АЛДЕ.01.01.001-07 Встроенное программное обеспечение LiveEOS. Исполнение 1.	Встроенное программное обеспечение, обеспечивающее работу изделия Aladdin LiveToken и его связь с средством вычислительной техники
Специальное программное обеспечение LiveBoot	RU.АЛДЕ.04.09.030-01 Специальное программное обеспечение LiveBoot	Программное обеспечение, предназначенное для загрузки установленной (сконфигурированной) операционной системы с USB-носителя

Наименование компонента	Обозначение компонента	Назначение компонента
Гостевая операционная система LiveOS	Доверенная ОС должна быть сертифицирована не менее чем по 4 уровню доверия. В качестве доверенных ОС могут выступать: • РУСБ.10015-01 "Операционная система специального назначения "Astra Linux Special Edition" версия 1.6 SE "Смоленск"; • RU.29926343.02.01-01 "Операционная система "РЕД ОС" Версия 7.3 "Муром".	Гостевая (безопасная) операционная система, являющаяся средой функционирования для набора программ пользователя, обеспечивающих безопасное подключение к удалённому рабочему столу (к рабочему СВТ пользователя)
Программное средство обеспечения защищённой передачи данных (VPN-клиент/ TLS-клиент)	В качестве сертифицированных VPN/TLS клиентов могут выступать: • ФРКЕ.00239-01 "Программный комплекс ViPNet Client 4U for Linux"; • МКЕЮ.00435-01 "Программный комплекс "VPN/FW "ЗАСТАВА" версия 6". Клиент".	Программное средство (программный комплекс), обеспечивающее (-ий) создание защищённого канала (туннеля) между доверенной ОС, запускаемой на личном СВТ пользователя и рабочим СВТ пользователя, входящем в ИС, в которой хранится и обрабатывается информация, не содержащая сведений, составляющих государственную тайну
Программа Aladdin SecureAdmin	RU.АЛДЕ.04.09.033-01 Программа Aladdin SecureAdmin	Программа администратора LiveOffice, развёртываемая на его АРМ (рабочем месте)
СКЗИ «Криптотокен 2 ЭП»	46538383.62.001 Средство криптографической защиты информации «Криптотокен 2 ЭП»	Сертифицированное средство криптографической защиты информации, имеющее следующие функции: • средство электронной подписи (создание ЭП, проверка ЭП, создание ключей ЭП и их проверки); • создание ключей преобразований по ГОСТ Р 34.12–2015, выполнение преобразований на основе шифра «Магма» по ГОСТ Р 34.12–2015 (а также ГОСТ 28147–89); создание ключей HMAC,

Наименование компонента	Обозначение компонента	Назначение компонента
		вычисление HMAC; генерация случайных чисел, хранение файлов и папок в памяти JaCarta-2 ГОСТ (МКСК).
ПК «Единый клиент JaCarta»	46538383.425000.011 ПК «Единый клиент JaCarta»	ПО "Единый клиент JaCarta" обеспечивает выполнение операций чтения, записи и удаления над аутентификационными данными, хранящимися в памяти электронного ключа JaCarta. Указанная аутентификационная информация, которой владеет пользователь или администратор информационной системы, используется при реализации многофакторной аутентификации в информационной системе
Программа Aladdin SecurLogon	RU.АЛДЕ.02.07.002 Программа Aladdin SecurLogon	Программное средство подключения к удалённому рабочему столу (RDP-клиент)

Изделия Aladdin LiveToken, входящие в состав средства Aladdin LiveOffice имеют корпус из прочного, износостойкого пластика и маркируются уникальным нестираемым машиночитаемым номером, отображаемым в программных интерфейсах Aladdin LiveOffice при подключении USB-накопителя к средству вычислительной техники.

Подключение ССМНИ к средствам вычислительной техники осуществляется через аппаратный интерфейс USB 2.0 (тип A).

Рисунок 1 — Изделие Aladdin LiveToken из состава Aladdin LiveOffice

Хранение информации осуществляется во флеш-памяти изделия (на microSD-карте установленного объёма: 6 или 32 ГБ). В процессе ввода в эксплуатацию, с помощью прикладных программ из состава Aladdin LiveOffice, доступное дисковое пространство разбивается на фрагменты, условно называемые "разделами". Каждый "раздел" имеет определённый объём и определяет тип доступа к блоку выделенной памяти.

Таблица 4 – Разделы в памяти носителя

Загрузочный раздел	Место хранения СПО LiveBoot. Раздел доступен в режиме "Чтение".
Системный раздел	Место хранения доверенной операционной системы, доступной в режиме "Чтение". Раздел отображается только в доверенной ОС из состава изделия, а также после прохождения аутентификации администратором в программе SecureAdmin.
Защищённый прикладной раздел	Место хранения пользовательских данных, задаваемых администратором безопасности. Раздел отображается только в доверенной ОС из состава изделия или после прохождения аутентификации администратором в программе SecureAdmin.
Защищённый пользовательский раздел	Место хранения системных профилей, настроек соединения и профилей VPN-клиента. Раздел защищен аппаратным шифрованием. Доступен только в доверенной ОС.
Служебный раздел	Место хранения журналов регистрации событий безопасности (журналов аудита изделия). Раздел не отображается.
Раздел "Info"	Место хранения инструкций для работы с изделием и другой полезной информации.

2.2.3 Режимы работы изделия

Существуют следующие основные режимы функционирования средства дистанционной безопасной работы:

1. Не инициализировано администратором.
2. Инициализировано администратором, не активировано пользователем: установлен пароль по умолчанию, не установлен идентификатор СВТ.
3. Изделие работает штатно.
4. Изделие заблокировано вследствие нарушения правил эксплуатации или неверного ввода аутентификационной информации.
5. Изделие подготовлено для обновления – режим "обновление".

2.3 Ограничения, связанные с использованием изделия

2.3.1 Организационные меры, связанные с использованием изделия

Этап подготовки к вводу в эксплуатацию является обязательным.

На этапе определяются:

- перечень АРМ, к которым будет разрешено подключение с помощью Aladdin LiveOffice;
- определение перечня носителей администратора (Aladdin LiveAdmin), предназначенных для проведения операций администрирования над носителями пользователей;
- правила изменения даты и времени на средствах вычислительной техники, на которых будет разрешено использование USB-носителей Aladdin LiveToken из состава Aladdin LiveOffice, а также правила изменения даты/времени на АРМ, к которым будет разрешено подключение с помощью Aladdin LiveOffice;
- правила физического доступа к СВТ, на которых будет устанавливаться ПО из состава Aladdin LiveOffice, гарантирующие:
  - целостность средств вычислительной техники (в соответствии с составленным перечнем), на которых будет использоваться Aladdin LiveOffice;
  - отсутствие возможности доступа к данным и резервным хранилищам данных администраторов Aladdin LiveOffice третьим лицам (в том числе пользователям, не относящимся к уполномоченным пользователям (администраторам) изделия);
  - уничтожение (стирание) или архивация данных, относящихся к Aladdin LiveOffice с АРМ администратора при: ремонте, замене комплектующих, списании АРМ.

Для предотвращения кражи или подмены данных, генерируемых в процессе работы программ, осуществляется их привязка к рабочим местам. Изменение конфигурации рабочего места (добавление или изменение структуры АРМ: замена или добавление жёсткого диска, оперативной памяти, материнской платы) – приводит к невозможности продолжения эксплуатации этого набора данных.

- перечень лиц, имеющих роли администраторов изделия и перечень АРМ, доступных конкретным лицам;
- правила хранения и выдачи пользователям машинных носителей;
- правила использования изделия пользователями (сотрудниками);
- организационные меры, регламентирующие документирование процесса вывода изделия Aladdin LiveOffice или его отдельных частей из эксплуатации;
- другие (прочие) организационные меры, относящиеся к "мерам по защите машинных носителей информации" (Приложение А).

2.3.2 Эксплуатационные ограничения

1. Aladdin LiveToken из состава Aladdin LiveOffice используется совместно со средствами вычислительной техники. Средства вычислительной техники должны быть исправны и заземлены, персонал, допущенный к работе со средствами вычислительной техники, должен пройти соответствующий занимаемой должности инструктаж и обладать необходимой группой электробезопасности.
2. К работе с Aladdin LiveOffice должен допускаться персонал, изучивший эксплуатационные документы, соответствующие выполняемым ролям: пользователь или администратор.
3. Ввод Aladdin LiveOffice в эксплуатацию должен проводиться в соответствии с настоящим руководством администратора.
4. Эксплуатация USB-накопителя должна проводиться при нормальных климатических условиях, представленных в таблице 5.

Таблица 5 – Нормальные климатические условия эксплуатации

Наименование характеристики	**Величина измерения**	**Значение характеристики**
Температура	°C	От плюс 15 до плюс 25 включительно
Относительная влажность воздуха	%	От 45 до 75 включительно
Атмосферное давление	мм рт. ст.	От 630 до 800
	кПа	От 84 до 107

5. Не допускается использование Aladdin LiveToken в случае повреждения USB-разъёма или повреждения его контактной группы, наличия в разъёме следов влаги, грибков, солей, мусора или других загрязнений.
6. Не допускается подключение электронного накопителя к заведомо повреждённым USB-интерфейсам средств вычислительной техники, либо подключение через USB-удлинители, не гарантирующие выполнение требований по питанию, выдвигаемых к стандартному исправному USB-интерфейсу в соответствии со спецификацией, и приведённых в таблице 6.

Таблица 6 – Требования к питанию электронного накопителя

Наименование характеристики	**Величина измерения**	**Значение характеристики**
Потребляемый ток	мА	300
Рабочее напряжение	В	от 4,75 до 5,25

7. Aladdin LiveToken не следует подвергать воздействию статического электричества. Работоспособность изделия не гарантируется после воздействия статического разряда напряжением более 5000 вольт.
8. Не допускается хранение и эксплуатация флеш-накопителя вблизи источников радиации и/или сильных электромагнитных излучений.
9. Aladdin LiveToken не должен подвергаться воздействию случайных вибраций со степенью жёсткости превышающей 4с [ГОСТ 30361].
10. Не допускается: совершение действий, приводящих к нарушению целостности корпуса флеш-накопителя, а также эксплуатация накопителей с повреждённым корпусом.
11. Aladdin LiveToken не следует подвергать ударам, аналогичным или превышающим по силе удары при свободном падении с высоты более 1 м.
12. Для корректной работы приложений из состава Aladdin LiveOffice должна обеспечиваться надёжность и единообразность системного времени – изменение меток времени должно осуществляться по строго регламентированным правилам и только уполномоченными пользователями.
13. Запрещается извлекать Aladdin LiveToken из USB-порта средства вычислительной техники и/или прерывать подачу питания на него при мигающем световом индикаторе. Невыполнение данного правила может привести к потере или порче записываемых во флеш-память Aladdin LiveOffice данных или нарушению его работоспособности. Информация обо всех некорректно прерванных операциях фиксируется в журнале флеш-накопителя и может служить основанием для выявления и подтверждения фактов нарушения правил эксплуатации, что автоматически приводит к отказу изготовителя от гарантийных обязательств.
14. Извлечение Aladdin LiveToken должно выполняться только после успешного завершения работы компьютера (CBT).

15. При проведении обновления встроенного программного средства Aladdin LiveToken запрещается извлекать устройство из USB-порта средства вычислительной техники и/или прерывать подачу питания на него до завершения обновления.
16. Вывод из эксплуатации Aladdin LiveToken из состава Aladdin LiveOffice производится только администратором изделия.
17. Пользователь изделия обязан оповестить администратора об утере, краже, поломке, подозрении или выявленной попытке несанкционированного использования защищенного носителя, следов попытки вскрытия корпуса. Администратор в свою очередь обязан провести блокировку защищенного носителя путем ограничения его доступа к информационной (автоматизированной) системе организации.

2.3.3 Основные принципы безопасной работы с изделием

При работе пользователей с изделием предполагаются следующие основные принципы:

1. После получения изделия Aladdin LiveToken от администратора пользователь не передаёт его третьим лицам.
2. Пользователь не использует простые или общедоступные пароли.
3. Пользователь не хранит аутентификационную информацию на бумажных или электронных носителях.
4. Пользователь ограничивает доступ к личному средству вычислительной техники для посторонних людей.
5. Пользователь тщательно осматривает накопитель на предмет наличия повреждений или вскрытия перед каждым использованием.
6. Пользователь не использует подключение к беспроводной сети не защищённое паролем.
7. При наличии проблем пользователь обращается к администратору изделия.
8. Пользователь не подключает USB-носитель через USB-хабы (удлинители) или дополнительные устройства.
9. Пользователь изделия обязан оповестить администратора об утере, краже, поломке, подозрении или выявленной попытке несанкционированного использования защищенного носителя, следов попытки вскрытия корпуса. Администратор в свою очередь обязан провести блокировку защищенного носителя путем ограничения его доступа к информационной (автоматизированной) системе организации.

3. Требования к среде функционирования составных частей Aladdin LiveOffice

3.1 Требования к СВТ пользователей

3.1.1 Аппаратные требования

Минимальные требования к аппаратному обеспечению, необходимому для функционирования Aladdin LiveToken из состава Aladdin LiveOffice.

Таблица 7 – Аппаратные требования

Видеоадаптер и монитор	VGA 1024x768 (минимально поддерживаемое разрешение 1024 на 768 пикселов)
Свободная оперативная память	от 4 ГБ
Устройства взаимодействия с пользователем	Монитор, клавиатура и мышь
USB-интерфейс	USB 2.0 тип A или совместимые
Сетевые интерфейсы	Интерфейс проводной локальной вычислительной сети (технология Ethernet[3]) и/или интерфейс беспроводной локальной вычислительной сети (технология Wi-Fi[4]) и/или интерфейс беспроводной высокоскоростной передачи данных сети подвижной радиотелефонной связи 3 или 4 поколения (3G/4G)
Процессоры	x64-совместимые процессор; x64, кроме: архитектур IA-64; процессоров AMD до Athlon 64; процессоров Intel до Pentium; архитектур VIA C3; архитектур Transmeta Crusoe.

3.2 Требования к удалённым рабочим местам

3.2.1 Перечень системного программного обеспечения

Поддерживается работа со следующими операционными системами:

Таблица 8 – Перечень операционных систем

Операционные системы семейства Windows (x32 и x64)	Microsoft Windows 8.1; Microsoft Windows 10.
Операционные системы семейства Linux (x64)	Astra Linux SE 1.5 SE (релиз «Смоленск»); Astra Linux SE 1.6 SE (релиз «Смоленск»); Альт 8 СП Рабочая станция;

[3] Технология Ethernet определяется семейством стандартов IEEE 802.3.

[4] Технология Wi-Fi определяется семейством стандартов IEEE 802.11.

	Альт 8 СП Сервер; ОС «ЕМИАС» 1.0; РЕД ОС 7.3 (релиз «Муром»).

3.3 Требования к АРМ администратора

3.3.1 Перечень системного программного обеспечения

Таблица 9 – Перечень системного ПО

Операционные системы семейства Linux (x64)	ОС Astra Linux Special Edition 1.6 (Смоленск) x64; РЕД ОС 7.3 (релиз "Муром").
Операционные системы семейства Windows (x32 и x64)	Microsoft Windows 8.1; Microsoft Windows 10.

3.3.2 Минимальные аппаратные требования

Минимальные аппаратные требования, необходимые для функционирования программ из состава Aladdin LiveOffice.

Таблица 10 – Аппаратные требования

Требуемое дисковое пространство	от 1 ГБ
Видеоадаптер и монитор	VGA 1024x768 (поддерживаемое разрешение 1024 на 768 пикселов)
Свободная оперативная память	от 128 МБ
Устройства взаимодействия с пользователем	Клавиатура и мышь
USB-интерфейс	USB 2.0 тип A или совместимые
Сетевые интерфейсы	Интерфейс проводной локальной вычислительной сети (технология Ethernet и/или интерфейс беспроводной локальной вычислительной сети (технология Wi-Fi) и/или интерфейс беспроводной высокоскоростной передачи данных сети подвижной радиотелефонной связи 3 или 4 поколения (3G/4G)
Процессоры	Процессоры с архитектурой x64, кроме: архитектур IA-32, IA-64; процессоров AMD до Athlon 64; процессоров Intel до Pentium; архитектур VIA C3; архитектур Transmeta Crusoe.

3.3.3 Требования к дополнительному ПО.

Для функционирования Aladdin LiveOffice в различных операционных системах необходимы установленные библиотеки/пакеты: PCSCD.

Указанные библиотеки входят в состав операционных систем семейства Windows.

Для операционных систем семейства Linux указанные пакеты входят в состав официальных репозиториев и могут быть либо установлены по умолчанию, либо в результате совершения дополнительных действий. Подробная инструкция по установке требуемых пакетов для конкретных операционных систем приведена в «Приложение B», [с. 65].

Дополнительные требования к составным частям изделия могут быть отражены в эксплуатационной информации на данные составные части.

Для формирования dst фалов используется программное обеспечение ViPNet Coordinator, а запись сертификатов пользователей на носители Aladdin LiveOffice осуществляется с помощью программного обеспечения КриптоПро CSP.

4. Порядок работы с изделием

В настоящем разделе представлен общий порядок работы с изделием "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice". В каждом подразделе приведены действия, которые необходимо совершить на указанном этапе работ. Подробное описание действий, используемых программных интерфейсов и операций, производимых в этих интерфейсах – приводится в соответствующих подразделах данного руководства.

4.1 Подготовка к вводу в эксплуатацию

4.1.1 Перечень работ, проводимых на этапе ввода в эксплуатацию проводимых администратором безопасности

На этапе подготовки к вводу в эксплуатацию осуществляется:

- приёмка изделия и проведение подготовительных процедур;
- определение состава административного персонала и подготовка перечня средств вычислительной техники, с которыми будет использоваться Aladdin LiveOffice;
- разработка организационно-распорядительной и организационно-технической документации, соответствующей разделу 2.3.1;
- установка Aladdin SecureAdmin из состава изделия на АРМ администратора;
- регистрация администратора;
- создание базы данных;
- создание ключевой информации;
- регистрация администратора с привязкой носителя администратора Aladdin LiveAdmin к конкретному должностному лицу.

4.1.2 Приемка носителей LiveToken

- получение носителей администратором;
- заполнение эксплуатационной документации (в том числе ознакомление с ней);
- вывод носителей из транспортного режима.

4.1.3 Подготовка перечня средств вычислительной техники

До начала работ с изделием, необходимо определить и настроить СВТ, к которым будет осуществляться подключение с помощью средства обеспечения безопасного дистанционной работы.

К перечню работ, осуществляемых при подготовке рабочих мест, относятся:

- определение перечня физических рабочих мест;
- проверка возможности установки удалённого подключения к рабочему месту пользователя путём проверки качества сети;
- составление перечня IP-адресов и определение возможности подключения к рабочим местам по протоколу RDP;
- создание правил фильтрации информационных потоков в ИС и др.

4.1.4 Поддержка ввода средств вычислительной техники пользователей к вводу в эксплуатацию Aladdin LiveOffice

При подготовке рабочих мест пользователей администратором выполняются следующие обязанности:

- сбор информации о домашних рабочих местах пользователей;
- осуществление поддержки в подготовке домашних рабочих мест пользователей к вводу в эксплуатацию Aladdin LiveOffice.

4.1.5 Подготовка рабочих мест администраторов к работе

Подготовка рабочего места администратора безопасности осуществляется с помощью установки на АРМ администратора программы Aladdin SecureAdmin из состава изделия, дополнительного ПО (при необходимости) и инициализации «*носителя администратора*» Aladdin LiveAdmin, предназначенного для администрирования *носителей пользователей*.

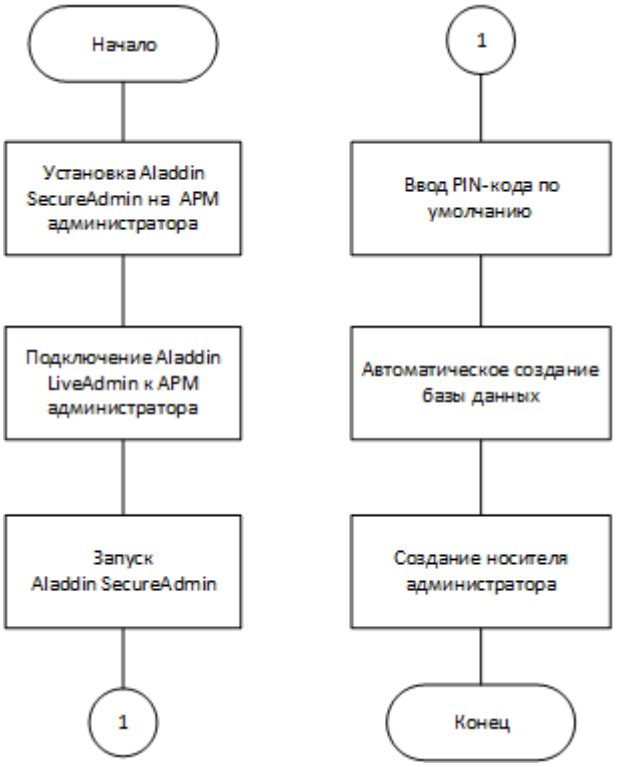

Рисунок 2 — Подготовка АРМ администратора

Общий алгоритм работы с программой Aladdin SecureAdmin после прохождения процедуры авторизации администратора представлен на рисунке ниже.

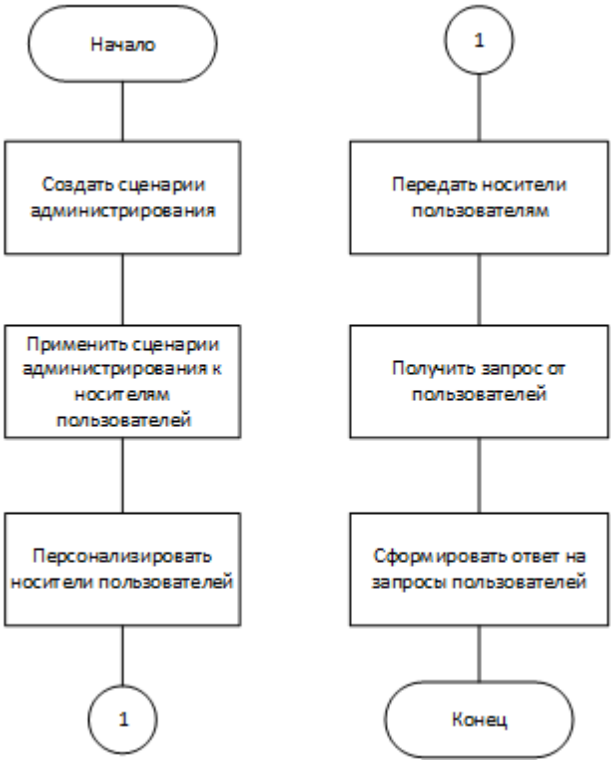

Рисунок 3 — Эксплуатация программы Aladdin SecureAdmin

4.1.5.1 Установка программ из состава изделия

В процессе подготовки автоматизированного рабочего места администратора устанавливаются следующие программы:

Таблица 11 – Автоматизированное рабочее место администратора

	Назначение	**Обязательность**
ПО SecureAdmin	Инициализация и управление носителями пользователей.	Да
ПК "Единый клиент" (приобретается отдельно)	Удобное управление носителями пользователей. Привязка сертификатов пользователей как автономным устройствам. Управление 2ФА.	Нет

Установка программ из состава изделия описана в разделе "Установка и удаление программ" [с. 65].

4.1.5.2 Создание баз данных

В процессе работы с Aladdin LiveOffice, администратором ведутся уникальные базы данных, хранящие информацию о:

- инициализированных носителях пользователей;
- версии микропрограммного обеспечения;
- о созданных сценариях администрирования;
- созданных шаблонах;
- настройках парольной политики;
- настройках аутентификации СВТ;
- настройках журналирования.

Создание базы данных в программе Aladdin SecureAdmin осуществляется автоматически при первом запуске программы, сразу после регистрации пользователя с ролью "администратор безопасности".

Место хранения файла базы данных db.alodb – директория (каталог) установки программы.

Диаграмма деятельности, визуализирующая работу программы на данном этапе, представлена на рисунке 4.

Рисунок 4 — Создание базы данных при первом запуске программы Aladdin SecureAdmin

Наличие старой базы данных на АРМ администратора не является ошибкой и не приводит к генерации дополнительного оповещения и событии безопасности. Новые события будут фиксироваться в уже существующей базе данных.

4.1.5.3 Создание мастер-ключа

При работе изделия Aladdin LiveOffice осуществляется генерация уникальных наборов данных, используемых при создании контуров безопасности.

Администратором генерируется первичный набор данных – *мастер-ключ*. Созданный *мастер-ключ* автоматически записывается на USB-носитель администратора (Aladdin LiveAdmin).

Создание ключей происходит с помощью программы Aladdin SecureAdmin.

Диаграмма деятельности, визуализирующая порядок действий на данном этапе, представлена на рисунке 5.

Рисунок 5 — Создание мастер-ключа в программе Aladdin SecureAdmin

4.1.5.4 Резервирование базы данных

Резервирование базы данных регистрации происходит путем экспорта базы с последующим сохранением резервной копии.

Создание резервной копии базы данных db.alodb осуществляется базовыми средствами ОС из директории установки программы.

4.1.6 Инициализация носителя администратора

В процессе подготовки рабочего места администратора, необходимо провести инициализацию носителя администратора.

Инициализация носителя администратора (Aladdin LiveAdmin) осуществляется путем смены базового PIN-кода и генерации мастер-ключа в программе Aladdin SecureAdmin.

Диаграмма деятельности, визуализирующая порядок действий на данном этапе, представлена на рисунке 6.

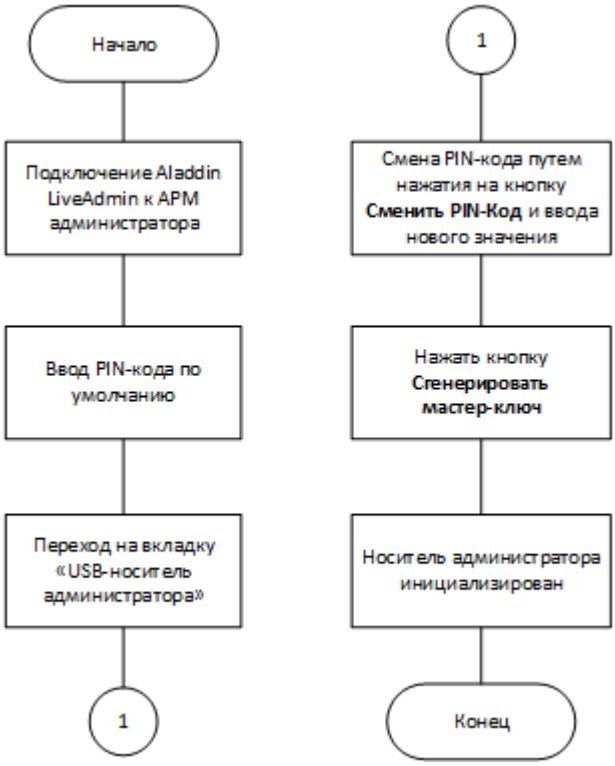

Рисунок 6 — Инициализация носителя администратора в Aladdin SecureAdmin

4.2 Эксплуатация изделия

Администрирование пользовательских носителей осуществляется с помощью сценариев администрирования, созданных в программе Aladdin SecureAdmin. Сценарии администрирования представляют собой xml-файлы с инструкциями в специальном формате.

