

JaCarta PKI в инфраструктуре Windows Server 2016

Руководство по внедрению

Листов: 179 Автор: DmitryShuralev

Аннотация

Настоящий документ представляет собой руководство по внедрению и использованию электронных ключей JaCarta PKI в среде Windows для обеспечения безопасности в сетях, включающих серверы и клиентские рабочие станции. Электронные ключи JaCarta PKI можно использовать с операционными системами Windows XP/7/Vista/8/10 и Server 2003/2008/2012/2016.

Действия по внедрению электронных ключей JaCarta PKI представлены на примерах операционных систем Windows Server 2016 Standard и Windows 10.

Следование приведенным в настоящем документе инструкциям является верным, но не всегда единственно возможным способом установки/настройки и работы с данным решением. В этом смысле они носят рекомендательный характер. Рассмотрение всех возможных способов настройки и использования данного решения не входит в задачи настоящего документа.

Для эффективного внедрения и управления электронными ключами JaCarta в сетевой среде Windows требуется квалифицированный системный администратор, обладающий навыками администрирования вычислительных сетей, включающих серверы Windows Server 2016 Standard и рабочие станции Windows 10.

Настоящий документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является

ЗАО "Аладдин Р.Д.". Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ.

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 компанией "Аладдин Р.Д." без предварительного уведомления. 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 компания "Аладдин Р.Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

Владельцем товарных знаков Аладдин, Aladdin, JaCarta, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО "Аладдин Р.Д.".

Владельцем товарных знаков Apple, iPad, iPhone, Mac OS, OS X является корпорация AppleInc. Владельцем товарного знака IOS является компания Cisco (CiscoSystems, Inc). Владельцем товарного знака WindowsVista и др. — корпорация Microsoft (MicrosoftCorporation). Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

При перепечатке и использовании данных материалов либо любой их части ссылки на ЗАО "Аладдин Р.Д." обязательны.

© ЗАО "Аладдин Р.Д.", 1995–2018. Все права защищены.

Оглавление

Введение	6
O JaCarta	7
Системные требования и описание демо-стенда	7
Требования к серверам	7
Требования к программному обеспечению	7
Требования к аппаратному обеспечению	8
Требования к рабочим станциям	8
Требования к программному обеспечению	8
Требования к аппаратному обеспечению	8
Описание демо-стенда	8
Использование цифровых сертификатов и полный отказ от паролей	9
Установка центра сертификации	10
Настройка шаблона выдачи сертификата	25
Выдача сертификатов	38
Выпуск сертификата Агента регистрации	41
Выпуск сертификата на электронный ключ JaCarta	44
Проверка работоспособности	50
Просмотр сертификата через Единый Клиент JaCarta	50
Вход в домен по сертификату на электронном ключе	52
Дополнительные возможности	54
Отключение возможности аутентификации по паролям	54
Автоматическое блокирование рабочей станции и выход из операционной систем при отсоединении JaCarta PKI	ы 64
Организация VPN-соединения для доступа к информационным ресурсам	65
Описание демо-стенда	66
Ход настройки	66
Установка роли IIS (Web-сервер) и запрос сертификата для IIS сервера	66
Установка роли IIS (Web-сервер)	67
Запрос сертификата для сервера IIS	73
Установка и настройка компонентов Удалённый доступ и Маршрутизация	75
Установка роли удалённый доступ и службы политики сети и доступа	75
Настройка маршрутизации	82
Назначение пользователю прав на использование VPN-подключения	90
Проверка работоспособности	91
Создание подключения	91
Подключение к шлюзу	94

Подключение к удалённому рабочему столу (RDP)	96
Описание демо-стенда	96
Ход настройки	96
Подключение к удалённому рабочему столу	97
Настройка рабочих станций и серверов	97
Действия пользователя	100
Доступ к информационным ресурсам по HTTPS	102
Общие сведения	102
Настройка сервера	102
Общие рекомендации и последовательность действий	102
Общие настройки сервера	102
Настройка сайта	104
Действия пользователя	105
Hастройка Mozilla Firefox и проверка входа на защищенный Web-сайт	106
Настройка конфигурации Mozilla Firefox	108
Действия пользователя	108
Защита документов Microsoft Office	109
Для чего нужна электронная подпись в MS Office?	109
Сертификат подписи и центр сертификации	109
Сертификат подписи	109
Центр сертификации	110
Что подтверждает цифровая подпись?	110
Какие приложения Microsoft Office поддерживают ЭП?	110
Хранение цифрового сертификата на электронном ключе	110
Добавление подписи к документу Microsoft Word 2016	110
Добавление подписи к документу Microsoft Excel 2016	119
Добавление подписи к документу Microsoft Power Point 2016	120
Защита электронной почты Outlook	121
Требования к инфраструктуре	121
Принцип работы	122
Для чего нужно шифровать сообщения?	122
Что подтверждает цифровая подпись?	123
Настройка и проверка шифрования и подписи	123
Настройка параметров безопасности	123
Отправка и получение подписанного сообщения	127
Отправка и получение зашифрованного сообщения	129
Шифрование данных EFS	132
Ход настройки	133
Выпуск сертификата шифрования	133
Настройка директорий шифрования	142

Проверка работоспособности	145
Шифрование данных BitLocker	147
Описание демо-стенда	148
Ход настройки	148
Установка компонента шифрования BitLocker	148
Редактирование шаблона сертификата пользователя	155
Настройка групповых политик BitLocker для взаимодействия с JaCarta PKI	158
Включение защиты (шифрования) носителя со стороны клиента	164
Проверка работоспособности	170
Разблокировка ключом восстановления	172
Отключение BitLocker	174
Контакты, техническая поддержка	176
Регистрация изменений	177

Ρ	егист	рация	изменений
-			

Введение



Применение смарт-карти USB-токенов JaCarta PKI в

инфраструктуре Windows Server позволяет полностью раскрыть потенциал инфраструктуры Windows как надежной платформы для ведения современного бизнеса. JaCarta в Windows может использоваться для аутентификации пользователей, доступа к внутрикорпоративным и интернетресурсам, шифрования данных, защиты данных и почтовой переписки.



Использование аутентификации на основе сертификатов X.509 в сетях на базе серверов Windows Server 2003/2008/2012/2016 позволяет полностью отказаться от парольной аутентификации. Внедрение данного решения — это кардинальное снижение влияния человеческого фактора на безопасность системы.

JaCarta в инфраструктуре Windows может быть использована в следующих сценариях:

- •аутентификация в домене Windows;
- •аутентификация на удалённом рабочем столе по протоколу RDP;
- •аутентификация в VPN-соединениях;
- •доступа к информационным ресурсам посредствам HTTPS (SSL);
- •защита электронной почты (подпись и шифрование, доступ к Outlook Web Access);
- •шифрования данных на жёстком диске (EFS, BitLocker);

•работа с любыми прикладными приложениями, поддерживающими смарт-карты и USB-токены.

Один и тот же электронный ключ JaCarta можно использовать для аутентификации в домене Windows и для работы с множеством приложений, использующих электронные ключи. Это позволяет уменьшить суммарную стоимость владения. При