Перечень работ, проводимых на этапе эксплуатации:

- инициализация носителей пользователей;
- управление носителями пользователей;
- администрирование запросов пользователей;
- обновление носителей;
- вывод из эксплуатации носителей и баз данных.

4.2.1 Инициализация носителей пользователей

Инициализация Aladdin LiveToken пользователей осуществляется путем применения сценариев "Инициализация USB-носителя", "Запись LiveOS" и "Запись загрузчика" в программе Aladdin SecureAdmin. При этом на Aladdin LiveToken пользователя записывается LiveOS и СПО LiveBoot, создается профиль пользователя.

Диаграмма деятельности, визуализирующая порядок действий на данном этапе, представлена на рисунке 7.

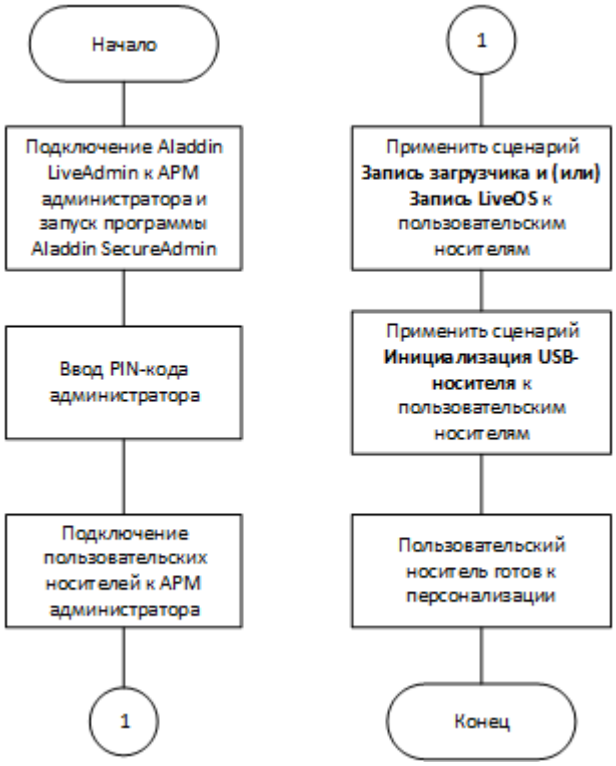

Рисунок 7 — Инициализация пользовательских носителей в Aladdin SecureAdmin

4.2.2 Администрирование запросов пользователей

В процессе работы пользователю могут потребоваться функции по регистрации и удалению СВТ, а также разблокировка носителя в случае его блокировки. Перед работой с изделием необходимо зарегистрировать место, с которого будет осуществляться подключение к корпоративной (частной) сети – получить разрешение на доступ в ИС с него. Пользователю предоставляется возможность удаления уже зарегистрированный СВТ с носителя и разблокировке носителя с помощью системы запрос-ответ при взаимодействии с администратором Aladdin LiveOffice. Регистрация и удаление рабочего места, а также разблокировка носителя осуществляются следующим образом:

1. Пользователь формирует запрос в загрузчике изделия (в зависимости от задачи) и передает его администратору по сторонним каналам связи.
2. Администратор в процессе работы, по отдельным каналам связи принимает запросы пользователей на регистрацию/удаление СВТ или разблокировку носителей и осуществляет генерацию ответов на запросы с помощью программы Aladdin SecureAdmin.
3. Администратор по отдельным каналам связи передаёт пользователю, генерируемый в программе Aladdin SecureAdmin ответ.
4. Пользователь вводит в предложенное поле ответ, переданный администратором.

> *Обмен запросами и ответами осуществляется по отдельным каналам связи, не относящимся к изделию Aladdin LiveOffice.*

Диаграмма деятельности, визуализирующая порядок действий на данном этапе, представлена на рисунке 8.

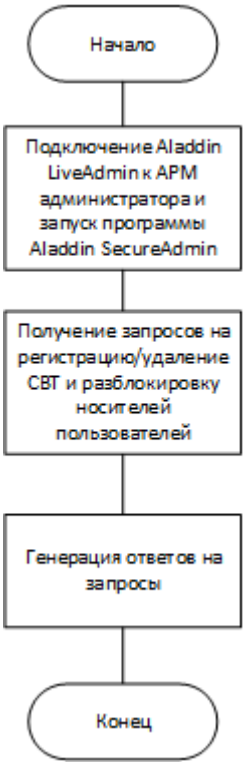

Рисунок 8 — Администрирование запросов в программе Aladdin SecureAdmin

4.2.3 Создание и редактирование сценариев для администрирования Aladdin LiveToken

Создание и редактирование сценариев администрирования Aladdin LiveToken осуществляется с помощью программы Aladdin SecureAdmin на вкладке **Сценарии**.

Диаграмма деятельности, визуализирующая порядок действий на данном этапе, представлена на рисунках 9 и 10.

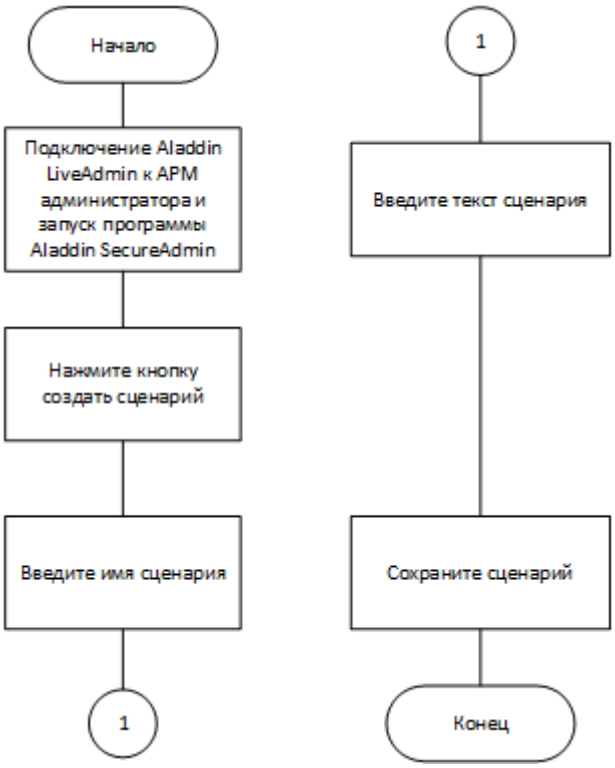

Рисунок 9 — Создание сценариев в программе Aladdin SecureAdmin

Рисунок 10 — Редактирование сценариев в программе Aladdin SecureAdmin

4.2.4 Применение сценариев для администрирования Aladdin LiveToken пользователей

Применение созданных сценариев администрирования Aladdin LiveToken осуществляется с помощью SecureAdmin на вкладке **Подключенные USB-носители**.

Диаграмма деятельности, визуализирующая порядок действий на данном этапе, представлена на рисунке 11.

Рисунок 11 — Применение сценариев в программе Aladdin SecureAdmin

4.2.5 Вывод из эксплуатации носителей и баз данных

Вывод из эксплуатации Aladdin LiveToken осуществляется путем применения сценария "Сброс к заводским настройкам" в программе Aladdin SecureAdmin.

Порядок работ, осуществляемых при выводе изделия из эксплуатации приведён в приложении Д – Порядок вывода изделия из эксплуатации.

5. Инструкции по работе с изделием "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice"

5.1 Настройка рабочего места для работы с изделием

При первом подключении изделий "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice" в ОС Windows происходит некорректное отображение устройства в диспетчере устройств (см. Рисунок 12). Связано это с некорректным выбором драйвера для подключенного изделия, которое применяет нестандартные команды SCSI при взаимодействии с ОС и программой Aladdin SecureAdmin.

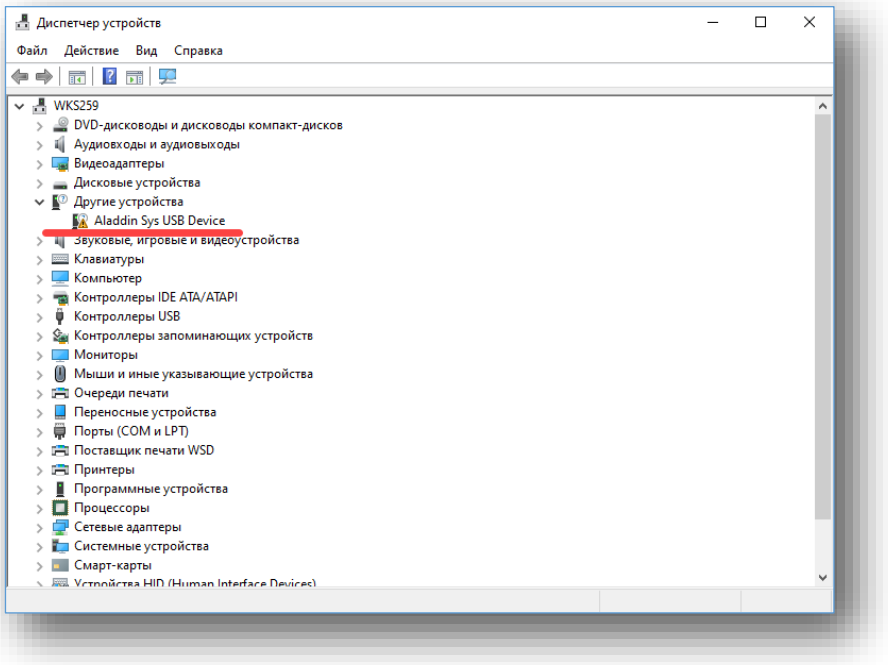

Рисунок 12 — Окно диспетчера устройств

Для корректного выполнения операций с носителем необходимо выполнить следующие действия:

1. В диспетчере устройств нажмите на Aladdin Sys USB Device правой кнопкой мыши и выберите действие "Обновить драйвер".

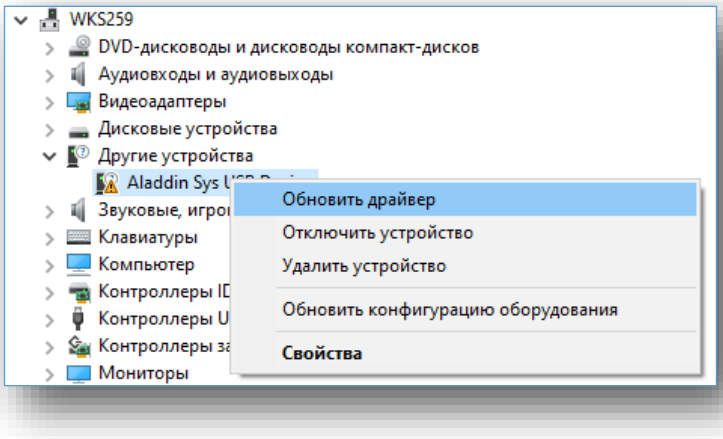

Рисунок 13 — Выбор действия "Обновить драйвер"

2. В появившемся окне выберите действие "Выполнить поиск драйверов на этом компьютере".

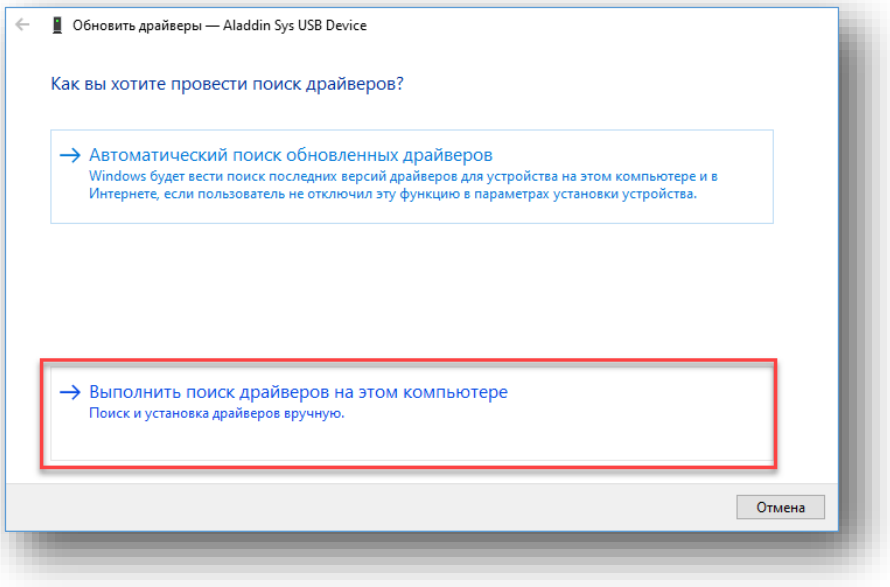

Рисунок 14 — Локальный поиск драйверов

3. Нажмите на поле "Выбрать драйвер из списка доступных драйверов на компьютере".

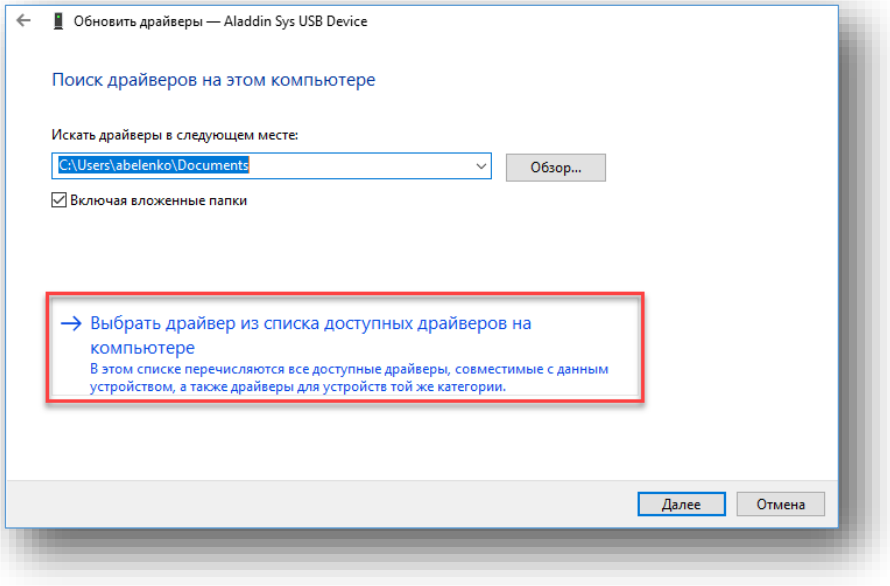

Рисунок 15 — Выбор драйвера из списка доступных

4. Выберите стандартный драйвер для съемных носителей (укажите тип устройства).

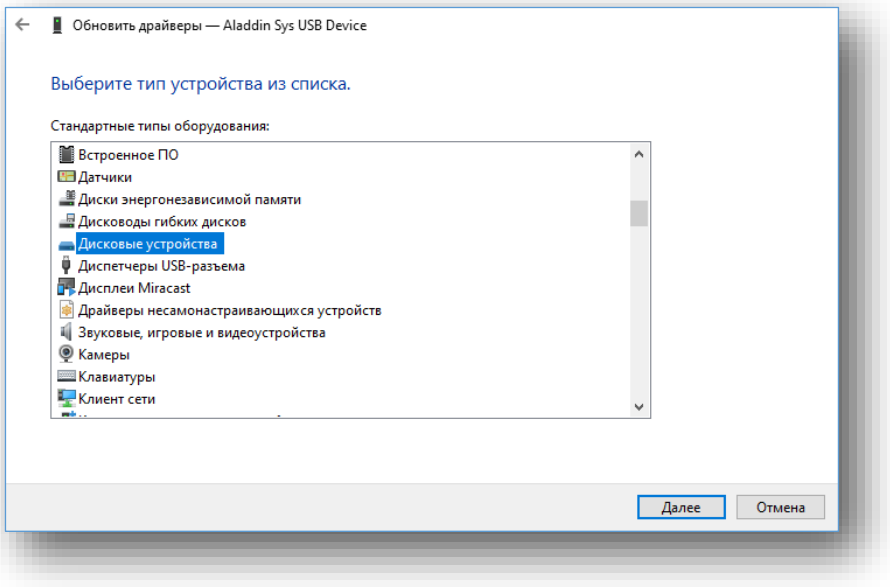

Рисунок 16 — Выбор типа устройства

5. В качестве модели устройства выберите "Дисковый накопитель" и нажмите кнопку <**Далее**>.

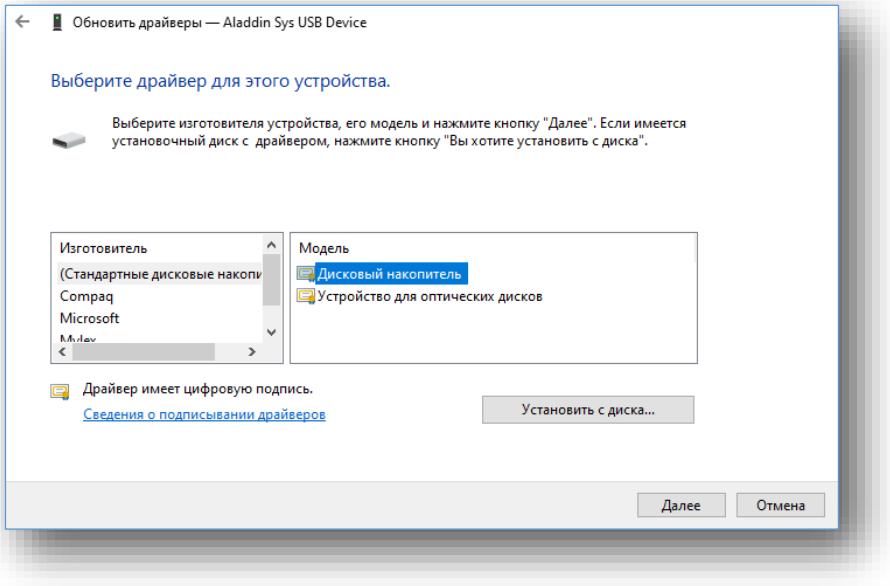

Рисунок 17 — Выбор драйвера модели устройства

6. После выбора модели устройства появится окно с предупреждением при обновлении драйвера. Нажмите на кнопку <**Да**>.

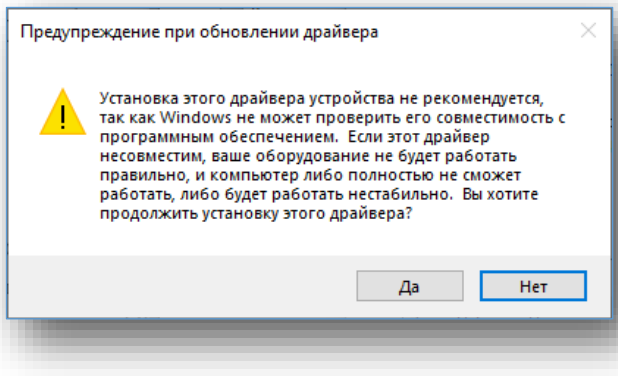

Рисунок 18 — Предупреждение при обновлении драйвера

7. После подтверждения действия произойдет применение выбранного драйвера для подключенного носителя Aladdin LiveOffice.

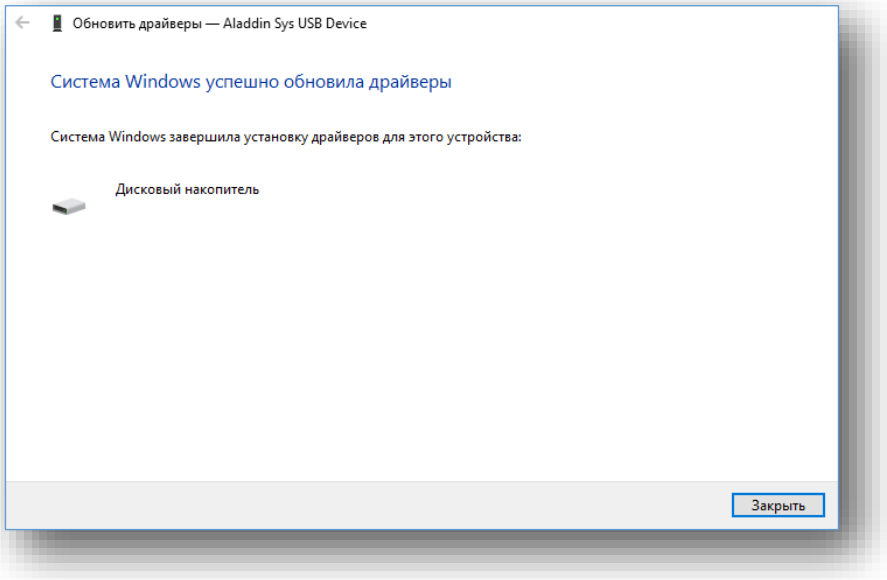

Рисунок 19 — Успешное обновление драйвера

В результате проделанных действий подключенное изделие отобразится в виде стандартного съемного носителя (см. Рисунок 20). Устройство готово к использованию.

> ***Рекомендуется использовать*** *Aladdin SecureAdmin в ОС семейства Linux, так как в них происходит автоматический выбор необходимых драйверов в соответствии с VID/PID подключаемых устройств.*

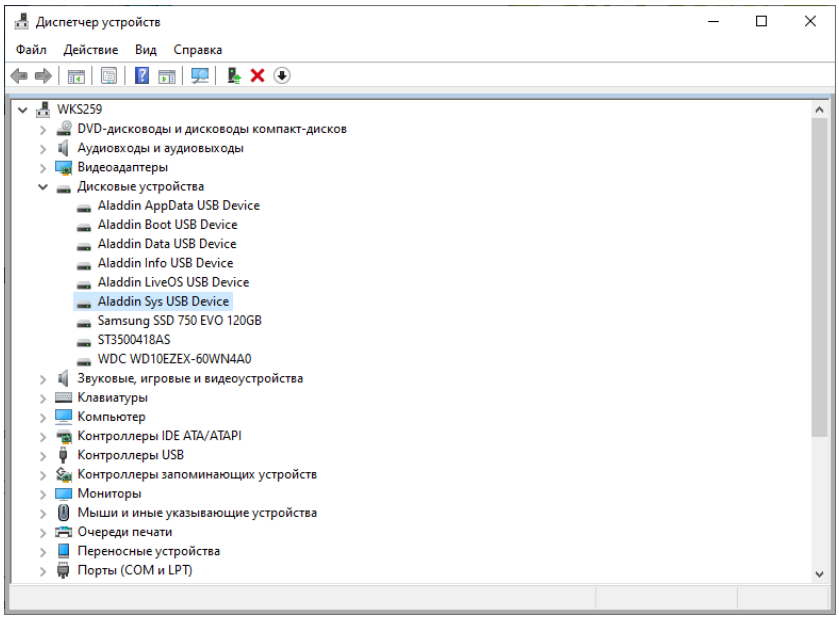

Рисунок 20 — Обновленное отображение подключенного носителя

5.2 Aladdin SecureAdmin

5.2.1 Общая информация о Aladdin SecureAdmin

Программа Aladdin SecureAdmin предназначена для администрирования USB-носителей Aladdin LiveToken из состава средства обеспечения безопасной дистанционной работы Aladdin LiveOffice.

Доступ к программе должен предоставляться только пользователям с ролью "администратор безопасности".

До запуска программы к АРМ администратора необходимо подключить носитель администратора Aladdin LiveAdmin, который будет использоваться для администрирования носителей пользователей. Доступ к программе осуществляется только после предъявления носителя Aladdin LiveAdmin.

Запуск программы в ОС семейства Linux осуществляется от имени пользователя с правом выполнения команды `sudo` через командную строку (необходим пароль суперпользователя):

```
cd /opt/Aladdin/SecureAdmin/

sudo ./secureadmin
```

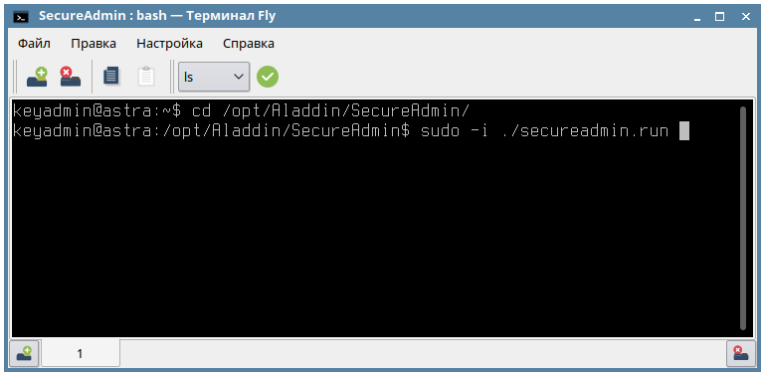

Рисунок 21 — Запуск программ из командной строки

Запуск программы в ОС семейства Windows осуществляется путем запуска .exe файла установленной программы или нажатием на ярлык приложения.

После запуска приложения появится окно с требованием подключить USB-носитель администратора (см. Рисунок 22). В качестве носителя администратора выступает Aladdin LiveAdmin.

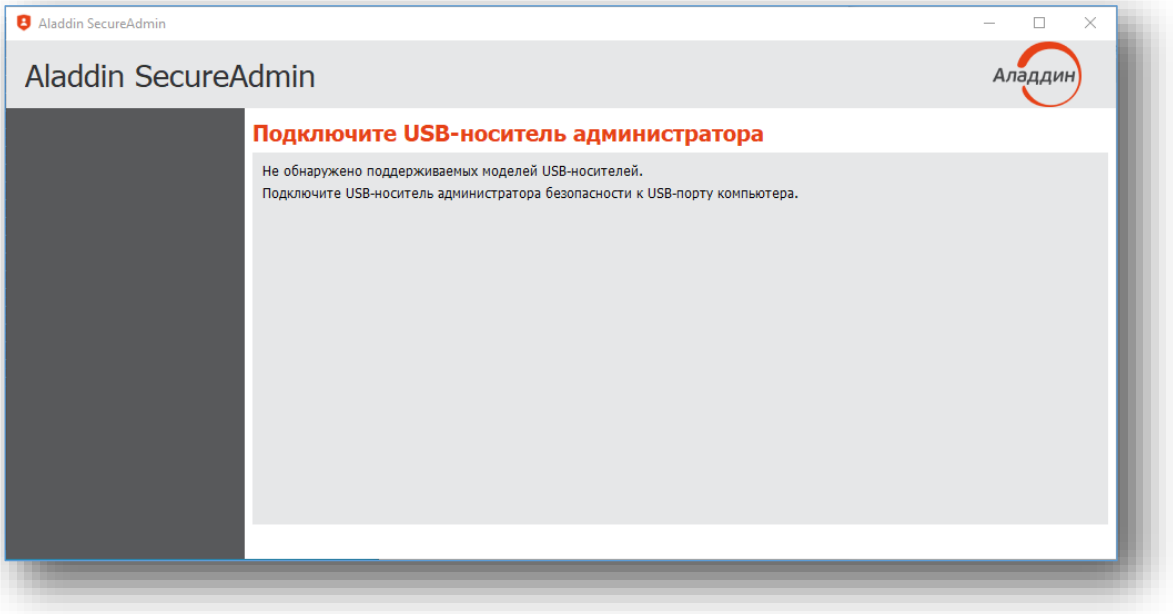

Рисунок 22 — Окно запуска программы

При подключении Aladdin LiveAdmin появится окно аутентификации администратора (см. Рисунок 23).

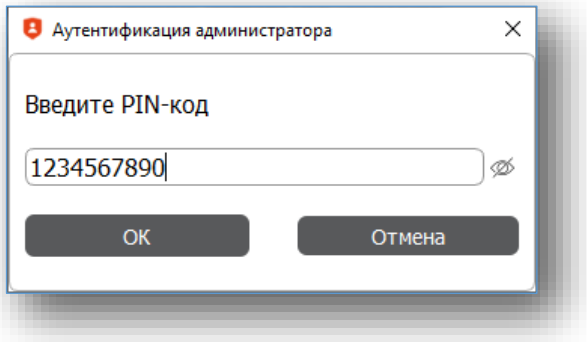

Рисунок 23 — Окно аутентификации администратора

> *Для прохождения аутентификации администратору необходимо ввести PIN-код, заданный по умолчанию (1234567890). Далее при использовании Aladdin LiveAdmin рекомендуется заменить PIN-код администратора для исключения ситуаций несанкционированного использования USB-носителя сторонними лицами.*

После установки и запуска программы Aladdin SecureAdmin в операционной системе Linux в директории `/opt/Aladdin/SecureAdmin/` будет находиться файл базы данных `db.alodb`, интерфейсная криптобиблиотека `libjckt2.so` и каталог `images`. Образы LiveOS и LiveBoot для выполнения сценариев "Инициализация USB-носителя", "Запись LiveOS", "Запись загрузчика" – необходимо хранить в директории `/opt/Aladdin/SecureAdmin/images/`.

После установки и запуска программы Aladdin SecureAdmin в операционной системе Windows в директории установки программы будет находиться файл базы данных `db.alodb`, интерфейсная криптобиблиотека `jckt2.dll` и каталог `images`. Образы LiveOS и LiveBoot для выполнения сценариев "Инициализация USB-носителя", "Запись LiveOS", "Запись загрузчика" – необходимо хранить в папке `images`.

Интерфейс главного окна программы представлен на рисунке 24.

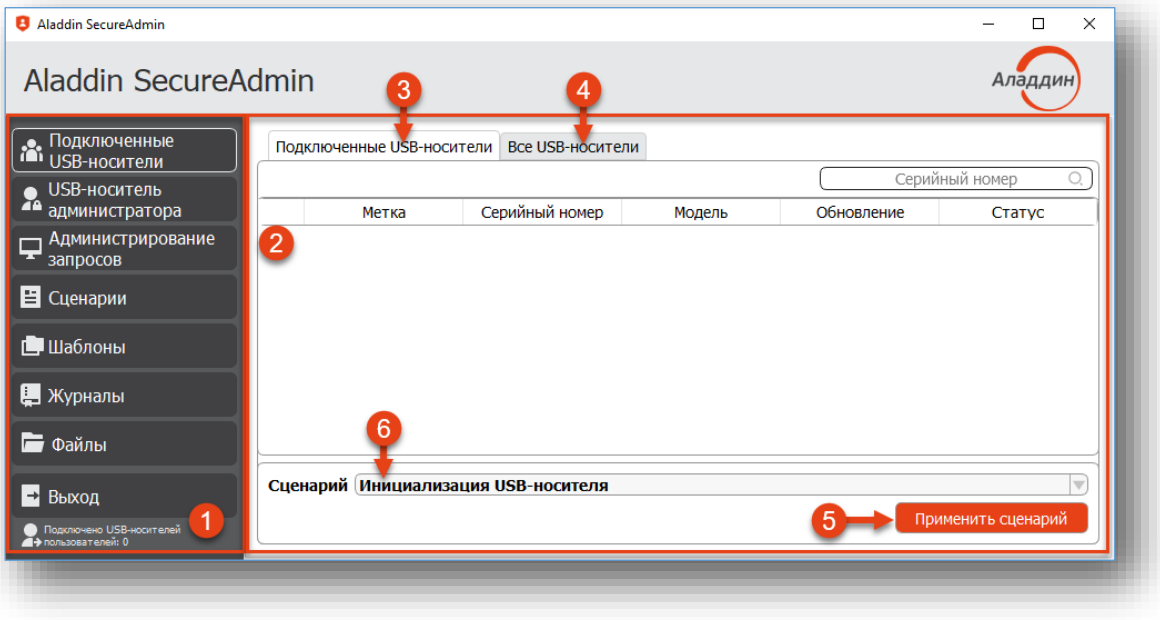

Рисунок 24 — Программа Aladdin SecureAdmin. Интерфейс основного окна программы

5.2.1.1 Вкладка Подключенные USB-носители

Интерфейс программы разделён на несколько зон.

В левой части окна находится *постоянная область* (1): группа вкладок (**Вкладки**), на которых отображаются элементы интерфейса, необходимые для управления программой, кнопка <**Выход**> и информация о количестве подключённых к СВТ администратора безопасности изделий Aladdin LiveToken.

В правой части окна находится *рабочая область* (2) – часть экранной формы, зависящая от выбора конкретной *вкладки* в постоянной области.

> *Обратите внимание: при запуске программа открывается на вкладке "Подключенные USB-носители".*

В рабочей области содержатся постоянные блоки, характерные для конкретной вкладки программы:

- Вкладки **Подключенные USB-носители** (3) и **Все USB-носители** (4), кнопка <**Применить сценарий**> (5), а также *область выбора сценария* (6).
- Вкладка **Подключенные USB-носители** (3) предназначена для работы с USB-носителями, подключенными в данный момент. На вкладке отображаются только *носители пользователей*.

На вкладке, *в рабочей области* (2) отображается следующая информация:

- метка USB-носителя, устанавливаемая администратором;
- серийный номер USB-носителя, записанный на производстве;
- модель;
- версия встроенного МПО (графа **Обновление**);
- статус носителя.

Вкладка **Все USB-носители** (4), предназначена для работы с ранее инициализированными USB-носителями, т.е. носителями, к которым был применён сценарий "Инициализация USB-носителя" и содержит параметры, идентичные параметрам на вкладке (3).

Кнопка <**Применить сценарий**> (5), а также область выбора сценария (6) служат для выбора сценария и применения его к конкретному носителю.

Применение сценариев к Aladdin LiveToken состоит из двух этапов:

1. Выбор Aladdin LiveToken.
2. Применение сценария.

Выбор Aladdin LiveToken осуществляется установкой флага в чекбоксе.

Применение сценария осуществляется в следующем порядке:

1. Нажатие на поле *Сценарий: имя_сценария* приводит к открытию выпадающего списка с помощью которого обеспечивается выбор конкретного сценария.
2. Нажатие на кнопку <**Применить сценарий**> запускается выполнение сценария.

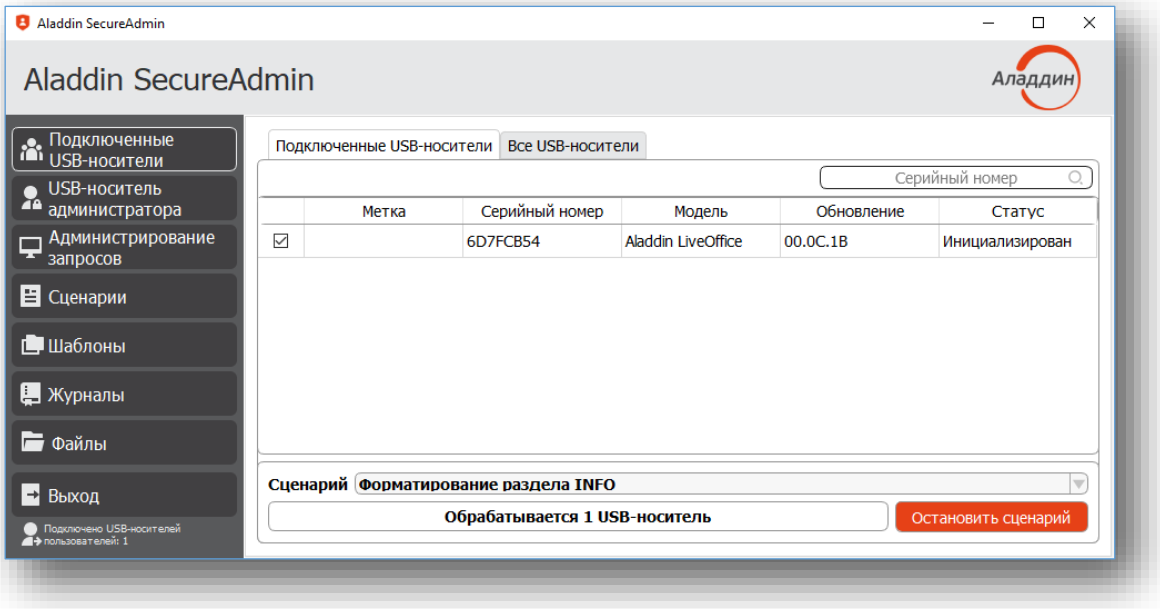

Рисунок 25 — Интерфейс программы Aladdin SecureAdmin. Применение сценария

Нажатием на кнопку <**Остановить сценарий**> осуществляется прерывание применяемого сценария.

Для установки метки носителя пользователя необходимо дважды нажать на столбец **Метка** таблицы подключенных носителей (см. Рисунок 26) и ввести новое значение метки (максимум 20 символов).

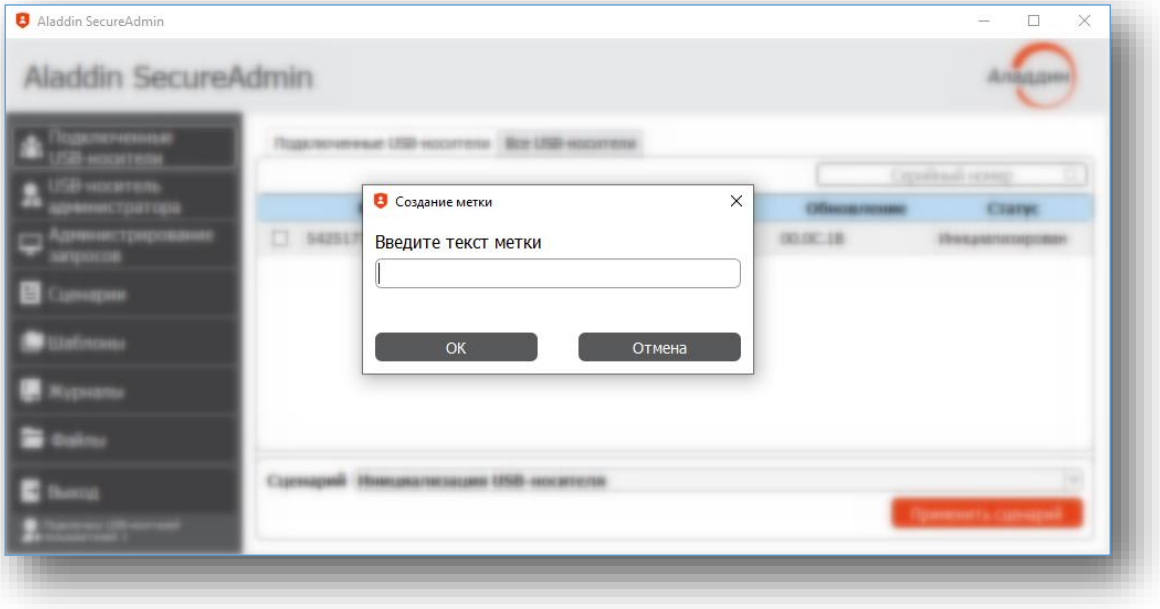

Рисунок 26 — Окно создания метки носителя

5.2.1.2 Вкладка USB-носитель администратора

Вкладка **USB-носитель администратора** позволяет управлять *носителем администратора* (Aladdin LiveToken администратора безопасности). Администратору предоставляются следующие возможности:

1. Генерация мастер-ключей.
2. Смена ПИН-кода.
3. Импорт/экспорт мастер ключа.

Экранная форма программы, отображающая содержимое вкладки **USB-носитель администратора** представлена на рисунке 27.

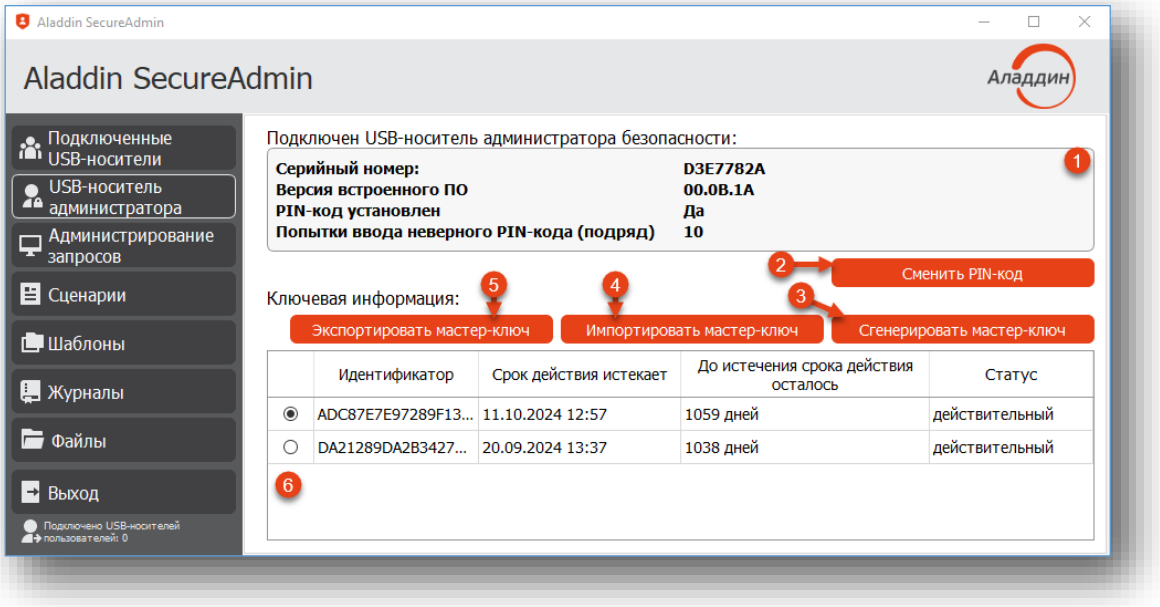

*Рисунок 27 — Интерфейс программы Aladdin SecureAdmin. Вкладка **USB-носитель администратора***

На вкладке **USB-носитель Администратора** находятся:

Блок USB-накопитель администратора безопасности (1) – содержит данные о серийном номере, версии встроенного программного обеспечения, PIN-коде USB-носителя.

Кнопка <**Сменить PIN-код**> (2) – вызывает окно смены PIN-кода.

Кнопка <**Сгенерировать мастер-ключ**> (3) – запускает выполнение алгоритма создания ключа, после которого сгенерированный ключ будет записан на носитель администратора и отобразится в интерфейсе программы Aladdin SecureAdmin в блоке **Ключевая информация** (6).

> ***Важно!*** *Нажатие кнопки <Сгенерировать ключ> для носителя администратора с уже установленным ключом – приводит к записи второго мастер ключа на носитель администратора. Последующие носители пользователей будут работать с последним (актуальным) ключом администратора.*

Кнопки <**Импортировать мастер-ключ**> (4) и <**Экспортировать мастер-ключ**> (5) предназначены для импорта/экспорта мастер-ключа. При экспорте мастер-ключа создается файл-контейнер в формате <вводимое имя контейнера>.cnt. При импорте мастер-ключа необходимо указать путь к ранее созданному контейнеру, содержащему мастер-ключ администратора.

> ***ВАЖНО!*** *Настоятельно рекомендуется провести резервирование мастер-ключа администратора, т.к. в случае его утери администрирование носителей становится невозможным.*

Блок **Ключевая информация** (6) содержит в себе данные об идентификаторе ключа, сроке действия ключа.

Удаление мастер-ключа с носителя администратора осуществляется нажатием правой кнопкой мыши на ключе и выбором пункта <Удалить> в контекстном меню.

5.2.1.3 Вкладка Администрирование запросов

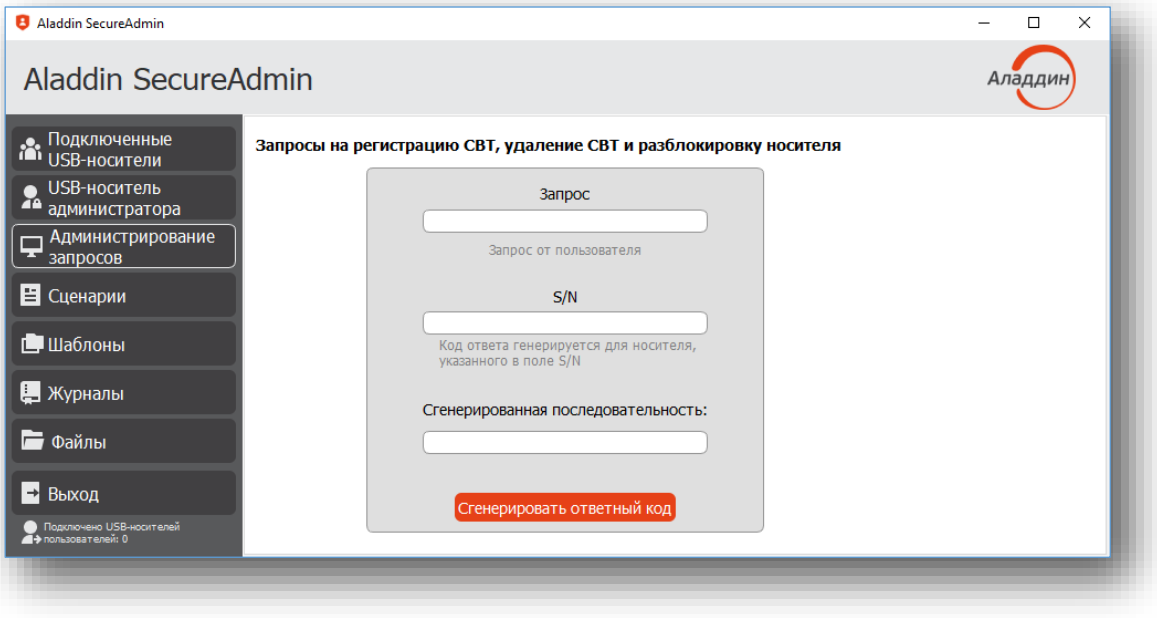

Рисунок 28 — Программа Aladdin SecureAdmin. Вкладка Администрирование запросов

Вкладка **Администрирование запросов** содержит в себе следующие элементы**:**

- **Запрос** – поле ввода запроса пользователей на запрашиваемое действие (удаление/регистрация СВТ или разблокировка носителей).
- **S/N** – поле ввода серийного номера носителя в котором сформирован запрос.
- **Сгенерированная последовательность** – поле, содержащее сгенерированную последовательность после ввода информации в поля **Запрос** и **S/N**.

Запросы формируются с помощью интерфейса загрузчика Aladdin LiveBoot по команде пользователей на совершение определенных операций (регистрация/удаление СВТ, разблокировка носителя).

Для формирования ответа на запрос пользователя необходимо выполнить следующее:

1. Открыть вкладку **Администрирование запросов** программы Aladdin SecureAdmin.
2. Ввести запрос, полученный от пользователя.
3. Ввести серийный номер носителя Aladdin LiveOffice с помощью которого был сформирован запрос.
4. Нажать на кнопку <**Сгенерировать ответный код**>.

После проделанных действий в поле **Сгенерированная последовательность** появится ответ на полученный запрос. Сгенерированная последовательность должна быть передана пользователю, создавшему запрос на определенные действия, по сторонним каналам связи.

Программа Aladdin SecureAdmin поддерживает администрирование (обработку) запросов на регистрацию/удаление СВТ и разблокировку носителей только от пользователей, носители которых были инициализированы ранее действующим мастер-ключом администратора. В иных случаях программа Aladdin SecureAdmin выдаст сообщение об ошибке.

5.2.1.4 Вкладка Сценарии

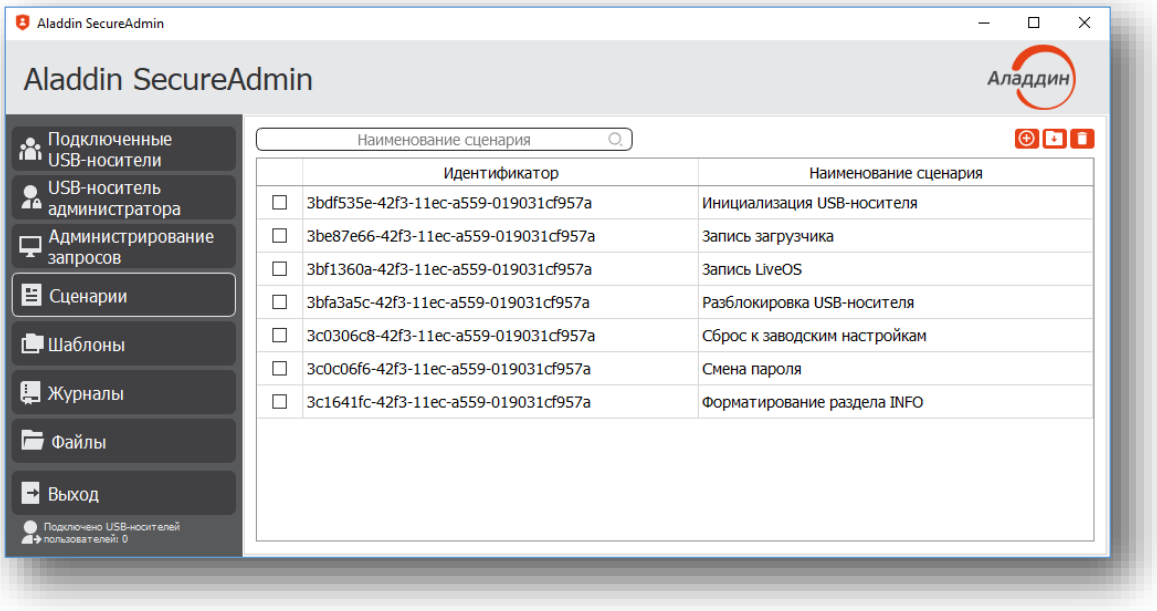

Рисунок 29 — Программа Aladdin SecureAdmin. Вкладка Сценарии

Вкладка **Сценарии** содержит в себе данные об идентификаторе сценария, наименовании сценария и кнопки <**Создать сценарий>**, <**Загрузить сценарий>**, <**Удалить>**. Редактирование сценариев осуществляется по двойному нажатию левой кнопки мыши на созданный ранее сценарий. Базовые сценарии не могут быть удалены или отредактированы.

Базовые сценарии:

1. Инициализация USB-носителя – инициализация носителя. Инициализация проводится с использованием мастер-ключа на *носителе администратора.*
2. Запись загрузчика – запись СПО LiveBoot из папки `images`.
3. Запись LiveOS – запись доверенной операционной системы из папки `images`.
4. Разблокировка USB-носителя – вывод носителя из режима "Заблокирован".
5. Сброс к заводским настройкам.
6. Смена пароля.
7. Форматирование раздела INFO.

Кнопка <**Удалить>** – позволяет удалить выбранный сценарий (за исключением базовых сценариев).

При нажатии на кнопку <**Создать сценарий>** выводится окно для ввода наименования сценария, затем выводится окно с текстовым редактором для создания нового сценария.

5.2.1.5 Вкладка Шаблоны

Вкладка Шаблоны осуществляет создание шаблонов пользователя, включающих настройку парольных политик и журналирования:

1. Параметры аутентификации:
   - Длина PIN-кода.
   - Число попыток ввода пароля.
   - Интервал времени для разблокировки.
   - Обязательность смены пароля.
   - Разрешение пользователю менять пароль.
   - Задание пароля по умолчанию.
2. Парольная политика (мощность алфавита):
   - Строчные буквы (a-z).

- Цифры (0-9).
- Прописные буквы (A-Z).
- Спецсимволы (! " # $ %...).

3. Парольная политика (срок действия пароля):
   - 1 год.
   - Неограниченно.
4. Журнал носителя (политика журналирования):
   - Циклическая перезапись.
   - Блокировать носитель до выгрузки журнала.
5. Регистрация СВТ
   - Количество попыток.
   - Максимальное число СВТ

Параметр **Интервал времени для разблокировки** определяет промежуток времени, через который пользователю будет предоставлена одна попытка ввода пароля.

Пользователю всегда будет доступна попытка ввода пароля, только спустя установленное время.

Параметр **Число попыток** определяет количество попыток ввода пароля пользователем.

При исчерпании попыток ввода пароля LiveToken пользователя будет заблокирован.

Параметр **Обязательная смена пароля** требует от пользователя сменить пароль, установленный по умолчанию на новый.

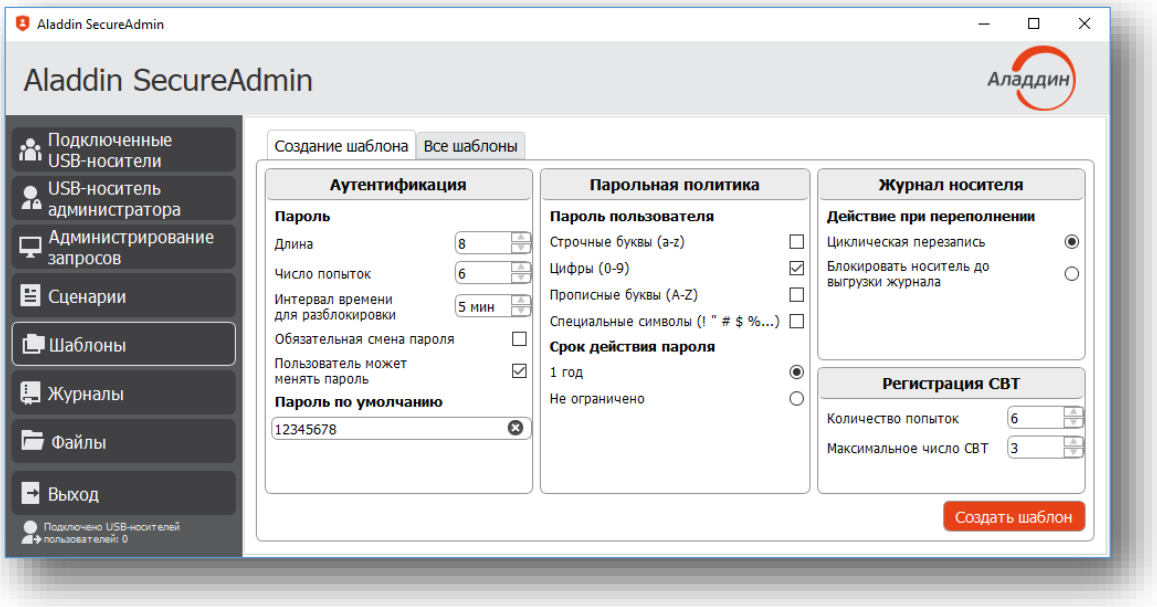

Рисунок 30 — Программа Aladdin SecureAdmin. Вкладка Шаблоны

5.2.1.6 Вкладка Журналы

Вкладка **Журналы** состоит из двух подвкладок **Журнал событий** и **Локальный журнал**.

Журнал событий разделен на три журнала:

- Журнал событий безопасности.
- Журнал администрирования.
- Журнал эксплуатации.

Для заполнения журнала событий в программе Aladdin SecureAdmin необходимо нажать на кнопку <**Импортировать журналы с носителя**> (см. Рисунок 31) указав при этом носитель с которого будет осуществлен импорт.

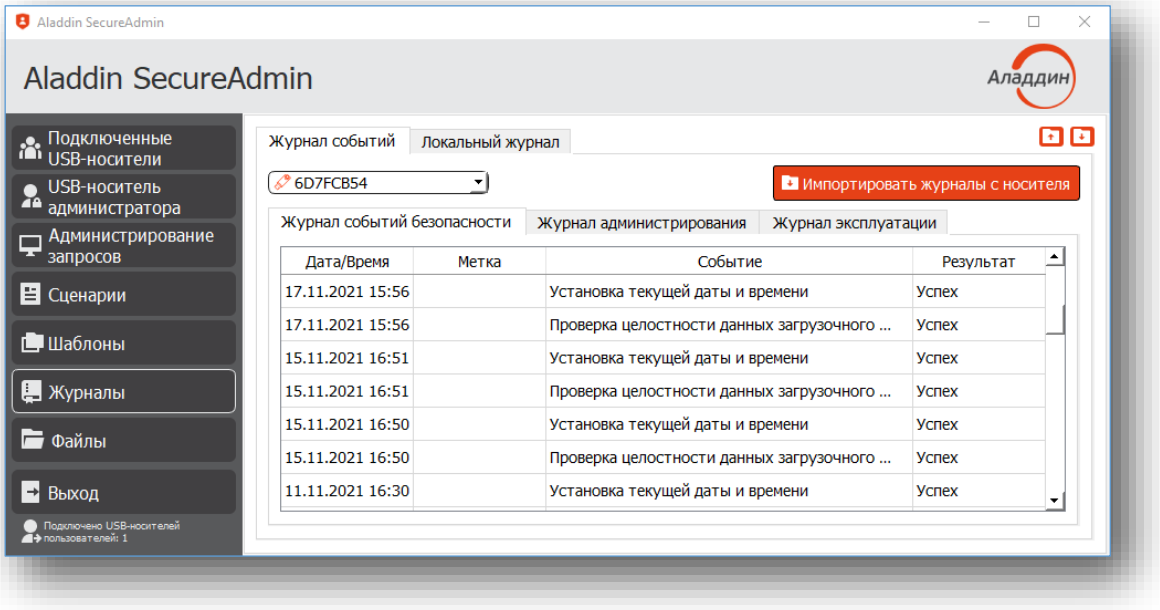

Рисунок 31 — Программа Aladdin SecureAdmin. Вкладка Журнал событий

После импорта журнала с выбранного носителя все три журнала будут в базе программы. При повторном импорте происходит запись новых событий (старые события при этом не дублируются).

Вкладка **Локальный журнал** содержит сведения о действиях администратора (см. Рисунок 32). Сведения данного журнала хранятся в базе программы и относятся к определенному носителю администратора.

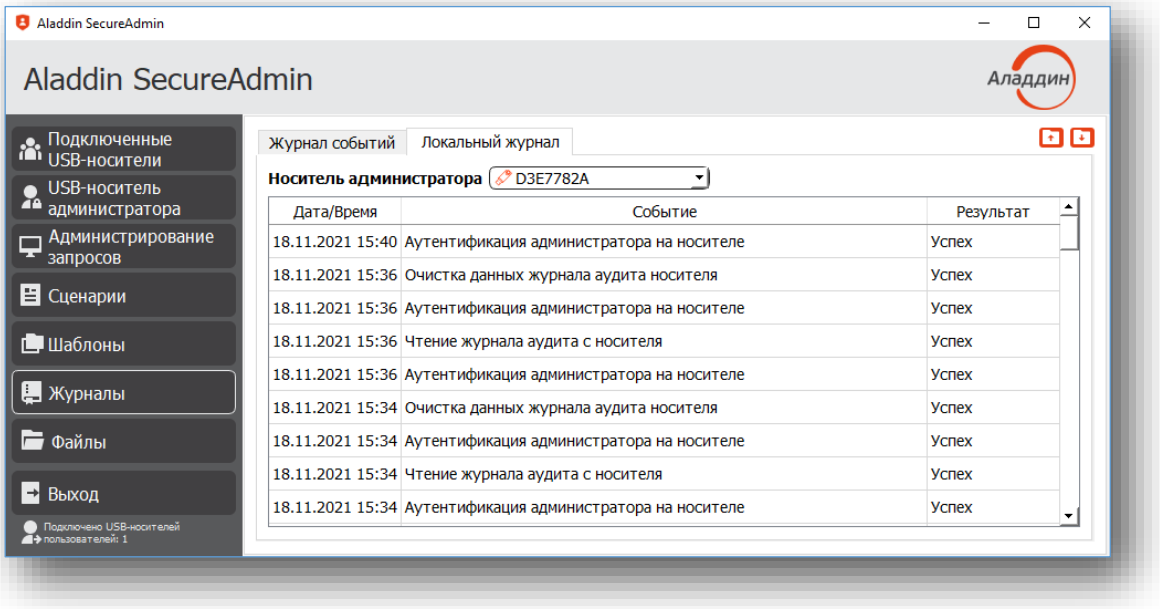

Рисунок 32 — Программа Aladdin SecureAdmin. Вкладка Локальный журнал

Также вкладка **Журналы** содержит кнопки экспорта и импорта базы (таблиц) журнала. При экспорте базы происходит создание файла базы данных, который затем можно импортировать на другой программе Aladdin SecureAdmin.

5.2.1.7 Вкладка Файлы

Вкладка **Файлы** предоставляет возможность администратору производить операции (загрузка/удаление) с файлами на прикладном разделе и в разделе INFO.

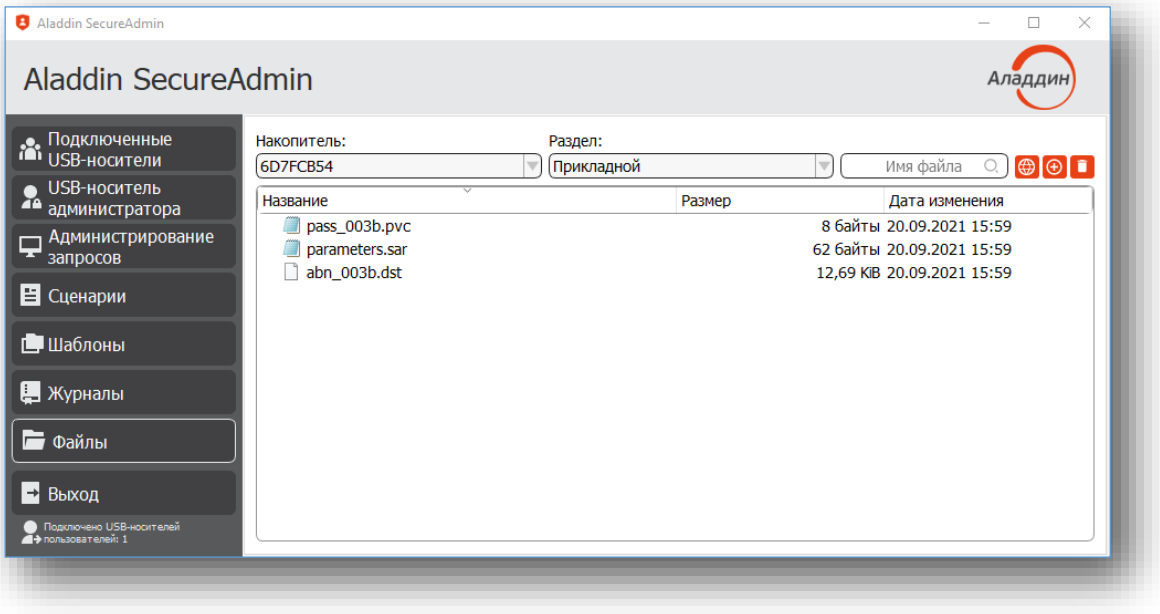

Рисунок 33 — Вкладка Файлы

Во вкладке представлены кнопки по заданию настроек от SecurLogon (доступно только при выборе прикладного раздела), добавлению и удалению файлов. Данная вкладка служит в основном для персонализации носителей пользователей.

5.2.2 Настройка носителя администратора безопасности

5.2.2.1 Создание носителя администратора

Создание носителя администратора безопасности происходит путем генерации и записи мастер-ключа на носитель Aladdin LiveAdmin с помощью программы Aladdin SecureAdmin.

Для создания *носителя администратора* выполните следующие действия:

1. Подключите одно изделие Aladdin LiveAdmin к СВТ.
2. Запустите программу Aladdin SecureAdmin.
3. Введите PIN-код администратора, заданный по умолчанию (1234567890).
4. Перейдите на вкладку **USB-носитель администратора**.
5. Нажмите кнопку <**Сменить PIN-код**>.
6. В появившемся окне введите текущий PIN-код и дважды введите новый.
7. Нажмите кнопку <**OK**>.
8. Нажмите кнопку <**Сгенерировать ключ**>.
9. Дождитесь генерации мастер-ключа.

Носитель администратора Aladdin LiveAdmin инициализирован и готов к работе с носителями пользователей.

5.2.3 Настройка, обслуживание и персонализация изделия Aladdin LiveToken пользователя

Подготовка носителя к эксплуатации состоит из четырёх этапов:

1. Инициализация носителя.
2. Персонализация носителя.
3. Смена пароля от изделия пользователем.
4. Выдача разрешения на эксплуатацию носителя на конкретных СВТ.

5.2.3.1 Инициализация Aladdin LiveToken для пользователей

Инициализация *носителей пользователей* осуществляется в следующем порядке:

1. В соответствии с подпунктом 5.2.2.1 Создайте носитель администратора или воспользуйтесь ранее созданным.
2. Перейдите на вкладку **Подключенные USB-носители**.
3. В открывшейся вкладке установите флаг в чекбокс для выбора Aladdin LiveToken, которые планируется инициализировать.
4. Далее нажмите на поле Сценарии и из выпадающего списка выберите сценарий **Инициализация USB-носителя**.

> *Информация о проинициализированных носителях отображается на вкладке "Все USB-носители".*
>
> *Если удалить информацию из вкладки "Все USB-носители", информация о проинициализированных носителях будет утеряна.*

5.2.3.2 Персонализация носителя LiveToken

Персонализация носителя зависит от используемого Aladdin LiveOffice. Так для версий Aladdin LiveOffice, использующих в качестве VPN клиента ViPNet Client 4U for Linux необходимо выполнить следующее:

1. Сформируйте следующие файлы для записи на носитель пользователя:
   - файл дистрибутива ключей (.dst-файл), создаваемый администратором сети ViPNet в программе ViPNet Administrator или ViPNet Network Manager для каждого пользователя сетевого узла ViPNet;
   - файл с паролем от файла дистрибутива ключей (.pvc). Данный файл содержит только пароль для определенного файла дистрибутива ключей. Структура названия файла: pass_<наименование .dst файла без расширения>.pvc. Файл содержит следующие параметры:
     – 127.0.0.1 (содержит адрес доверенного сервера внутри корпоративной сети. Данный параметр необходим для корректной работы индикации в подключаемых изделиях к сети организации);

> *Указанный параметр задается только в случае использования РЕД ОС в качестве доверенной операционной системы.*

     – 11111111 (пароль от файла дистрибутива ключей, задаваемый администратором вручную. Пароль от контейнера задается при его создании).
   - файл настроек для программы SecurLogon (parameters.sar), содержащий следующие параметры (см. Рисунок 34):
     – rdp-server=ip_address (содержит IP-адрес RDP сервера);
     – user=name (содержит имя пользователя);
     – host=name (содержит имя хостовой машины);
     – smartcard-rdp=0 (указывается тип подключения: 0 – по логину и паролю, 1 – по ЭЦП).

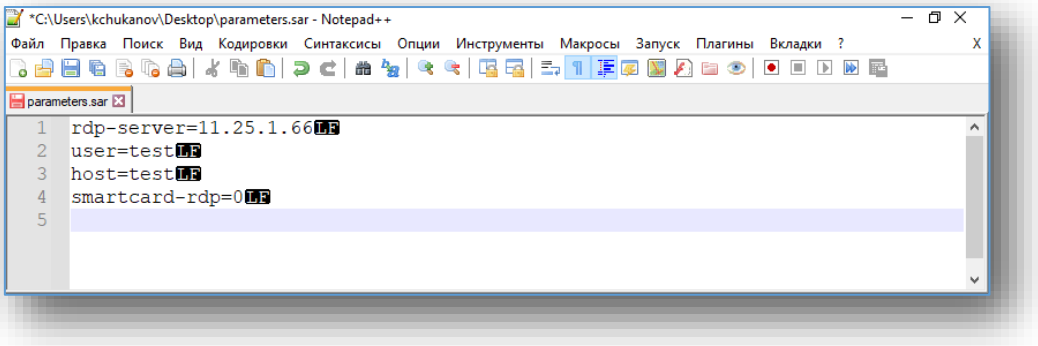

Рисунок 34 — Вид содержимого файла parameters.sar в Notepad

Обязательно убедитесь, что при создании файлов parameters.sar и pass_*.pvc в конце каждой строки стоит символ LF (переход на следующую строку). При отсутствии данного символа происходит некорректная обработка указанных данных.

Файл настройки программы SecurLogon может быть также сформирован с помощью программы Aladdin SecureAdmin. Для этого необходимо перейти во вкладку "Файлы", выбрать носитель и его прикладной раздел, нажать на кнопку в виде глобуса. В появившемся окне (см. Рисунок 35) ввести необходимые данные.

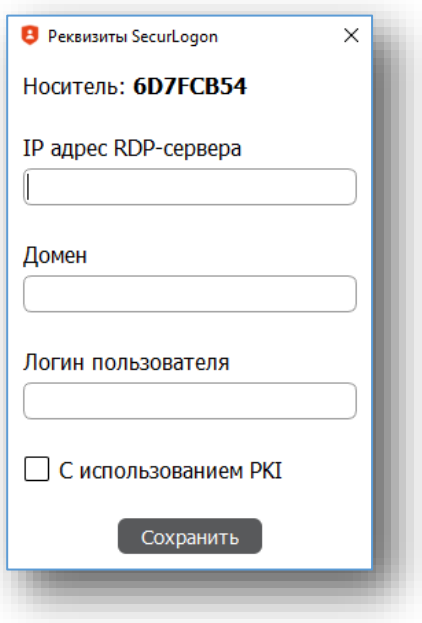

Рисунок 35 — Окно настройки параметров подключения RDP с помощью программы SecurLogon

После ввода необходимых данных в указанной форме и нажатия кнопки <**Сохранить**> произойдет автоматическое создание файла parameters.sar со структурой, описанной ранее.

2. Запустите программу Aladdin SecureAdmin.
3. Подключите носитель администратора Aladdin LiveAdmin и введите PIN-код.

По умолчанию на носитель администратора установлен PIN-код 1234567890.

4. Подключите носитель пользователя.
5. Перейдите во вкладку "**Подключенные USB-носители**".
6. Выберите носитель пользователя и проведите его инициализацию, применив соответствующий сценарий.
7. Перейдите во вкладку "**Файлы**".
8. Выберите накопитель пользователя и его прикладной раздел через выпадающие окна.
9. Нажмите на кнопку загрузки файлов ("плюс").
10. Выберите сформированные в п.1 файлы и нажмите на кнопку <**Загрузить**>.

Носитель с VPN клиентом ViPNet Client 4U for Linux готов к передаче пользователю. При загрузке доверенной ОС автоматически произойдет подключение к частной сети, через которую будет осуществляться RDP подключение к удаленному рабочему месту.

Для версий Aladdin LiveOffice, использующих в качестве VPN клиента "VPN/FW "ЗАСТАВА" версия 6". Клиент" при персонализации носителей необходимо выполнить следующие действия:

1. Сформируйте следующие файлы для записи на носитель пользователя:
   - файл настроек для программы SecurLogon (parameters.sar), содержащий следующие параметры:
     - rdp-server=ip_address (содержит IP-адрес RDP сервера);
     - user=name (содержит имя пользователя);
     - host=name (содержит имя хостовой машины);

  - smartcard-rdp=0 (указывается тип подключения: 0 – по логину и паролю, 1 – по ЭЦП)
- файл zastava.pvc в формате ipaddress=<IP адрес сервера политик> содержащий перечень IP адресов серверов политик, устанавливающих перечень адресов к которым может подключиться пользователь и номер лицензии в формате licenseCSP=00000-00000-00000-00000-00000.

Наличие файла *zastava.pvc* на прикладном разделе является не обязательным. Файл загружается только при необходимости корректировки любого и заданных параметров - номер лицензии или IP-адрес сервера политики.

2. Запустите программу Aladdin SecureAdmin.
3. Подключите носитель администратора Aladdin LiveAdmin и введите PIN-код.

По умолчанию на носитель администратора установлен PIN-код 1234567890.

4. Подключите носитель пользователя.
5. Перейдите во вкладку "**Подключенные USB-носители**".
6. Выберите носитель пользователя и проведите его инициализацию, применив соответствующий сценарий.
7. Перейдите во вкладку "**Файлы**".
8. Выберите накопитель пользователя и его прикладной раздел через выпадающие окна.
9. Нажмите на кнопку загрузки файлов ("плюс").
10. Выберите сформированные в п.1 файлы и нажмите на кнопку <**Загрузить**>.
11. Завершите работу с программой Aladdin SecureAdmin.
12. Запустите приложение (криптопровайдер) КриптоПро CSP.

На данном этапе администратором должны быть сформированы контейнеры личных сертификатов пользователей, для последующей записи на носители Aladdin LiveOffice.

13. Выполните запись контейнера личного сертификата на апплет Laser (LiveOffice). Запись контейнера осуществляется в следующем порядке:
    a. В приложении КриптоПро CSP нажмите на вкладку "**Сервис**".
    b. В разделе "**Контейнер закрытого ключа**" нажмите на кнопку <**Скопировать**>.
    c. Нажмите на кнопку <**Обзор…**> и выберите ключевой контейнер пользователя, сформированный в УЦ.
    d. Нажмите кнопку <**Далее**>.
    e. Введите имя для создаваемого ключевого контейнера.
    f. Нажмите на кнопку <**Готово**>.
    g. В открывшемся окне выберите подключенный носитель пользователя (Aladdin LiveOffice) в разделе "**Устройства**" и нажмите кнопку <**OK**>.
    h. Введите PIN-код для записи контейнера.

По умолчанию установлен пароль: 11111111.

После удачного ввода пароля появится сообщение об успешном копировании контейнера на носитель пользователя.

Носитель пользователя готов к передаче пользователю и может эксплуатироваться в соответствии с руководством пользователя.

5.2.3.3 Разблокировка USB-носителя

При невыполнении условий эксплуатации носителя, например, превышении количества попыток ввода PIN-кода пользователем, USB-носитель переходит в режим блокировки.

Для разблокирования носителя (перевода носителя в штатный режим работы), выполните следующие действия:

1. Подключите носитель администратора и запустите программу Aladdin SecureAdmin.
2. Подключите носитель пользователя.

В программе Aladdin SecureAdmin:

1. Перейдите на вкладку **Подключенные USB-носители**.
2. На вкладке подключенные USB-носители найдите носитель пользователя, который необходимо разблокировать.

3. Установите флаг в чекбокс (выберите USB-носитель).
4. Выберите сценарий Разблокировка USB-носителя.
5. Нажмите кнопку <**Применить сценарий**>.

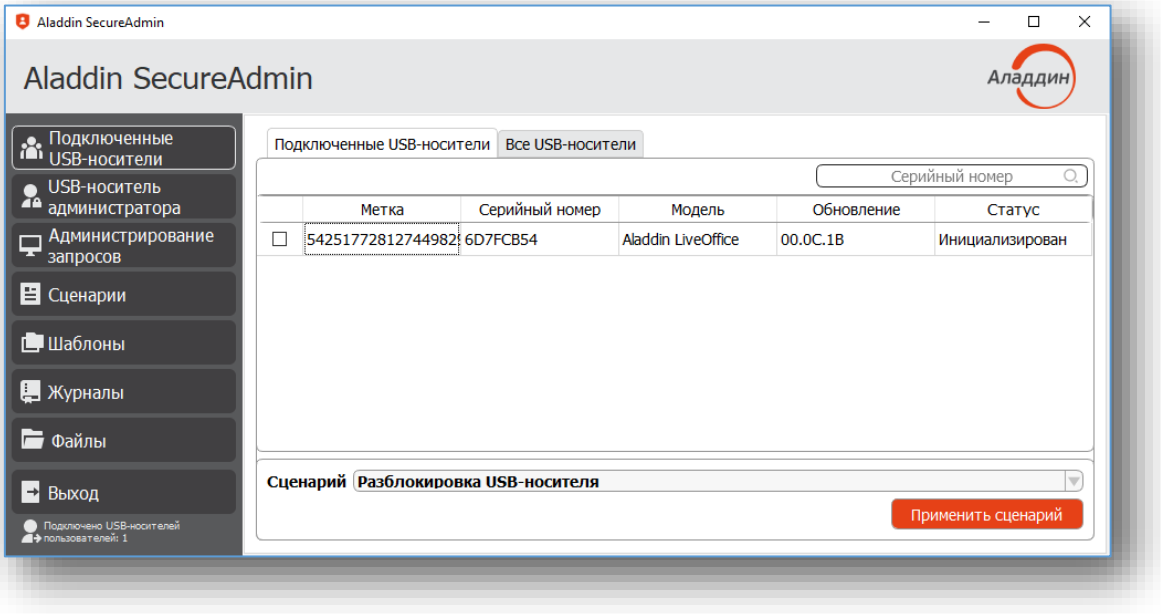

Рисунок 36 — Разблокировка USB-носителя локально

Для разблокировки носителя удаленно необходимо выполнить следующее:

1. Получить запрос на разблокировку и серийный номер устройства от пользователя по сторонним канал связи.
2. Ввести полученные данные в программе Aladdin SecureAdmin во вкладке **Администрирование запросов**.
3. Нажать на кнопку <**Сгенерировать ответный код**>.
4. Передать пользователю сгенерированную последовательность.

После ввода пользователем полученного от администратора ответа произойдет разблокировка устройства

5.2.3.4 Сброс к заводским настройкам

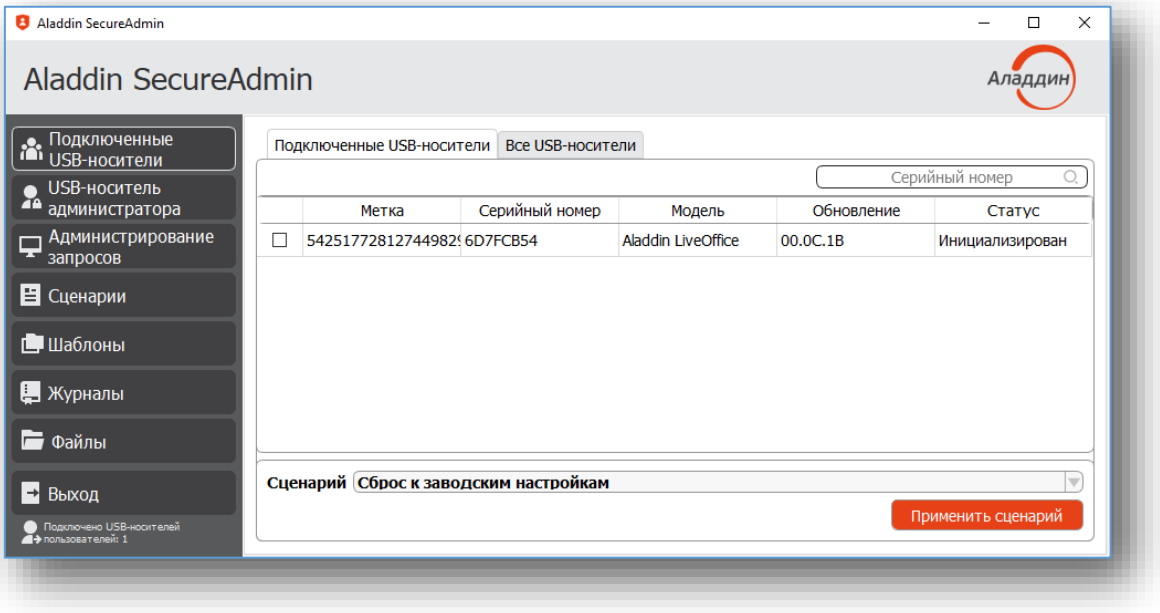

Рисунок 37 — Сброс к заводским настройкам

Для перевода носителя в первоначальное состояние (к заводским настройкам), выполните следующие действия:

1. Подключите носитель администратора и запустите программу Aladdin SecureAdmin.
2. Подключите носитель пользователя.

В программе Aladdin SecureAdmin:

1. Перейдите на вкладку **Подключенные USB-носители**.
2. На вкладке подключенные USB-носители найдите носитель пользователя, который необходимо разблокировать.
3. Установите флаг в чекбокс (выберите USB-носитель).
4. Выберите сценарий **Сброс к заводским настройкам**.
5. Нажмите кнопку <**Применить сценарий**>.

5.2.3.5 Обновление СПО LiveBoot и (или) образа операционной системы LiveOS

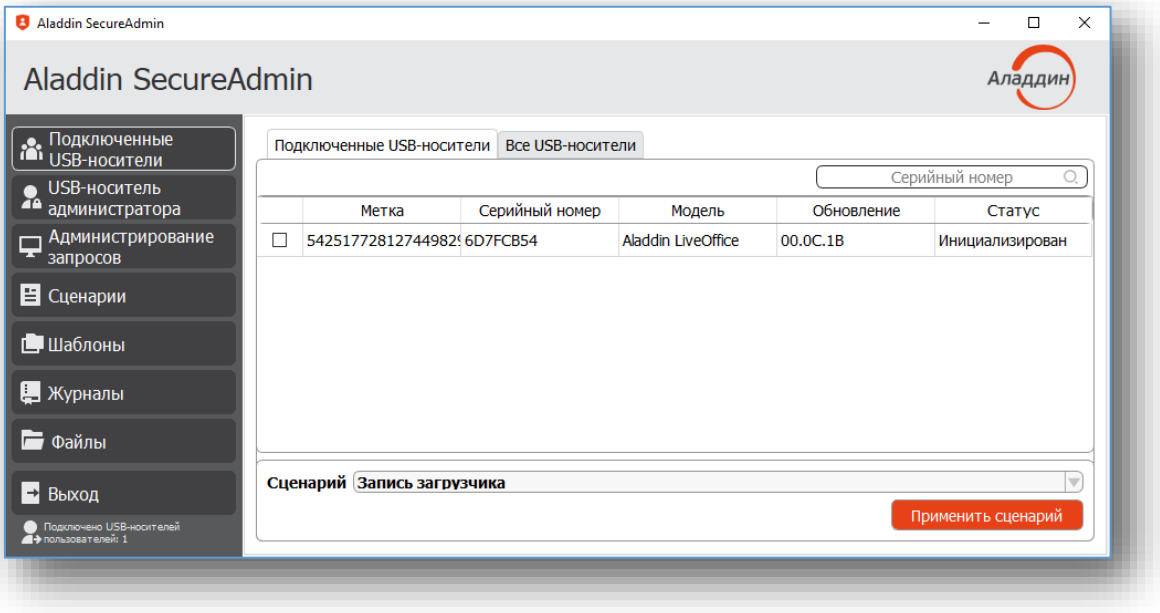

Рисунок 38 — Обновление LiveBoot

> *Программа осуществляет поиск LiveBoot и LiveOS в соответствии со сценарием. В сценарии указывается место хранения файла-образа LiveBoot и LiveOS и его наименование, поэтому перед использованием сценария **Запись загрузчика** или **Запись LiveOS** необходимо изучить применяемый сценарий и подготовить образ в соответствии с ним.*

Для обновления СПО LiveBoot или образа операционной системы (перевода носителя в штатный режим работы), выполните следующие действия:

1. Подключите носитель администратора и запустите программу Aladdin SecureAdmin.
2. Подключите носитель пользователя.

В программе Aladdin SecureAdmin:

1. Перейдите на вкладку **Подключенные USB-носители**.
2. На вкладке подключенные USB-носители найдите *носитель пользователя*, который необходимо разблокировать.
3. Выберите носитель с помощью чекбокса.
4. Выберите сценарий **Запись загрузчика** или сценарий **Запись LiveOS**.
5. Нажмите кнопку <**Применить сценарий**>.
6. Дождитесь записи образа на носитель.

5.2.4 Работа со сценариями

Работа со сценариями осуществляется на вкладке **Сценарии**, описанной в пункте 5.2.1.4, [с.46].

5.2.5 Создание сценариев

Для создания собственных сценариев администрирования выполните следующие действия:

1. Подключите носитель администратора.
2. Запустите программу Aladdin SecureAdmin.
3. Перейдите на вкладку **Сценарии**.
4. В открывшейся вкладке нажмите на кнопку <**Добавить сценарий**> (в виде значка), представленную на рисунке ниже.
5. Введите имя сценария.
6. Нажмите кнопку <**OK**> для перехода в текстовый редактор.

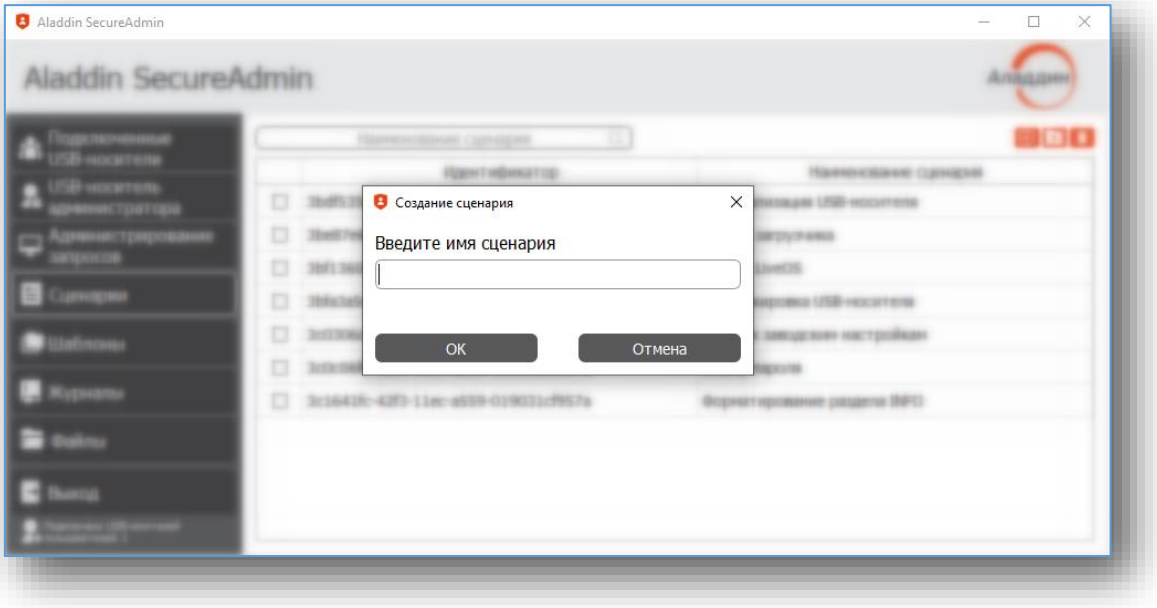

Рисунок 39 — Окно для ввода наименования сценария

7. Осуществите запись нового сценария путем задания последовательности операций.
8. Нажмите на кнопку <**OK**>. Сценарий будет успешно создан.

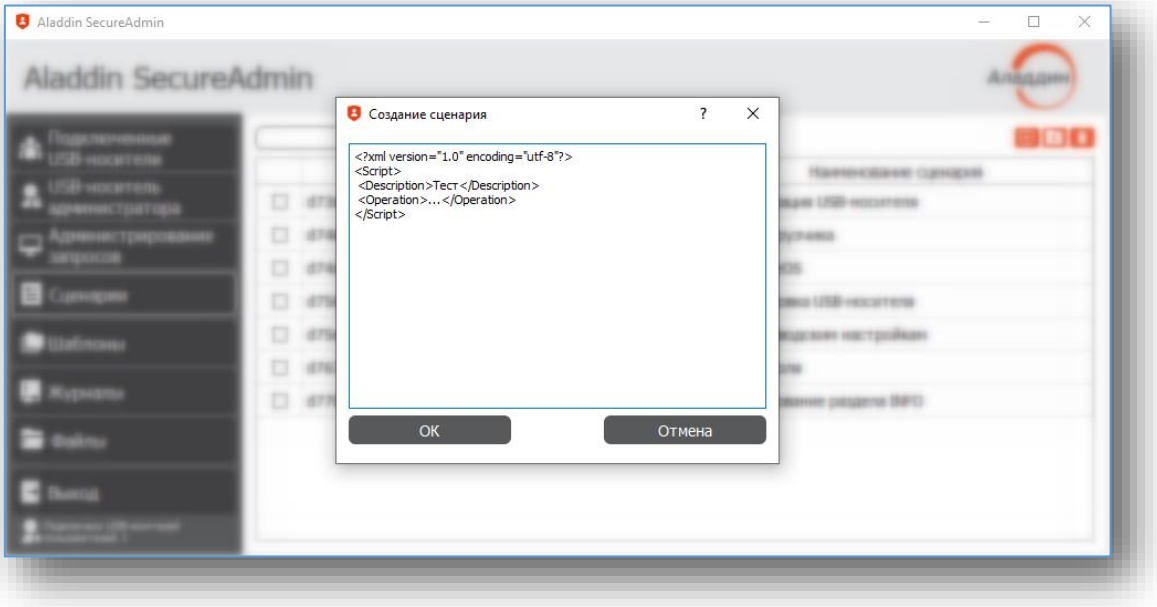

Рисунок 40 — Окно создания сценария

Сценарии представляют собой xml-файлы с инструкциями администрирования в специальном формате:

1. `<?xml version="1.0" encoding="utf-8"?>` – стандартное описание xml-файла;
2. `<Script></Script>` – тег начала и конца описания сценария (обязательная секция);
3. `<Description>Script Name</Description>` – название сценария (обязательная секция);
4. `<Operation>ActivateSD</Operation>` – операция;
5. `<Operation lun="boot" file="LiveBoot.img">LoadImage</Operation>` – операция с параметрами.

Операции доступные для создания сценариев администрирования.

- `<Operation>FactoryReset</Operation>` – сброс к заводским настройкам.

- `<Operation force="false">CleanSD</Operation>` – очистка SD-карты, параметр `force` принимает значение `true` (принудительная очистка) и `false` (ожидание завершения текущих операций токена).
- `<Operation lun="boot" file="LiveBoot.img">LoadImage</Operation>` – запись образа. Параметр `lun` принимает значения: `LiveBoot` (загрузчик) и `LiveOS` (образ ОС), в параметре `file` указывается путь к образу для записи.
- `<Operation>ActivateSD</Operation>` – активация SD-карты.
- `<Operation template="xxxxxx-xx-…-xxxxxx">CreateUser</Operation>` – инициализация пользовательского пароля и применение шаблона `template`.
- `<Operation>DeleteUser</Operation>` – удаление пользователя и настроек.
- `<Operation lun="boot">CalcCheckSum</Operation>` – проверка контрольной суммы раздела.
- `<Operation>UnlockPIN</Operation>` – разблокирование счетчиков неудачных попыток ввода пароля.
- `<Operation>ChangePsw</Operation>` – смена пароля USB-носителя.

5.2.5.1 Базовые сценарии

Все доступные сценарии отображаются на вкладке **Сценарии**. SecureAdmin позволяет создавать/загружать/удалять собственные сценарии администрирования, но необходимо строго соблюдать вышеописанный формат.

Сценарии, созданные автоматически при первом запуске программы, не удаляются. Используя как пример базовые сценарии, можно создавать собственные и сохранять их в базе данных.

5.2.5.2 Инициализация Aladdin LiveToken

Описание работы сценария:

1. Создается пользователь с паролем по умолчанию 12345678.
2. Активируется microSD-карта.
3. Данные LiveToken заносятся в таблицу **Все USB-носители**.

Таблица 12 – Содержание сценария "Инициализация USB-носителя"

Наименование	**Описание**
<?xml version="1.0" encoding="utf-8"?>	Стандартное описание xml-файла
<Script>	Тег начала описания сценария(обязательная секция)
<Description>Инициализация USB-носителя</Description>	Название сценария (обязательная секция)
<Operation template="xxxxxx-xx-…-xxxxxx">CreateUser</Operation>	Инициализация пользовательского пароля и применение настроек шаблона, параметр template принимает значение уникального идентификатора шаблона из таблицы "Все шаблоны";
<Operation>ActivateSD</Operation>	Активация microSD-карты;
<Operation lun="boot"> CalcCheckSum</Operation>	Вычисление контрольной суммы загрузчика
<Operation lun="liveos"> CalcCheckSum</Operation>	Вычисление контрольной суммы доверенной ОС
</Script>	Тег конца описания сценария(обязательная секция)

5.2.5.3 Запись загрузчика

Описание работы сценария:

1. В LUN0 записывается образ LiveBoot.img.

Таблица 13 – Содержание сценария "Запись загрузчика"

Наименование	**Описание**
<?xml version="1.0" encoding="utf-8"?>	Стандартное описание xml-файла
<Script>	Тег начала описания сценария(обязательная секция)
<Description>Запись загрузчика</Description>	Название сценария (обязательная секция)
<Operation lun="boot" file="LiveBoot.img"> LoadImage</Operation>	Запись образа. Параметр lun принимает значения: LiveBoot(загрузчик), в параметре file указывается путь к образу для записи;
</Script>	Тег конца описания сценария(обязательная секция)

5.2.5.4 Запись LiveOS

Описание работы сценария:

1. В LUN1 записывается образ доверенной ОС.

Таблица 14 – Содержание файл сценария Запись LiveOS

Наименование	**Описание**
<?xml version="1.0" encoding="utf-8"?>	Стандартное описание xml-файла
<Script>	Тег начала описания сценария(обязательная секция)
<Description>Запись LiveOS</Description>	Название сценария (обязательная секция)
<Operation lun="liveos" file="LiveOS.iso"> LoadImage</Operation>	Запись образа. Параметр lun принимает значения: LiveOS (образ ОС), в параметре file указывается путь к образу для записи
</Script>	Тег конца описания сценария(обязательная секция)

5.2.5.5 Разблокировка USB-носителя

Описание работы сценария:

1. Происходит сброс счетчиков неудачных попыток ввода пароля.

Таблица 15 – Содержание файл сценария Разблокировка USB-носителя

Наименование	**Описание**
<?xml version="1.0" encoding="utf-8"?>	Стандартное описание xml-файла
<Script>	Тег начала описания сценария(обязательная секция)
<Description>Разблокировка USB-носителя</Description>	Название сценария (обязательная секция)
<Operation>UnlockPIN</Operation>	Разблокировка счетчиков неудачных попыток ввода пароля

</Script>	Тег конца описания сценария(обязательная секция)

5.2.5.6 Сброс к заводским настройкам

Описание работы сценария:

1. USB-носитель сбрасывается к заводским настройкам.
2. Из таблицы "Все USB-носители" удаляются данные LiveToken.

Таблица 16 – Содержание файл сценария Сброс к заводским настройкам

Наименование	**Описание**
<?xml version="1.0" encoding="utf-8"?>	Стандартное описание xml-файла
<Script>	Тег начала описания сценария(обязательная секция)
<Description>Сброс к заводским настройкам</Description>	Название сценария (обязательная секция)
<Operation>FactoryReset</Operation>	Сброс к заводским настройкам
</Script>	Тег конца описания сценария(обязательная секция)

5.2.5.7 Смена пароля

Описание работы сценария:

1. После нажатия на кнопку <**Применить сценарий**> администратору отображается окно ввода нового пароля с подтверждением текущего пароля.
2. Устанавливается новый пароль для пользователя LiveToken.

Таблица 17 – Содержание файл сценария "Смена пароля"

Наименование	**Описание**
<?xml version="1.0" encoding="utf-8"?>	Стандартное описание xml-файла
<Script>	Тег начала описания сценария(обязательная секция)
<Description>Смена пароля</Description>	Название сценария (обязательная секция)
<Operation>ChangePsw</Operation>	Смена пароля LiveToken
</Script>	Тег конца описания сценария(обязательная секция)

5.2.5.8 Форматирование раздела INFO

Описание работы сценария:

1. После нажатия на кнопку <**Применить сценарий**> происходит форматирование раздела INFO (при этом происходит удаление всей информации из данного раздела).

Таблица 18 – Содержание файл сценария "Форматирование раздела INFO"

Наименование	**Описание**
<?xml version="1.0" encoding="utf-8"?>	Стандартное описание xml-файла
<Script>	Тег начала описания сценария(обязательная секция)
<Description>Смена пароля</Description>	Название сценария (обязательная секция)

<Operation>FormatInfo</Operation>	Форматирование раздела INFO
</Script>	Тег конца описания сценария(обязательная секция)

5.2.5.9 Создание и применение шаблонов

Создание шаблонов администрирования осуществляется во вкладке **Шаблоны** путем выбора требуемых настроек и нажатия на кнопку <**Создать шаблон**>. SecureAdmin выведет окно представленное на рисунке 41 для ввода имени шаблона.

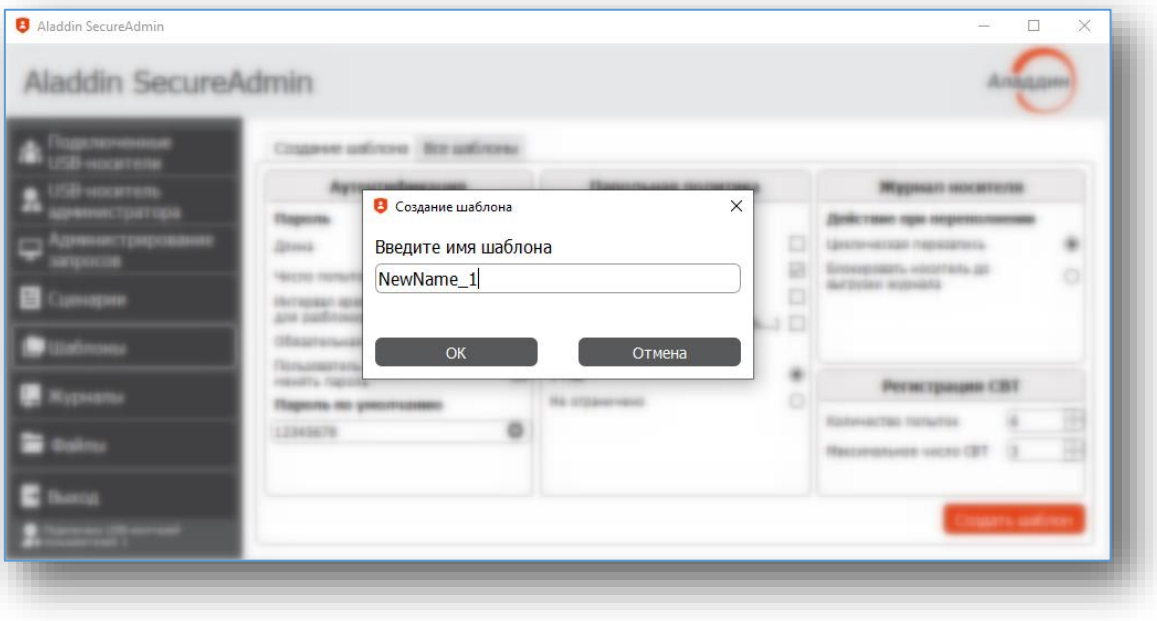

Рисунок 41 – Окно создания шаблона

Все созданные шаблоны отображаются на вкладке **Все шаблоны.**

Вкладка **Все шаблоны** содержит в себе:

1. Имя файла.
2. Название шаблона.
3. Дату создания шаблона.
4. Кнопку <**Удалить>**.
5. Базовый шаблон.

Кнопка <**Удалить>** – позволяет удалить выбранный шаблон.

Применение шаблонов осуществляется на этапе создания сценариев. При создании пользователя в параметрах сценария прописывается имя файла.

Таблица 19 – Пример использования

Наименование	Описание
<Operation template="xxxxxx-xx-...-xxxxxx">CreateUser</Operation>	Инициализация пользовательского пароля и применение настроек шаблона, параметр template принимает значение уникального идентификатора шаблона из таблицы "Все шаблоны"

Приложение А. Меры по защите машинных носителей информации

А.1 Защита машинных носителей информации

Таблица А.1 – Защита машинных носителей информации

ЗНИ.0	Регламентация правил и процедур защиты машинных носителей
ЗНИ.1	Учёт машинных носителей информации
ЗНИ.2	Управление физическим доступом к машинным носителям информации
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны
ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации
ЗНИ.6	Контроль ввода (вывода) информации на съемные машинные носители информации
ЗНИ.7	Контроль подключения съемных машинных носителей информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации

Приложение Б. Порядок приёмки изделия

Б.1 Общее описание комплекта поставки

Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice поставляется в соответствии с заключенным договором, в комплектности, описанной в разделе 5 "Комплектность поставки" документа "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice. Формуляр" (АЛДЕ.467669.011ФО).

В Договоре указываются исполнения поставляемого изделия "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice", а также наличие/отсутствие средств криптографической защиты (Криптотокен 2 ЭП, исполнение 9), "АРМ администратора безопасности "JaCarta"), обозначенные как "**в соответствии с запросом**".

Б.1.1 Электронные носители

Электронные носители Aladdin LiveToken АЛДЕ.467669.012 из состава изделий поставляются в:

- пластиковых упаковках – блистерах, включающих от 1 до 10 изделий;
- картонных упаковках, с нанесённым логотипом АО "Аладдин Р. Д.", включающих от 1 до 5 блистеров.

Каждому блистеру соответствует уникальный идентификационный номер, содержащий информацию о уникальных идентификационных номерах носителей.

Каждой картонной упаковке соответствует уникальный номер, дублируемый штрихкодом в формате EAN-13, наносимый на упаковку или добавляемый в упаковку на специальном вкладыше.

Перечень штрихкодов и уникальных номеров носителей, передаваемых в блистерах, передаётся официальному лицу организации-приобретателя "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice".

Б.1.2 Программные компоненты

Встроенное программное средство передаётся в составе электронного носителя.

Обновления на программное средство передаются по защищенным каналам в виде отдельных файлов. Для каждого передаваемого файла рассчитывается и передаётся контрольная сумма.

Программы из комплекта программных средств передаются на поставочном диске.

Для файлов программ из комплекта программных средств рассчитываются контрольные суммы, указываемые в формуляре изделия.

Для поставочного диска рассчитывается контрольная сумма, наносимая на диск или упаковку, в которой передаётся поставочный диск.

Б.1.3 Документация на изделие

Каждая партия изделий обязательно сопровождается формуляром, поставляемым в печатном виде и приложением к формуляру, поставляемым в электронном или печатном виде.

В формуляре на изделие содержится следующая контрольная информация:

- идентификационная информация изделия;
- контрольные суммы на файлы программ;
- сведения о упаковке и приёмке изделия.

Приложение Б к формуляру на изделие включает в себя:

- серийный (заводской) номер изделия;
- идентификатор изделия;
- дату изготовления изделия;
- номера СКЗИ из состава изделия.

Б.2 Процедуры поставки Aladdin LiveOffice

Б.2.1 Требования к процедуре поставки

Процедуры поставки должны соответствовать требованиям, установленным п. 13.3.3 ГОСТ 15408-3, и включают действия получателя Aladdin LiveOffice, направленные на выполнение этих требований. В рамках выполнения требований:

1. Обеспечивается точное соответствие между изделием, полученным заказчиком, и изделием, прошедшим оценку сертификационной лабораторией.
2. Обеспечивается защиту от подделки актуальной версии "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice".
3. Предотвращается поставки фальсифицированной версии "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice".
4. Обеспечивается защита от утечки информации о распространении Aladdin LiveOffice заказчику.
5. Предотвращается задержка или срыв поставки.

> *Окончанием фазы поставки считается момент передачи продукции под ответственность заказчика. Заказчик после получения продукции должен соблюдать положения поставляемой документации.*

Б.2.2 Сведения о порядке поставки

Поставка Aladdin LiveOffice состоит из четырёх этапов:

1. Комплектация поставки.
2. Хранение сформированных комплектов поставки.
3. Доставка комплекта поставки.
4. Приёмка изделий.

На этапе комплектации поставки выполняются процедуры по производству изделий, подготовки соответствующей документации и прикладного ПО. На этапе хранения производится хранение готовых комплектов поставки на складе АО "Аладдин Р.Д." (далее Компания).

> *На этапе доставки осуществляется доставка заказчику. Этап приёмки изделий включает в себя получение изделий заказчиком, проверку соответствия поставляемой продукции – заявленной.*

Б.2.3 Этапы поставки и меры, принимаемые для выполнения требований

Б.2.3.1 Комплектация

При проверке на производстве считывается и сверяются контрольные суммы ПО.

> *Процесс приёмки предусматривает возможность проверки контрольных сумм изделия организацией-получателем.*

При производстве изделий Aladdin LiveOffice каждому электронному носителю присваивается уникальный идентификационный номер (УИН), формируемый по защищенному алгоритму. УИН изделия гравируется на поверхности изделия и отображается в программах из состава при подключении к средствам вычислительной техники.

Документация, поставляемая в печатном виде, копируется с учтенных подлинников, хранящихся в архиве Компании.

В уникальные бумажные документы, соответствующие каждой партии изделий, уполномоченными сотрудниками Компании вносятся необходимые сведения (сведения о упаковке, сведения о приёмке и др.)

> *Соответствующие разделы должны быть заполнены при приёмке изделия.*

Документация, поставляемая в виде электронных копий печатных документов, записывается на поставочный диск.

Для поставочного диска, который включает в себя комплект ПО, электронные копии основных эксплуатационных документов и другие файлы (например, ключи подписи deb-пакетов) снимается контрольная сумма, которая наносится на верхнюю (нерабочую) поверхность диска либо печатается на этикетке.

Б.2.3.2 Доставка

Доставка продукции осуществляется по выбору заказчика:

- самостоятельно (сотрудники заказчика получают продукцию в офисе Компании);
- курьерской службой Компании.

Выдача продукции представителю заказчика осуществляется на основании предъявляемых документов, удостоверяющих полномочия. При передаче заполняется акт сдачи-приёмки с обязательным проставлением подписей и печатей.

В целях соблюдения конфиденциальности при выполнении и оформлении доставки в документах могут использоваться кодовые обозначения продукции.

Б.3 Порядок приёмки изделия

Выдача продукции представителю заказчика осуществляется на основании предъявляемых документов, удостоверяющих полномочия, в сроки, установленные договором. При передаче заполняется акт сдачи-приёмки с обязательным проставлением подписей и печатей.

При получении изделия заказчиком заполняется гарантийный талон на изделия с обязательным проставлением дат, подписей и печатей.

До проведения подготовительных процедур, уполномоченным лицом, представляющим заказчика (потребителя), проводится проверка целостности поставочного диска и программ из, входящих в состав "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice". Для проведения проверки должно применяться сертифицированное программное средство, указанное в документации на изделие.

При несовпадении контрольных сумм необходимо оповестить указанные в договоре на поставку уполномоченные лица, представляющие АО "Аладдин Р. Д.".

Приложение В.Установка и удаление программ

В.1 Общие сведения

Подготовительные процедуры включают в себя приёмку, а также подготовку к установке и, непосредственно, установку программ из состава Aladdin LiveOffice в среде функционирования.

Приёмка изделия, а также идентификация изделия и проверка целостности программных средств, поставляемых на этапе приёмки, описаны в настоящем документе в разделе "Порядок приёмки изделия" (Приложение Б).

После прохождения необходимых проверок СЗИ может быть развёрнуто в средах функционирования, удовлетворяющих условиям эксплуатации [см. раздел Требования на с. 23].

В общем виде процесс подготовки к использованию состоит из следующих фаз:

1. Подготовка СВТ к использованию Aladdin LiveOffice.
2. Установка программ из состава Aladdin LiveOffice.

При этом, подготовка СВТ к использованию Aladdin LiveOffice включает в себя следующие возможные действия:

1. Обеспечение совместимости программ из состава Aladdin LiveOffice и системных программных средств (ОС), установленных на СВТ.
2. Настройка параметров безопасности ОС, включающая выдачу необходимых для работы с Aladdin LiveOffice разрешений.

В.2 Установка программ из состава Aladdin LiveOffice на СВТ под управление ОС семейства Linux

В.2.1 Установка на СВТ с ОС Astra Linux 1.6

В.2.1.1 Установка необходимых пакетов

```
pcscd
```

Для того чтобы проверить, установлен ли пакет – выполните следующие действия:

1. Запустите командную оболочку Astra Linux (терминал Fly): главное меню ОС Astra Linux – системные – терминал Fly.
2. Проверьте наличие (статус) пакета в системе с помощью команды:

```
dpkg -s pcscd
```

Не установленный пакет будет отображен в сообщении:

dpkg-query: пакет «имя_пакета» не установлен.

Установленный пакет будет иметь статус:

Package: pakage_name

Status: install ok installed

При необходимости установите необходимый пакет с дистрибутива (с загрузочного диска ОС Astra Linux), для этого:

1. Вставьте загрузочный диск в дисковод (или подключите DVD-дисковод Вашей виртуальной машины, например, для VMware: виртуальная машина-> съёмные устройства-> CD/DVD (IDE)).
2. В терминале Fly введите следующие команды:

подключение дисковода (здесь, и далее – символом # выделен «комментарий», строка не обязательна для ввода).

```
sudo apt-cdrom add
```

получение нового списка пакетов

```
sudo apt-get update
```

установка пакета `pcscd`

```
sudo apt-get install pcscd
```

3. Ознакомьтесь с выводимой в командной строке информацией и подтвердите установку пакета `pcscd`: введите «д» с помощью кнопки <**д**> и нажмите <**Enter**>.

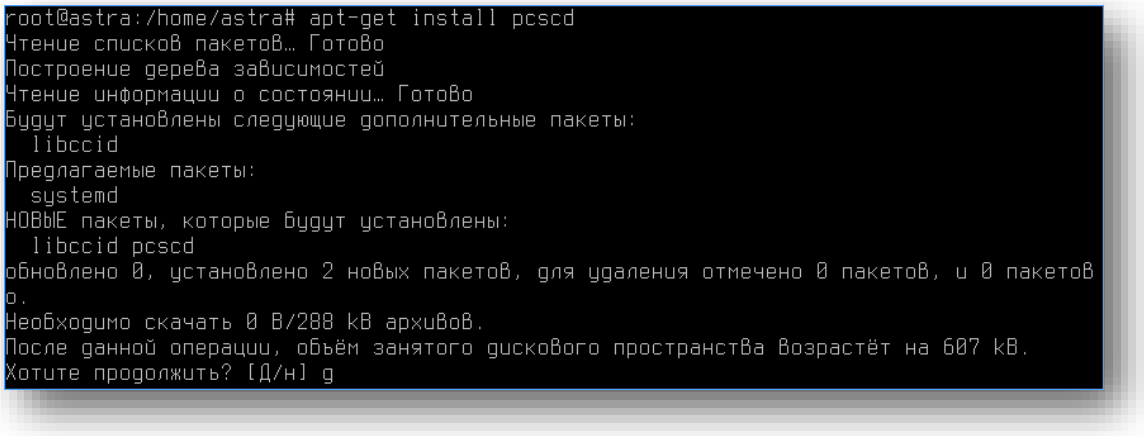

Рисунок 42 — Установка пакетов и подтверждение установки

Подробнее с информацией об управлении репозиториями и о загрузке пакетов можно ознакомиться на официальном сайте производителя операционной системы Astra Linux [https://wiki.astralinux.ru/pages/viewpage.action?pageId=3276859].

4. Добавьте службу pcscd в перечень автоматически запускаемых служб:

```
sudo systemctl enable pcscd
```

B.2.1.2 Установка программ:

Перед установкой программ из состава Aladdin LiveOffice необходимо внести следующие изменения в файлы ОС:

1. В файле `/etc/x11/fly-dm/fly-dmrc` найдите параметр:

```
#ServerUID
```

2. Удалите символ # (раскомментируйте параметр).
3. Установите значение параметра, как `root`:

```
ServerUID=root
```

4. Выполните команду:

```
systemctl restart fly-dm
```

Для установки программ из состава выполните следующие действия:

1. Переместите установочные пакеты на СВТ с Astra Linux 1.6.
2. Уточните версию ядра вашей ОС, для этого используйте команду:

```
sudo uname -a
```

3. Установите программы из состава в соответствии с составом АРМ, для этого в «терминале fly» используйте команды вида:

```
sudo dpkg –i <инсталляционный пакет>
```

Например,

```
sudo dpkg –i alo_secureadmin_1.1.0.202_al1.6_x64.deb
```

B.2.1.3 Установка программ в режиме замкнутой программной среды

Astra Linux 1.6 SE может работать в режиме замкнутой программной среды, требующем внедрения цифровой подписи на основе публичного ключа.

Использование механизма замкнутой программной среды вносит особенности в установку и использование ПО на СВТ под управлением Astra Linux 1.6.

До установки программ из состава Aladdin LiveOffice выполните следующие действия:

1. Установите пакет `astra-digsig-oldkeys`:
2. При установке с поставочного диска Astra Linux, вставьте поставочный диск в дисковод, запустите терминал fly и введите:

```
sudo apt cd-rom add

sudo apt-get update

sudo apt-get-install astra-digsig-install
```

3. В каталог `/etc/digsig/keys` поместите переданный в составе комплекта поставки открытый (публичный) ключ `ZAO_aladdin_pub_key.gpg` или Aladdin_pub.key
4. В файле `/etc/digsig/digsig_initramfs.conf` найдите параметр:

```
DIGSIG_ELF_MODE
```

5. Установите значение параметра:

```
DIGSIG_ELFMODE=2
```

6. Используйте команду:

```
update-initramfs -u -k all
```

7. Перезагрузите СВТ.
8. Установите программы из состава, соответствующие АРМ.

B.2.1.4 Установка программы администратора безопасности

Установка выполняется штатными средствами ОС, например, для Astra Linux:

```
$ sudo dpkg -i alo_secureadmin_1.1.0.202_al1.6_x64.deb
```

Программа Aladdin SecureAdmin устанавливается в директорию /opt/Aladdin/SecureAdmin/. Программа взаимодействует с Aladdin LiveToken с помощью APDU-команд и SCSI-команд. SCSI-команды используются для записи образов загрузчика и LiveOS. Linux предоставляет доступ к SCSI интерфейсу только суперпользователю (root), поэтому для выполнения сценариев записи образов программу необходимо запускать с повышенными привилегиями.

B.2.1.5 Добавление файла info.plist на рабочее место администратора безопасности

Для корректной работы ПО SecureAdmin на рабочем месте администратора безопасности, необходимо выполнить следующие действия:

Для штатного функционирования Aladdin LiveToken на СВТ администратор безопасности должен добавить Aladdin LiveToken в Info.plist системы. Для добавления Aladdin LiveToken в Info.plist системы требуется выполнить следующие шаги:

1. Файл plistconf устанавливается в директорию /opt/Aladdin/SecureAdmin/ во время установки программы SecureAdmin.

2. Запустите командную оболочку Astra Linux (терминал Fly): главное меню ОС Astra Linux – утилиты – терминал Fly и прописать в терминале следующие команды.

```
chmod +x ./plistconf

sudo ./plistconf

sudo service pcscd restart
```

B.2.2 Установка Aladdin SecureAdmin в РЕД ОС 7.3 "Муром"

Для работы программного обеспечения SecureAdmin нужно установить пакет (службу) `pcscd` в операционной системе. Служба `pcscd` входит в состав других пакетов, например, в состав пакета `pcsc-lite-acsccid.x86_64` для установки которого необходимо ввести следующую команду:

```
sudo dnf install pcsc-lite-acsccid.x86_64
```

где `sudo` – команда выполнения с правами суперпользователя, `dnf` – команда управления пакетами из репозитория ОС, `install` – команда установки выбранного пакета.

После установки пакета `pcsc-lite`, можно начать установку программного обеспечения SecureAdmin. Для этого необходимо ввести следующую команду:

```
sudo rpm –ivh <название RPM-пакета>
```

Программное обеспечение SecureAdmin готово к работе.

B.3 Установка программ из состава Aladdin LiveOffice на СВТ под управление ОС семейства Windows

Установка в операционной среде Windows выполняется в штатном режиме путем запуска установочного msi-пакета. По умолчанию программа устанавливается в папку C:\Program Files\Aladdin\SecureAdmin, данные программы (база данных) хранятся в папке <System_Disk_Name>:\Users\<User_Name>\Aladdin\SecureAdmin. После установки программа Aladdin SecureAdmin готова к работе.

Приложение Г.Настройка загрузки с USB-накопителя

Г.1 Вход в BIOS/UEFI/SETUP

> *До начала подготовки к работе с Aladdin LiveOffice убедитесь, что в Вашей домашней операционной системе отключено шифрование дисков. Например, в Windows 10 должно быть отключено средство BitLocker Drive Encryption*
> *(Пуск -> Панель управления -> Все элементы панели управления -> Шифрование диска Bitlocker).*

Г.1.1 Вход в UEFI из операционной системы Windows

> *Предложенные варианты работают не на всех аппаратных платформах. Необходимым условием является использование современной системной (материнской) платы с интерфейсом UEFI.*

Г.1.1.1 ОС Windows 8 и 8.1

1. Зажмите клавишу <**Shift**> и в меню "Пуск" или на контрольной панели справа выберите пункт **Перезагрузка**.

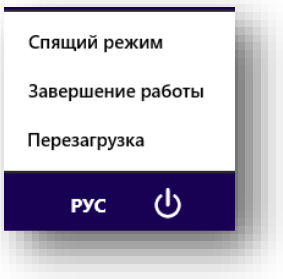

Рисунок 43 — Запуск меню Диагностика

2. В открывшейся экранной форме выберите **Диагностика,** а затем **Дополнительные параметры** или **Поиск и устранение неисправностей**:

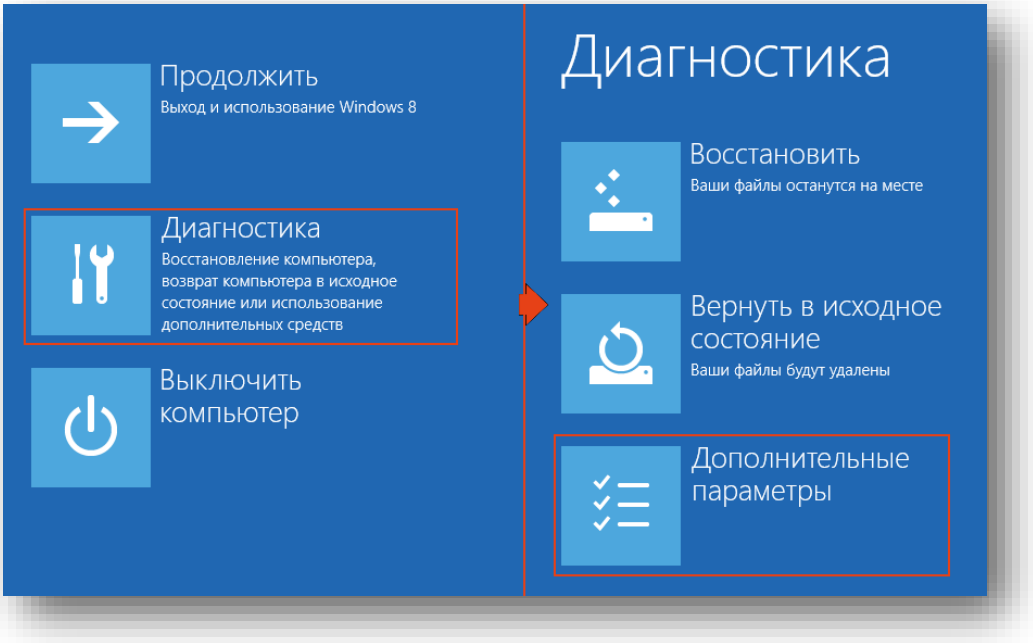

*Рисунок 44 — Вход в меню **Дополнительные параметры***

3. В экранной форме **Дополнительные параметры** выберите пункт **Параметры встроенного ПО**. В случае, если в экранной форме отсутствует указанный пункты, выберите **Выключить компьютер** и воспользуйтесь инструкцией в п.Г.1.3, [с. 74].

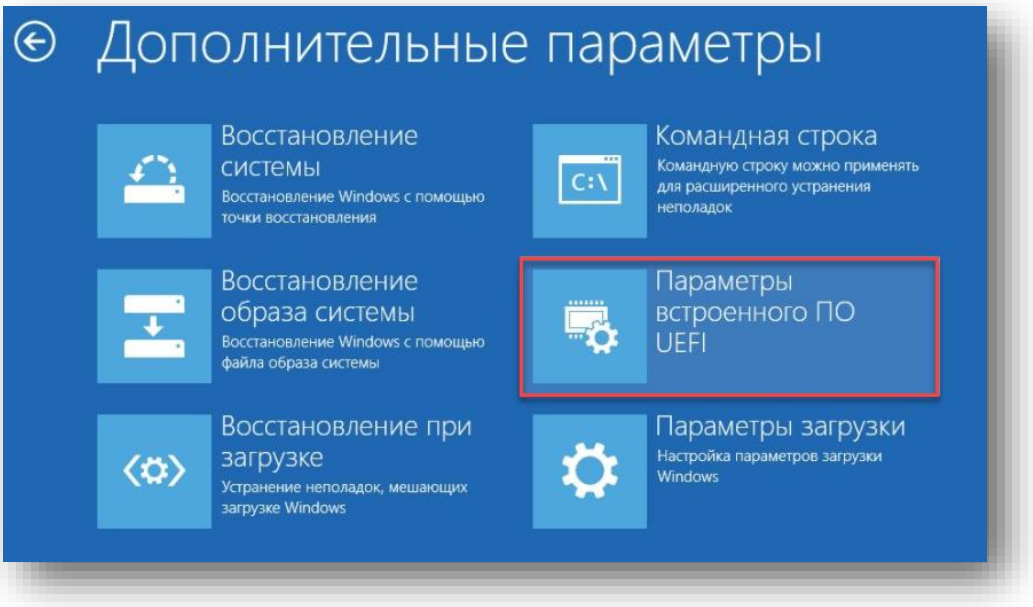

Рисунок 45 — Вход в UEFI

Г.1.1.2 ОС Windows 10

Выполните действия, указанные в п. Г.1.1.1 или воспользуйтесь инструкцией ниже.

1. Войдите в меню параметры:

- В меню "Пуск" выберите пункт "Параметры".

либо

- В строке поиска введите "Параметры".

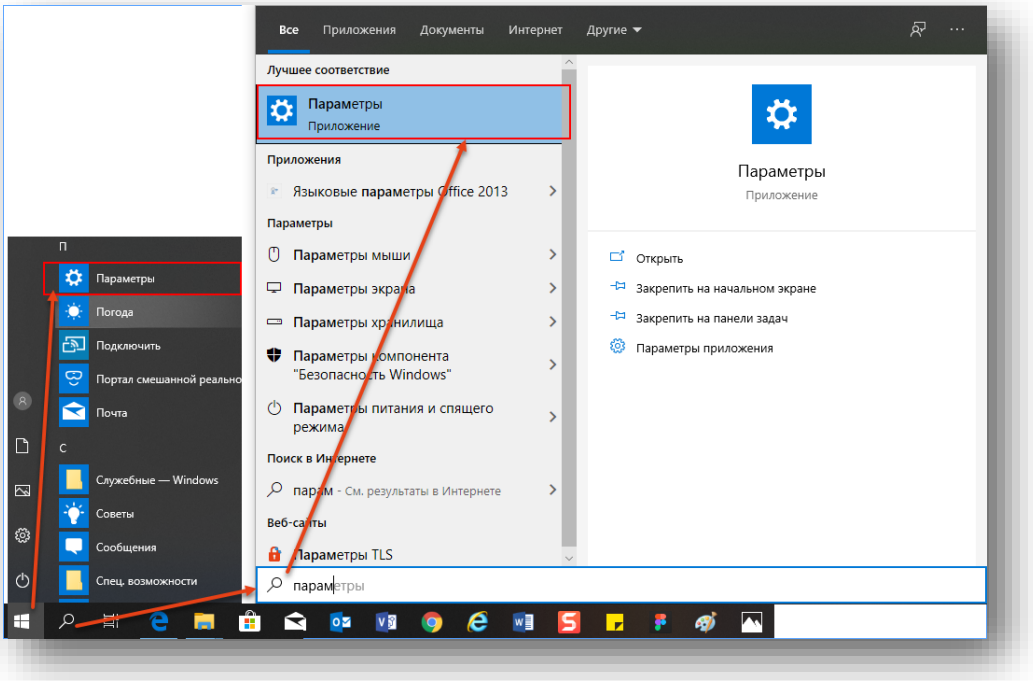

*Рисунок 46 — Запуск приложения **Параметры***

2. В окне **Параметры Windows,** приведённом на рисунке 47 выберите **Обновление и безопасность**.

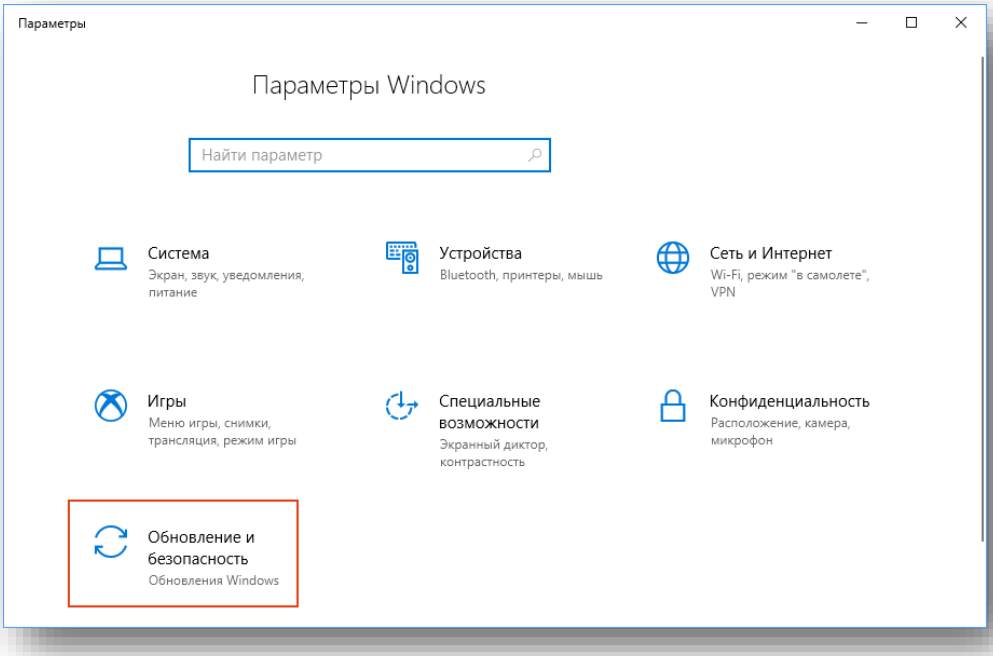

*Рисунок 47 — Меню **Обновление и безопасность***

3. В **окне Параметры Windows,** приведённом на рисунке 48 выберите вкладку **Восстановление** и в блоке **Особые варианты загрузки** кнопку <**Перезагрузить сейчас**>.

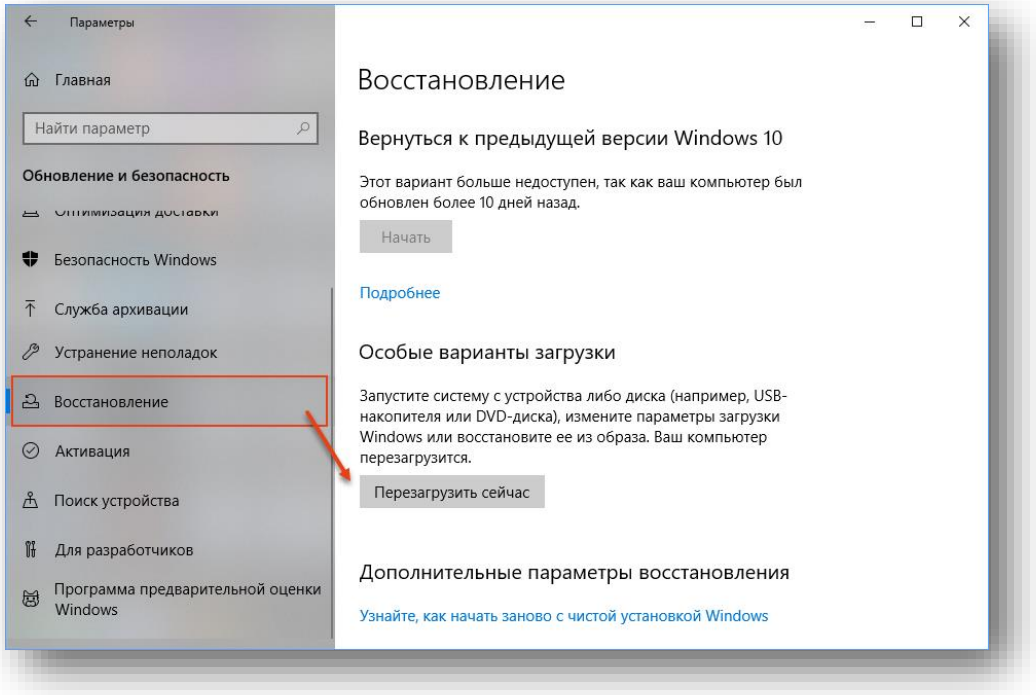

*Рисунок 48 — Пункт меню **Восстановление***

4. В открывшейся экранной форме выберите **Диагностика**, а затем **Дополнительные параметры**.

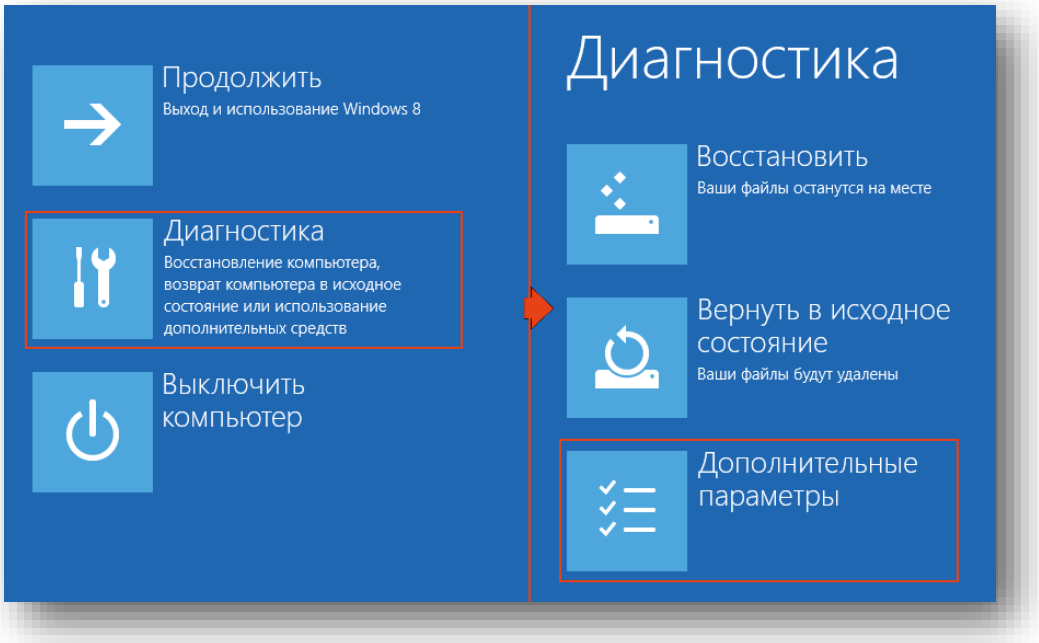

*Рисунок 49 — Вход в меню **Дополнительные параметры***

5. В экранной форме **Дополнительные параметры** выберите пункт **Параметры встроенного ПО.** В случае, если в экранной форме отсутствуют указанные пункты, выберите **Выключить компьютер** и воспользуйтесь инструкцией в п.Г.1.3, [с. 74].

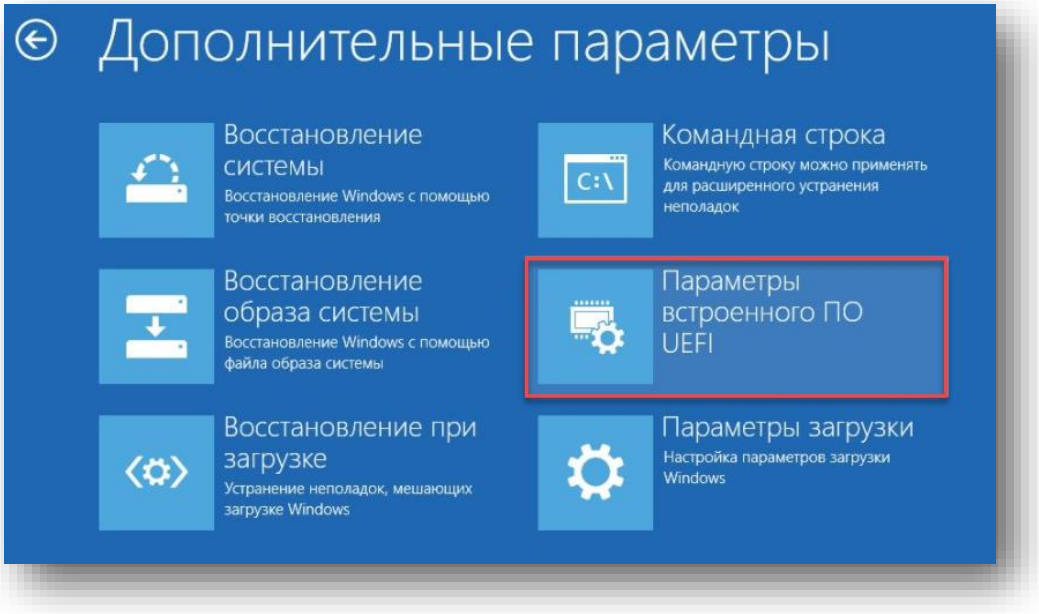

Рисунок 50 — Вход в UEFI

Г.1.1.3 Вход в UEFI с помощью командной строки ОС Windows

Вход в UEFI также возможен с помощью командной строки Windows.

1. Одновременно нажмите клавиши <**Win**> + <**X**> (+ <**X**>).
2. В открывшемся меню выберите Windows PowerShell (Администратор).
3. Введите `shutdown /fw /r`
4. В случае, если встроенное ПО вашего ПК не поддерживает загрузку из ОС (в командной оболочке отображается надпись "Загрузка в пользовательский интерфейс встроенного ПО не поддерживается встроенным ПО этой системы" – перейдите к п.Г.1.3, [с. 74].

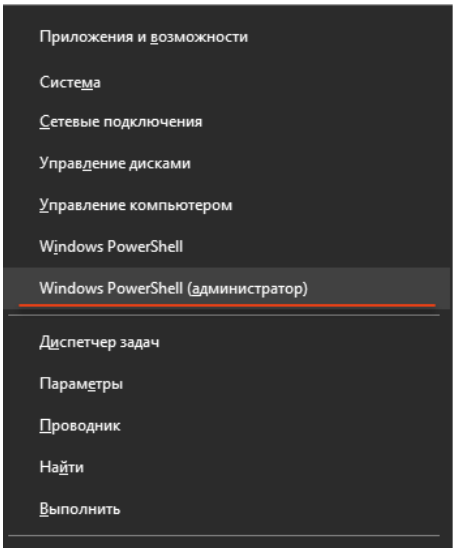

Рисунок 51 — Меню Windows ЦМП

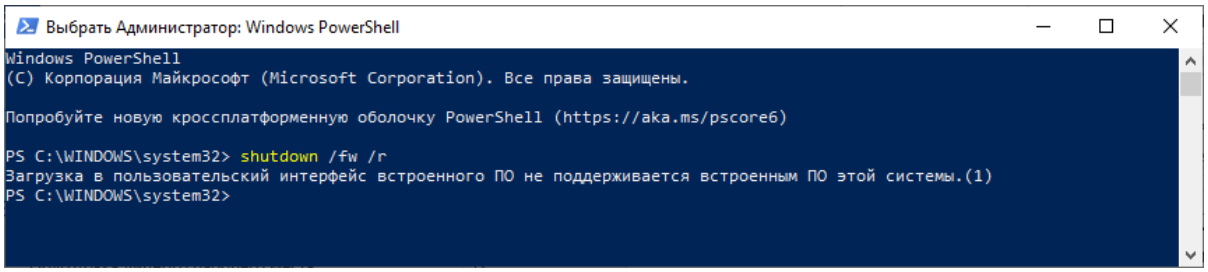

Рисунок 52 — Windows PowerShell

Г.1.2 Вход в BIOS/UEFI из операционной системы Linux

> *Предложенный вариант работает не на всех операционных системах семейства Linux.*

Для запуска firmware:

1. Запустите Терминал (консоль).
2. Воспользуйтесь командой:

```
sudo systemctl reboot --firmware-setup
```

Г.1.3 Вход в BIOS/UEFI с помощью горячих клавиш

BIOS/UEFI/Setup могут быть запущены до загрузки операционной системы с помощью нажатия "горячих клавиш". Клавиши для нажатия заранее определяются производителем ПК или ноутбука (при установке BIOS/UEFI).

Информация о конкретном сочетании клавиш обычно выводится на экран ПК или ноутбука при его загрузке. В этом случае, для запуска BIOS/UEFI/Setup:

1. Перезагрузите ПК или ноутбук.
2. Дождитесь появления изображения на мониторе.
3. Ознакомьтесь с выводимой на экран информацией.
4. Нажмите несколько раз на необходимую клавишу или сочетание клавиш.
5. Дождитесь загрузки BIOS/UEFI.

Примеры надписей на экране:

- Press <F8> (любую другую кнопку) to start SETUP.
- Press <F2> to run BIOS/UEFI.
- Press <F2> or <DEL> to enter UEFI BIOS settings.
- Press <F1> to run UEFI-boot menu.

В случае, если информация о конкретном сочетании клавиш не выводится на экран ПК или ноутбука при его загрузке – для запуска BIOS/UEFI/Setup воспользуйтесь клавишами, указанными в таблице 20).

6. Перезагрузите ПК или ноутбук.
7. Нажмите на указанные клавиши или сочетания клавиш до загрузки логотипа производителя материнской платы компьютера/ноутбука.
8. Нажмите несколько раз на указанные клавиши или сочетания клавиш после загрузки логотипа производителя материнской платы компьютера/ноутбука.
9. Дождитесь загрузки BIOS/UEFI.
10. В случае, если BIOS/UEFI не будет загружен, повторите, используя альтернативные клавиши.

Таблица 20 – Горячие клавши для запуска BIOS/UEFI

Производитель материнской платы компьютера/ноутбука	Горячая клавиша для запуска BIOS/UEFI	Примечание
Abit	DEL	После появления сообщения PRESS DEL TO ENTER SETUP
Acer (Aspire, eMachines , Veriton, Extensa, Ferrari, TravelMate)	DEL или F1	После нажатия на кнопку "Питание" и после загрузки экрана с логотипом Acer.
Acer Aspire, Emachines, Timeline	F2	После нажатия на кнопку "Питание" на корпусе ПК или ноутбука.
Acer Emachines	Tab или Esc, или DEL	
Acer (старые модели ПК)	F1 или Ctrl+Alt+Esc	
ASUS	DEL, F2, INS Ctrl+Alt+Delete	Сразу после нажатия на кнопку "Питание" на корпусе ПК.
ASUS (старые модели ПК)	F9, F10	
AMI (American Megatrends AMIBIOS, AMI BIOS)	DEL	После загрузки экрана с логотипом American Megatrends
AMI (American Megatrends AMIBIOS, AMI BIOS) – (старые модели ПК)	F1 или F2	После загрузки экрана с логотипом American Megatrends
ASRock	DEL или F2	Сразу после нажатия на кнопку "Питание" на корпусе ПК.
Award BIOS (AwardBIOS)	DEL	
Award BIOS (AwardBIOS) – старые модели ПК	Ctrl+Alt+Esc	
BIOSTAR	DEL	После загрузки экрана с логотипом
Compaq (Presario, Prolinea, Deskpro, Systempro, Portable)	F10	
Chaintech	DEL	
DELl (XPS, Dimension, Inspiron, Latitude. OptiPlex, Precision, Vostro)	F2	иногда F1 сразу после загрузки экрана Dell Повторять до загрузки UEFI или появления в одном из углов надписи loading
ECS (Elitegroup)	DEL или F1	
EVGA	DEL	Сразу после нажатия на кнопку "Питание" на корпусе ПК.
Fujitsu (LifeBook, Esprimo, Amilo, Tablet, DeskPower)	F2	После загрузки экрана с логотипом FuJitsu
Foxconn	DEL	
GIGABYTE	DEL	
Hewlett-Parkard (HP Pavilion, TouchSmart, Vectra, OmniBook, Tablet)	F1	
Hewlett-Parkard (HP Alternative)	F2 или Esc	
Hewlett-Parkard (HP) Tablet PC:	F10 или F12	
IBM ThinkPad using Phoenix BIOS	Ctrl+Alt+F11	
IBM (Старые модели)	F2	
Intel	DEL или F2	
JetWay	DEL	
Lenovo (ThinkPad, IdeaPad, 3000 Series, ThinkCentre, ThinkStation)	F1 или F2 FN + F1	Для Lenovo ThinkPad, ThinkCentre, ThinkStation дождитесь появления логотипа Lenovo
MSI (Micro-Star)	DEL или F2	После загрузки экрана с логотипом, но до загрузки

Производитель материнской платы компьютера/ноутбука	Горячая клавиша для запуска BIOS/UEFI	Примечание
	В очень редких случаях Tab, затем DEL	операционной системы. Предпочтителен вход в BIOS из ОС
NEC (PowerMate, Versa, W-Series)	F2	
Packard Bell (8900 Series, 9000 Series, Pulsar, Platinum, EasyNote, imedia, iextreme)	DEL или F1, F2	
Sapphire	DEL	
Sharp	F2	
Samsung	F2	
Sony (VAIO, PCG-Series, VGN-Series)	F1, F2 или F3	
XFX	Del или F4	

В случае, если на стартовом экране Вашего компьютера отсутствует подсказка и он отсутствует в списке:

1. Уточните название вашей материнской платы в настройках Вашего ПК.
2. Уточните версию BIOS/UEFI.
3. Воспользуйтесь материалами таблицы или поиском в сети "Интернет".

Для этого в ОС Windows 7, 8, 8.1, 10:

1. Нажмите на клавиатуре <**Win**> + <**R**> (+ <**R**>).
2. В открывшееся окно введите msinfo32 (рисунок 53) и нажмите **OK**.
3. Просмотрите информацию о версии BIOS/UEFI и изготовителе основной (материнской) платы (рисунок 54).
4. При необходимости получите информацию о кнопке запуска BIOS/UEFI в инструкции производителя основной (материнской) платы.

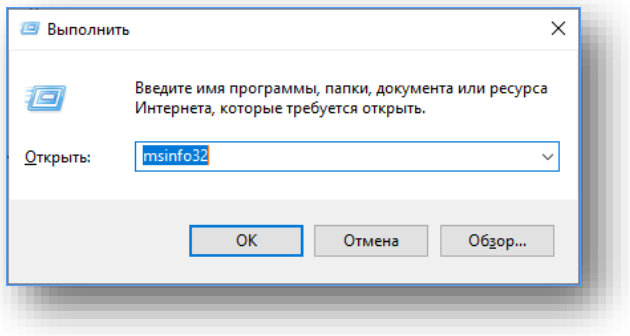

Рисунок 53 — Запуск программы msinfo32

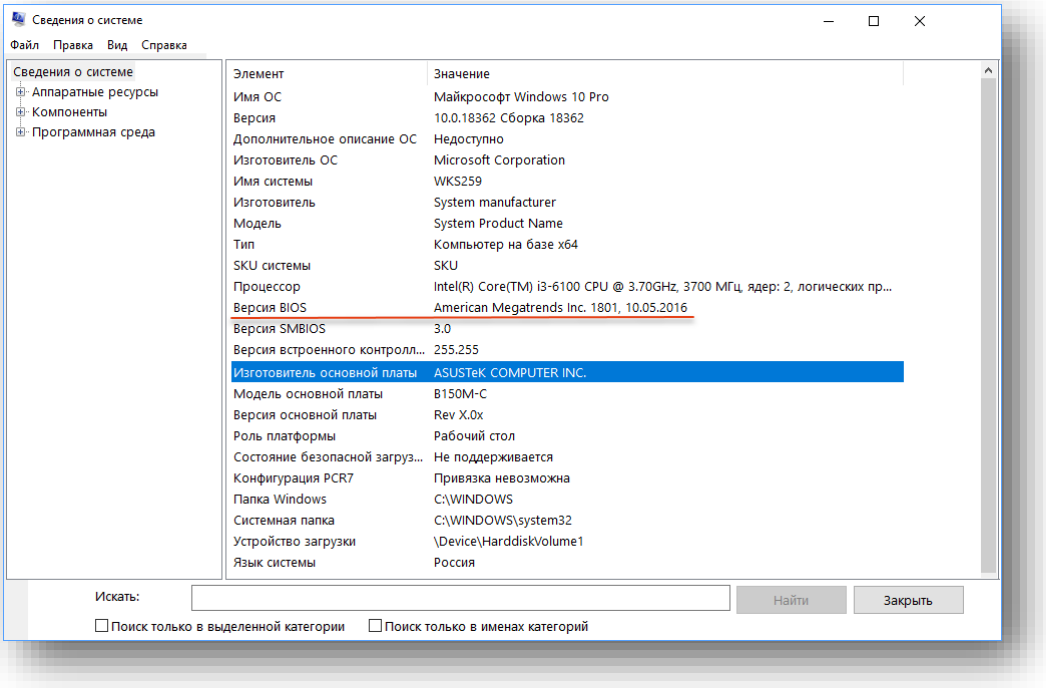

Рисунок 54 — Версия BIOS/UEFI в программе msinfo32

Г.2 Настройка BIOS

Определите производителя материнской платы вашего компьютера (ноутбука).

1. В основном меню найдите наименование производителя.
2. Установите в BIOS настройки, указанные в соответствующем подразделе настоящего руководства.
3. В случае отсутствия необходимой инструкции ознакомьтесь с примерами и выполните аналогичные настройки.
4. В случае, если интерфейс BIOS отличается от представленного в примерах, найдите указанные в примерах параметры, в интерфейсе Вашего BIOS и приведите их в соответствие настоящему руководству. Перезагрузите компьютер.

   4.1. В случае, если всё настроено верно – Ваш компьютер начнёт загрузку с носителя информации из комплекта Aladdin LiveOffice.

   4.2. В случае, если загрузка с носителя информации после перезагрузки ПК (ноутбука) не осуществляется:

      4.2.1. Убедитесь, что применены все указанные настройки.

      4.2.2. Убедитесь, что Aladdin Boot находится на первом месте в списке **Boot Order** или **Boot Priority.**

      4.2.3. Сделайте фотографии Вашего BIOS и направьте в техническую поддержку АО "Аладдин Р.Д." (см. раздел "Техническая поддержка", [с. 91]).

Г.2.1 AmiBIOS (American Megatrends, Inc.)

Пример отображения AmiBIOS представлен на рисунке ниже.

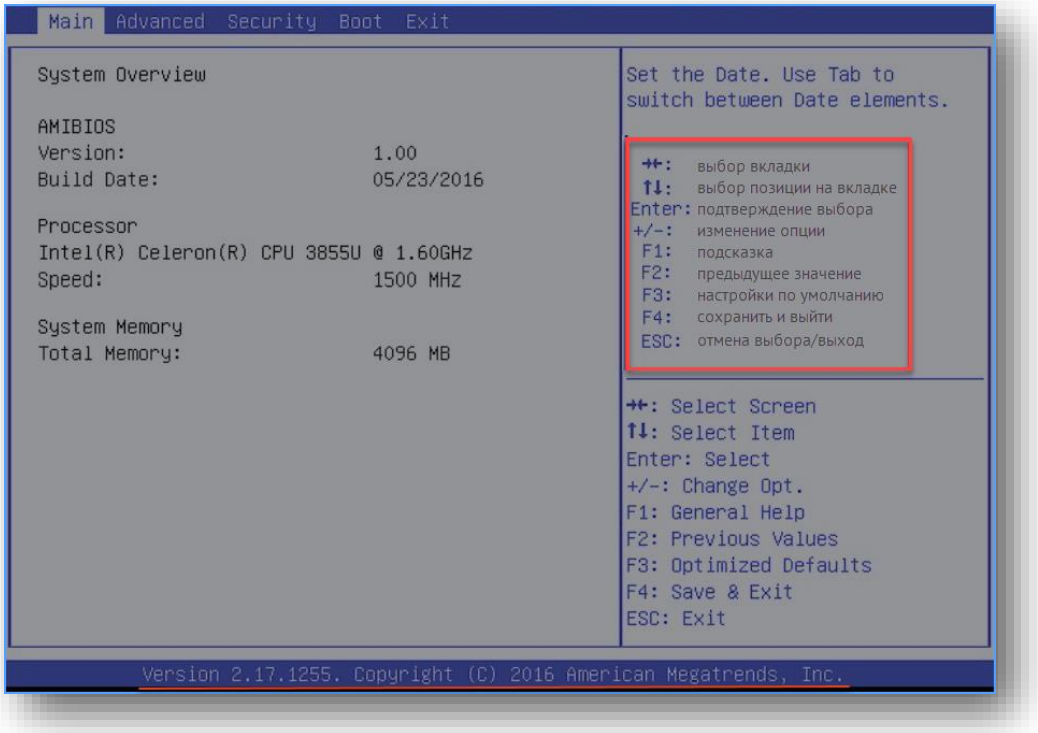

Рисунок 55 — Основное окно AmiBIOS (American Megatrends, Inc. BIOS)

В AMIBIOS (AmiBIOS), необходимо установить значение параметров в соответствии с указанным на рисунках 56 и 57.

Для установки параметров в BIOS воспользуйтесь инструкцией в правой части экрана (красная рамка):

1. Перемещайтесь между вкладками с помощью клавиш вправо и влево (→ и ←), расположенных в правой части клавиатуры.
2. Выбирайте конкретные записи с помощью стрелок вверх и вниз (↑ и ↓) расположенных в правой части клавиатуры.
3. Клавиша <**Enter**> позволяет выбрать конкретный пункт меню для его изменения. Нажатие на клавишу позволяет выбрать одно из предустановленных значений.
4. Клавиша <**Esc**> позволяет отменить изменения и выйти из BIOS.
5. Клавиша <**F4**> позволяет сохранить изменения и выйти из BIOS.

Подчёркнутые (указанные) параметры могут также располагаться на других вкладках (зависит от версии BIOS).

1. Параметр **Boot from USB-device** (загрузка с USB-устройства), должен находиться в положении **Enabled** (включено).
2. Boot **Device Priority** (приоритет загрузки с устройств) на позиции #1 должен иметь **Aladdin Boot**.
3. **Boot Mode Select** должен иметь значение **Legacy**.
4. **Secure Boot Control** должен иметь значение **Disabled** (отключен).

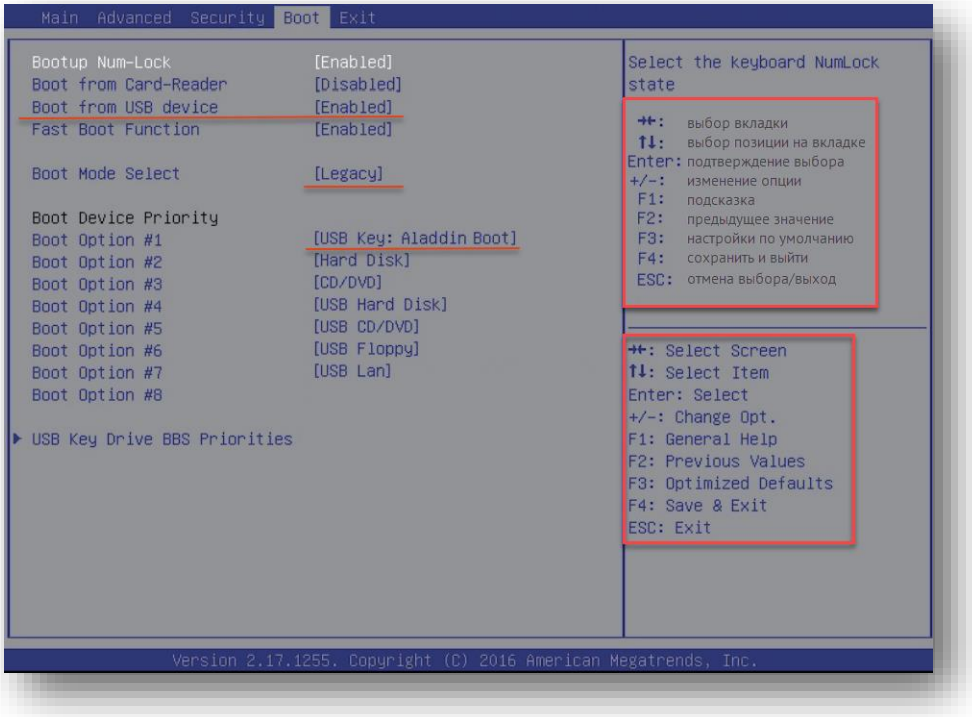

Рисунок 56 — Настройка Boot для AmiBIOS (American Megatrends, Inc. BIOS)

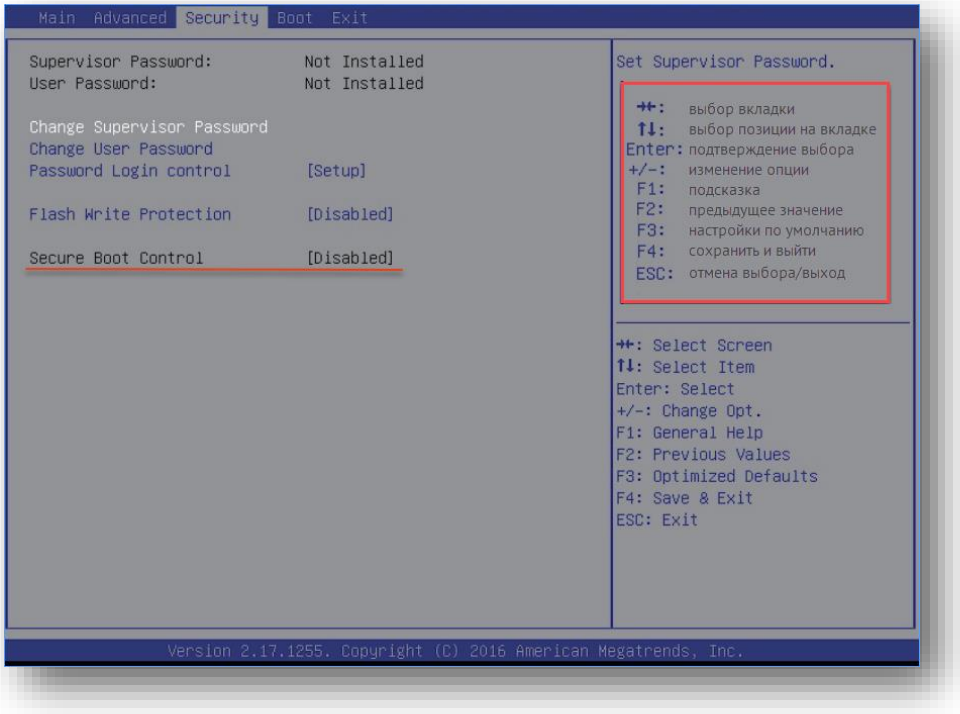

Рисунок 57 — Настройка SecureBoot для AmiBIOS (American Megatrends, Inc. BIOS)

Г.2.2 AwardBIOS (Award Software)

Пример отображения AwardBIOS (CMOS) представлен на рисунке ниже.

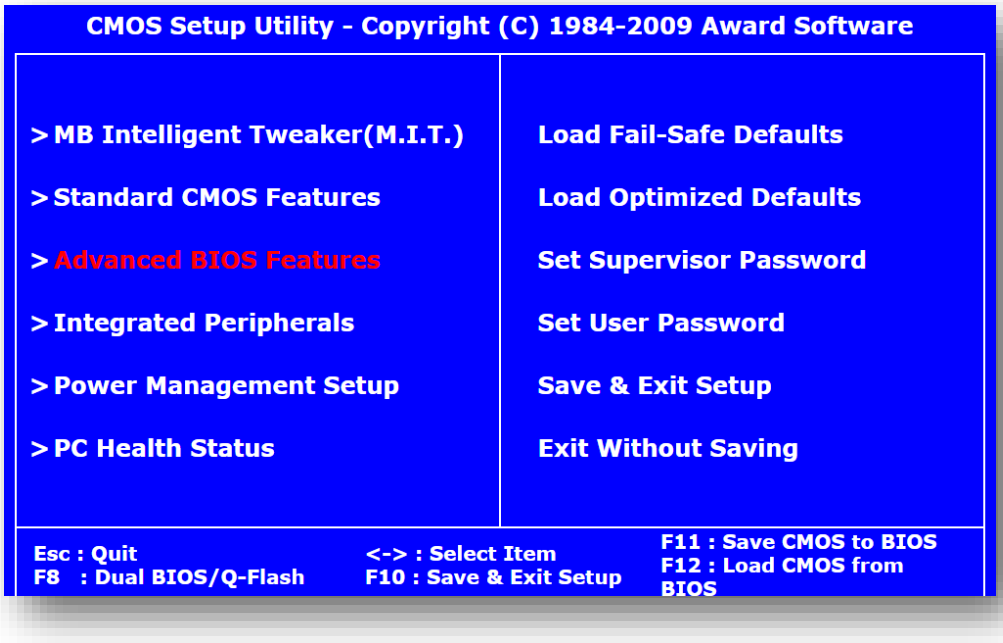

Рисунок 58 — Основное окно AwardBIOS (CMOS)

Перечень горячих клавиш для работы с CMOS представлен в таблице 21.

Таблица 21 – Горячие клавши для работы с CMOS

Горячая клавиша	Назначение
↑ и ↓	Перемещение между вкладками в меню
→ и ←	Выбор пункта
+ и -	Изменение численного значения
<Esc>	Выход
F10	Сохранить и выйти

В AwardBIOS:

1. Выберите **Advanced BIOS Features**.
2. Выберите с помощью ↑ и ↓ и клавиши <**Enter**> **Hard Disk Boot Priority**.
3. Установите в качестве первого устройства **Aladdin Boot**.
4. Нажмите <**ESC**>.
5. Установите в качестве **First Boot Device** – USB: HDD.
6. Нажмите <**ESC**>.
7. Выберите **Integrated peripherals**.
8. Установите:
   - **USB-controllers** – **Enabled**;
   - **USB Legacy Function** – **Enabled**;
   - **USB Storage Function** – **Enabled**.

Г.3 Настройка UEFI

Г.3.1 BIOSTAR UEFI

Пример отображения BIOStaR UEFI представлен на рисунке ниже.

Рисунок 59 — Основное окно BIOStar UEFI

В BIOStar, необходимо установить значение параметров в соответствии с указанным на рисунках 60–63.

Для установки параметров в BIOS воспользуйтесь инструкцией в правой части экрана (красная рамка):

1. Перемещайтесь между вкладками с помощью клавиш вправо и влево (→ и ←), расположенных в правой части клавиатуры.
2. Выбирайте конкретные записи с помощью стрелок вверх и вниз (↑ и ↓) расположенных в правой части клавиатуры или с помощью одиночного щелчка левой кнопки мыши.
3. Клавиша <**Enter**> или двойной щелчок мышью позволяют выбрать конкретный пункт меню для его изменения. Нажатие на клавишу позволяет выбрать одно из предустановленных значений.
4. Клавиша <**F3**> позволяет сбросить параметры до «оптимальных» (предустановленных производителем).
5. Клавиша <**Esc**> позволяет отменить изменения и выйти из BIOS.
6. Клавиша <**F10**> позволяет сохранить изменения и выйти из BIOS.

Подчёркнутые (указанные) параметры могут также располагаться на других вкладках (зависит от версии BIOS. На вкладке **Advanced** параметры USB могут быть сгруппированы в пункте **USB-configuration**.

1. Параметр **Legacy USB Support** (загрузка с USB-устройства), должен находиться в положении **Enabled** (включено).
2. Параметр **USB Mass Storage Driver Support**, должен находиться в положении **Enabled** (включено).
3. На вкладке **Security** в меню **Secure Boot** значение параметра **Secure Boot** должно быть **Disabled** (рисунки 61–62).
4. На вкладке **Boot** в меню **Boot Option Filter** указан параметр **UEFI and Legacy**.
5. На вкладке **Boot** в пункте **Boot Option Priority** переместите **Aladdin Boot** на позицию #1.
6. Сохраните настройки и перезагрузите компьютер (в меню **Save & Exit** выберите **Save Changes and Reset**).

Рисунок 60 — Основное окно BIOStar. Включение поддержки USB

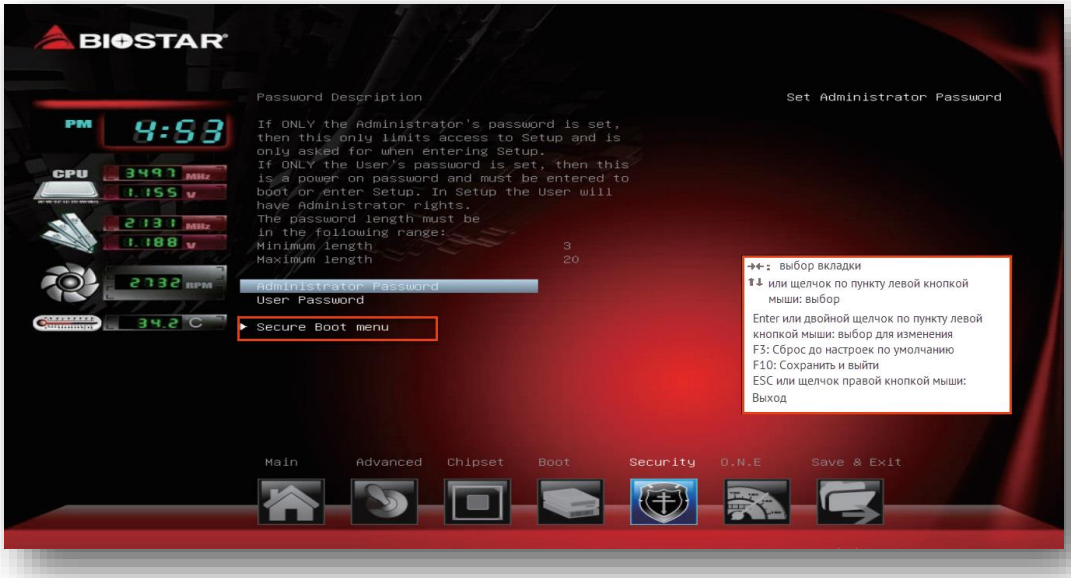

Рисунок 61 — Вызов Secure Boot menu

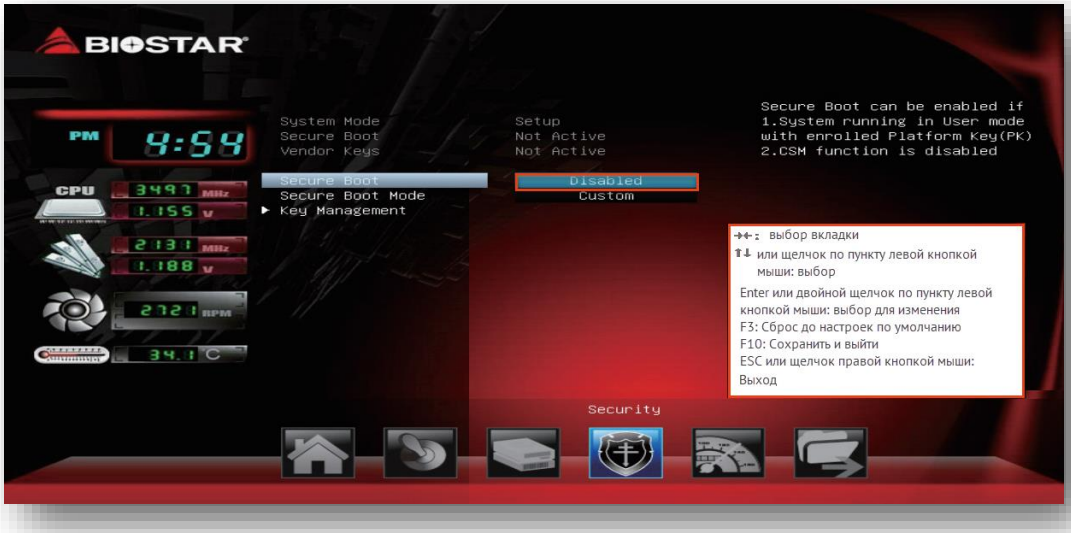

Рисунок 62 — Настройка SecureBoot (отключение)

Рисунок 63 — Настройка приоритета загрузки ОС

Рисунок 64 — Сохранение настроек и выход (Save Changes and Reset)

Г.3.2 ASUS UEFI

ASUS UEFI после загрузки работает в упрощённом режиме. И поддерживает работу как с помощью клавиатуры (клавиши →, ←, ↑ и ↓, <**Enter**>), так и с помощью "компьютерной мыши".

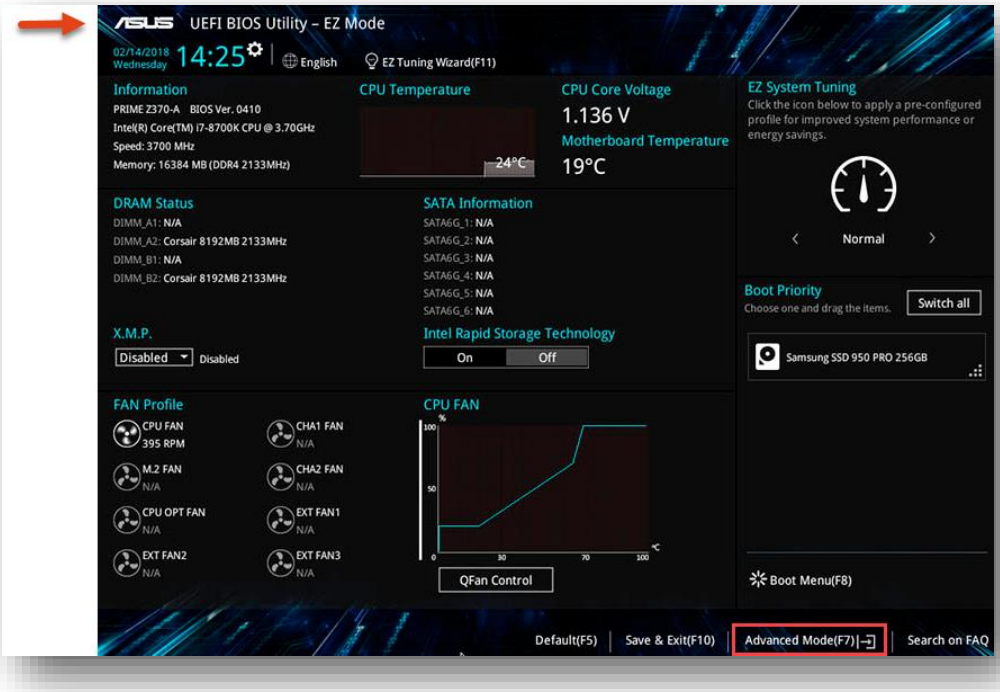

Рисунок 65 — Пример отображения Asus UEFI BIOS Utility (Ez mode)

Для настройки перейдите в **Advanced Mode** с помощью клавиши <**F7**> (не зависит от версии UEFI).

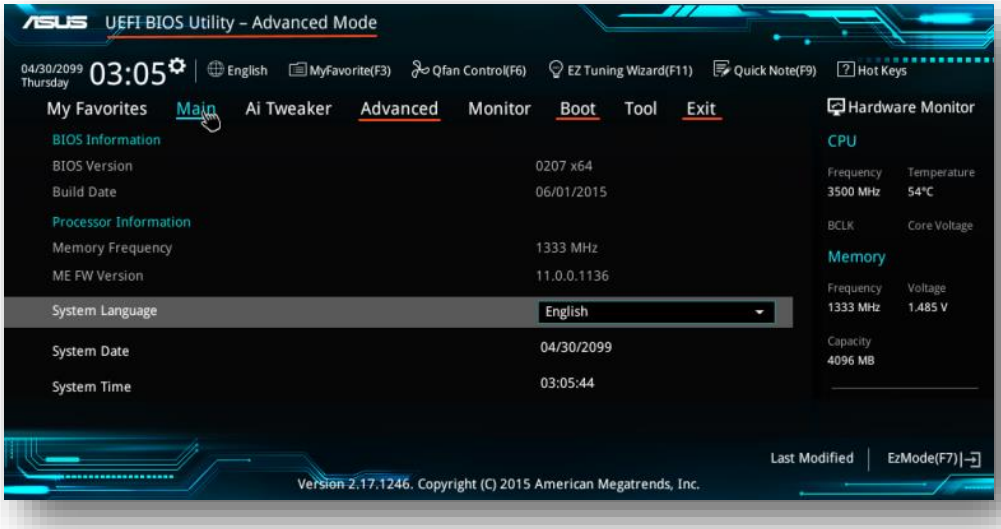

Рисунок 66 — Пример отображения Asus UEFI BIOS Utility (Advanced mode)

В **UEFI BIOS Utility** выберите следующие параметры работы:

1. На вкладке **Advanced**:
   - в пункте **USB-configuration** выберите **Legacy USB Support** и из выпадающего списка установите **Enabled**.
2. На вкладке **Boot**:
   - в пункте **SecureBoot** выберите значение **Other OS**;
   - в пункте **Boot Option Priorities** установите в позицию #1 (верхнюю) **Aladdin Boot.**
3. В пункте **CSM** (**Compatibility Support Mode**) при его наличии:
   - Для подпункта **Launch CSM** установите значение [**Enabled**].
   - Для подпункта **Boot device Control** установите значение [**UEFI and Legacy OPROM**].
   - Для подпункта **Boot from storage devices** установите [**Legacy only**].
4. На вкладке **Exit** выберите **Save Changes & Reset**. Подтвердите операцию во всплывающем окне (**Yes** или **OK**)

Г.3.3 ASRock UEFI

ASRock UEFI после загрузки работает в упрощённом режиме. И поддерживает работу как с помощью клавиатуры (клавиши →, ←, ↑ и ↓, **<Enter>**), так и с помощью "компьютерной мыши".

Для настройки перейдите в **Advanced Mode** с помощью клавиши <**F6**> (не зависит от версии UEFI).

В **UEFI BIOS Utility** выберите следующие параметры работы:

1. На вкладке **Advanced**:
   - в пункте **USB-configuration** выберите **Legacy USB Support** и из выпадающего списка установите **Enabled**.
2. На вкладке **Boot**:
   - в пункте **Boot Option Priorities** установите в позицию #1 (верхнюю) **Aladdin Boot**;
   - в пункте **PCI ROM Priority** установите **Legacy ROM**;
   - в пункте **CSM** (**Compatibility Support Module**) выберите **Enabled** или **Other OS** (при наличии).
3. На вкладке **Security:**
   - в пункте **SecureBoot** выберите **Disabled** или **Other OS**.
4. На вкладке **Exit** выберите **Save Changes & Reset**. Подтвердите операцию во всплывающем окне (**Yes** или **OK**).

Г.4 Настройка Setup

Г.4.1 Dell Setup

Пример интерфейса ноутбуков Dell представлен на рисунке 67. Оранжевым цветом выделены вкладки интерфейса с настраиваемыми параметрами. Описание параметров приведено ниже.

Ноутбуки Dell поддерживают работу в Setup с помощью "компьютерной мыши" или контрольной панели.

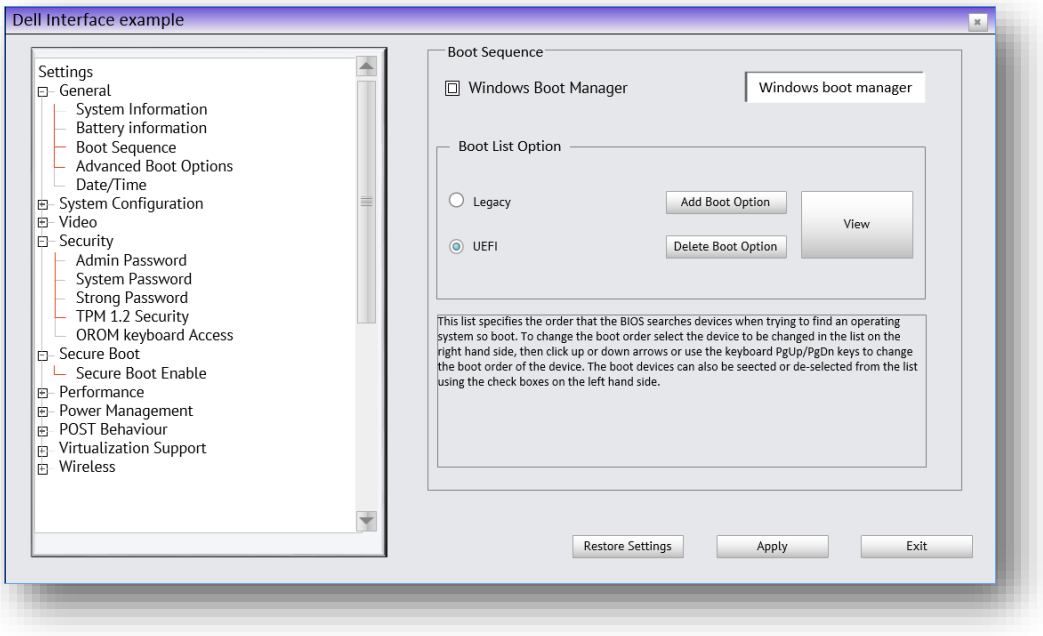

Рисунок 67 — Пример использования интерфейса Setup Dell

В меню **Setup** выберите следующие параметры работы ноутбука:

1. На вкладке **General**:
   - уберите галочку из чекбокса Windows Boot Manager (при её наличии);
   - в пункте **Boot Sequence** выберите **UEFI**;
   - в пункте **List Option** выберите **UEFI**.
2. На вкладке **Security**:
   - в пункте **TPM 1.2 Security** выберите параметр **Disabled** (переключите радиокнопку) или полностью отключите TPM 1.2 (снимите галочку);
3. На вкладке **Security Boot** выберите параметр (переключите радиокнопку) **Security boot disabled**.
4. На вкладке **General**: в пункте **Advance Boot Options** выберите параметр **Enable Legacy Options ROM** (установите галочку).
5. В правом нижнем углу экрана нажмите на кнопку **Apply**.
6. Нажмите **Exit**.

Запустите **One-time boot menu**. Для этого:

7. Перезапустите ноутбук или дождитесь появления логотипа (надписи) Dell.
8. Нажимайте на клавишу <**F12**> до появления в верхнем правом углу жёлтой надписи "**Starting One-time boot menu**".
9. Выберите **Aladdin Boot**.

> *One-time boot menu осуществляет однократную загрузку с Aladdin LiveOffice – разовый запуск.*

Г.4.2 Lenovo Setup

Таблица 22 — Горячие клавиши для работы с Lenovo Setup

Горячая клавиша	Назначение
↑ и ↓	Перемещение между вкладками в меню
→ и ←	Вызов вкладки.
+ и -	Изменение численного значения
<Enter>	Выбор подменю
<Esc>	Выход
F9	Сброс до настроек «по умолчанию»
F10	Сохранить и выйти

Некоторые вкладки или пункты из описания ниже могут отсутствовать в разных версиях Setup. Пропустите их. У IdeaPad Gaming на экране входа необходимо выбрать "More Settings".

В Setup menu выберите следующие параметры работы ноутбука:

1. На вкладке **Device** выберите **USB Setup**:
   - установите значение параметра **USB Port Access** – **Enabled**;
   - проверьте, что все необходимые порты (USB 1–8) включены (**Enabled**);
   - установите значение параметра **USB Support – Enabled;**
   - установите значение **USB Legacy Support – Enabled.**
2. На вкладке **Security**:
   - в пункте **Secure Boot** выберите параметр **Disabled**;
   - в пункте **Device Guard** выберите параметр **Disabled**.
3. На вкладке **Configuration**:
   - в пункте **Secure Boot** выберите параметр **Enabled**.
4. На вкладке **Startup**
   - выберите **Primary Boot Sequence** и переместите на позицию №1 **Aladdin Boot**;

*В некоторых версиях Setup перечень устройств выводится на вкладке **Boot** в пункте **Boot**, вне пунктов или с заголовком **Boot Priority Order** (**Boot Device List**). Подсказка о кнопках для перемещения пунктов в порядке загрузки находится в правой части экрана.*

   - в пункте **CSM** установите **Enabled** или **Yes**;
   - в пункте **Boot Priority** выберите **Legacy First**;
   - в пункте **Boot Mode** выберите **Auto** или **Legacy support.**
5. На вкладке **Boot** (опционально):
   - в пункте **Boot Mode** выберите параметр **Legacy Support**;
   - в пункте **USB Boot** выберите параметр **Enabled**.
6. На вкладке **Exit** (или **Restart**) для **OS Optimized Defaults** установите значение **Disabled** или **Other OS**.
7. На вкладке **Exit** (или Restart) выберите **Save Changes and Exit** и подтвердите.
8. Нажмите **Exit**.

Приложение Д.Порядок вывода изделия из эксплуатации

Д.1 Общие сведения о порядке вывода Aladdin LiveOffice из эксплуатации

Процедуры вывода из эксплуатации Aladdin LiveOffice предусматривают:

- Вывод из эксплуатации СЗИ "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice" на АРМ.
- Вывод из эксплуатации отдельных электронных носителей или запрет их использования на отдельных СВТ.

Вывод из эксплуатации отдельных электронных носителей возможен в двух вариантах:

- временный (носитель может быть использован повторно);
- постоянный (физическое уничтожение носителя).

Процедуры вывода изделия из эксплуатации учитывают наличие нескольких версий изделия, а также возможность наличия на электронном носителе дополнительных программ и программных средств, загруженных в виде апплетов.

Если с использованием носителя переносилась или обрабатывалась информация, содержащая персональные данные или относящаяся к ГИС – носитель не может быть передан другому пользователю и в обязательном порядке выполняются пункты, описывающие физическое уничтожение носителей. Процедуры утилизации носителей, на которых хранилась другая информация ограниченного доступа (информация, представляющая собой коммерческую тайну и др.), устанавливаются владельцем информации.

Д.2 Порядок вывода Aladdin LiveOffice из эксплуатации

Д.2.1 Общий порядок вывода изделия из эксплуатации

Вывод из эксплуатации "Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice" выполняется в следующем порядке:

1. Архивирование (при необходимости) информации, хранящейся на съемных носителях, а также записей из журналов аудита Aladdin LiveOffice (выполняется экспорт журналов), в соответствии с настоящим руководством по эксплуатации.
2. Стирание данных, относящихся к программным СЗИ или СКЗИ, используемым совместно с Aladdin LiveOffice (например, ключевых контейнеров Криптотокен-2 ЭП). Стирание данных происходит в соответствии с инструкциями по эксплуатации вышеупомянутых СЗИ или СКЗИ.
3. Стирание (обезличивание) информации на электронных носителях Aladdin LiveOffice уполномоченным пользователем с ролью "администратор безопасности".
4. Стирание информации, сгенерированной в процессе эксплуатации Aladdin LiveOffice:
   - уничтожение (удаление) баз данных, расположенных в защищенных директориях;
   - уничтожение (удаление) ключевых контейнеров.
5. Удаление программных средств в ОС семейства Linux осуществляется с помощью команды `sudo rm <название пакета>` и с помощью раздела "**Программы и компоненты**" (*Панель управления → Все элементы панели управления → Программы и компоненты*) в ОС семейства Windows.
6. Физическое уничтожение носителей информации.
7. Документирование физического уничтожения носителей.

Д.2.2 Физическое уничтожение носителей информации

Физическое уничтожение носителя выполняется в случае вывода изделия из эксплуатации, и осуществляется в соответствии с внутренними организационно-распорядительными мерами организации, эксплуатирующей изделие, либо в соответствии с инструкцией, приведённой ниже:

1. Подготовьте комплект инструментов, необходимый для выполнения работ. Рекомендуемый состав комплекта:
   - плоскогубцы (комбинированные, исполнение 1, общей длиной 200 мм, с изолирующими рукоятками по ГОСТ Р 53925 [C1] или аналогичные) – 1 шт.;
   - плоскогубцы (комбинированные, исполнение 2, общей длиной 200 мм, с изолирующими рукоятками по ГОСТ Р 53925 [c1] или аналогичные) – 1 шт.;
   - кусачки (тип 1, общей длиной 200 мм, с изолирующими рукоятками, обозначение 7814-0406 по ГОСТ 28037 [c2] или аналогичные) – 1 шт.;
   - кусачки (тип 2, общей длиной 200 мм, с изолирующими рукоятками, обозначение 7814-0128 по ГОСТ 28037 [c2] или аналогичные) – 1 шт.;
   - отвертку (тип 2, исполнение 1, обозначение 7810-1044, 7810-1051 по ГОСТ 17199 [c3] или аналогичные) – 2 шт.;
   - комплект средств индивидуальной защиты рук (размер 6-10 по ГОСТ 12.4.252 [c4] или аналогичные) – не менее 1 пары каждого размера.
2. Выполните следующие операции:
   а) воспользуйтесь комплектом индивидуальной защиты рук;
   б) снимите с USB-носителя колпачок;
   в) закрепите изделие в губках тисков, поместив USB-разъем и часть корпуса внутрь;
   г) разрушьте корпус USB-носителя кусачками до появления печатной платы и электронных элементов, закрепленных на ней;
   д) извлеките карту памяти (microSD-карту) из разъема;
   е) разрушьте кусачками карту памяти (microSD-карту);
   ж) удалите отверткой с печатной платы электронные элементы;
   з) уничтожьте с помощью кусачек электронные элементы, удалённые с платы;
   и) закрепите изделие в губках тисков, поместив USB-разъем внутрь;
   к) плоскогубцами отделите печатную плату от USB-разъема;
   л) соберите и упакуйте все полученные части USB-носителя.
   м) утилизируйте остатки изделия.

Размер фрагментов (после уничтожения флеш-памяти, микроконтроллера общего назначения и смарт-карты) – не должен превышать 1 мм^3.

Утилизация электронных элементов (микросхем и т.п.) изделия должна осуществляться организациями, имеющими разрешение на данный вид деятельности. Не рекомендуется утилизировать изделие вместе с бытовыми отходами.

Д.2.3 Временный вывод из эксплуатации в случае истечения срока действия ключей

Ключевые наборы, генерируемые в программе главного администратора, имеют ограниченный срок действия. По истечению срока действия, рекомендуется временный вывод из эксплуатации электронных носителей, осуществляемый в следующем порядке:

1. Архивирование (при необходимости) информации, хранящейся на съемных носителях, а также информации хранящейся в журналах аудита Aladdin LiveOffice (экспорт журналов) в соответствии с настоящим руководством по эксплуатации.

2. Стирание данных, относящихся к программным СЗИ или СКЗИ, используемым совместно с Aladdin LiveOffice (например, ключевых контейнеров Криптотокен-2 ЭП). Стирание данных происходит в соответствии с инструкциями по эксплуатации вышеупомянутых СЗИ или СКЗИ.
3. Стирание (обезличивание) информации на электронных носителях Aladdin LiveOffice уполномоченным пользователем с ролью "администратор безопасности".
4. Удаление разрешений с локальных (изолированных) рабочих мест и из базы данных доступа (в случае, если носитель был обезличен с помощью другой базы данных доступа).
5. Архивирование ключевого контейнера с ключевым набором с истёкшим сроком действия.
6. Повторный ввод электронных носителей в эксплуатацию на основе ключевого набора с действующим сроком годности.

Временный вывод изделия из эксплуатации и передача его другому пользователю должны осуществляться в соответствии с внутренней организационно-распорядительной документацией эксплуатирующей организации.

Д.3 Порядок вывода носителей из эксплуатации

Д.3.1 Временный вывод из эксплуатации при передаче ССМНИ другому пользователю

В случае, если правила организации обеспечивают возможность передачи ССМНИ (электронного носителя) для эксплуатации между пользователями, осуществляется временный вывод ССМНИ из эксплуатации.

Порядок действий, выполняемый администратором при выводе из эксплуатации, предполагает следующие шаги:

1. Перенесите данные из журнала аудита ССМНИ в журнал аудита СВТ.
2. Экспортируйте журнал аудита СВТ.
3. Выполните обезличивание и повторную инициализацию носителя.
4. Зафиксируйте (если требуется) совершённые действия в документации.

Контакты, техническая поддержка

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания АО "Аладдин Р. Д.".

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40.

Факс: +7 (495) 646-08-82.

E-mail: aladdin@aladdin.ru (общий).

Web: www.aladdin.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

Техническая поддержка

Запросы на техническую поддержку оформляются преимущественно в виде заполненной формы через Web-сайт изготовителя (производителя) или по электронной почте, а также в устной форме посредством телефонной связи (при обращении по телефону и, если вопрос достаточно сложный, инженер технической поддержки вправе потребовать завести запрос через Web-сайт/эл.почту).

Адрес для обращений в техническую поддержку изготовителя (производителя):

https://alo.aladdin-rd.ru

Адрес электронной почты:

techsup@aladdin-rd.ru

Регистрация изменений

Версия	Изменения
1.0	Проведена актуализация документа для ALO версии MVP-2

Коротко о компании

Компания АО "Аладдин Р. Д." основана в апреле 1995 года и является российским разработчиком (вендором) средств защиты информации.

Компания является признанным экспертом и лидером российского рынка средств двухфакторной аутентификации пользователей, электронной подписи и защиты данных.

Основные направления

- Обеспечение безопасного доступа к информационным ресурсам предприятия, веб-порталам и облачным сервисам (строгая двух- и трёхфакторная аутентификация).
- Электронная подпись (ЭП с неизвлекаемым закрытым ключом, формируемая в защищённом чипе), PKI.
- Защита персональных данных, данных на дисках компьютеров, серверов, баз данных.
- Все основные продукты имеют необходимые сертификаты ФСТЭК, ФСБ и Министерства обороны (включая работу с гостайной до уровня секретности СС).

Лицензии

- компания имеет все необходимые лицензии ФСТЭК России, ФСБ России и Министерства обороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной и производство продукции в рамках гособоронзаказа.
- Система менеджмента качества продукции в компании соответствует стандарту ГОСТ ISO 9001-2015 и имеет соответствующие сертификаты.
- Система проектирования, разработки, производства и поддержки продукции соответствует требованиям российского военного стандарта ГОСТ РВ 15.002-2012, необходимого для участия в реализации гособоронзаказа.

Аладдин

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.2017

Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17

Лицензия Министерства обороны РФ № 1823 от 26.08.19

Система менеджмента качества компании соответствует требованиям ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) и ГОСТ РВ 0015-002-2012. Сертификаты соответствия № ВР 21.1.15048-2021 и № ВР 21.1.15049-2021

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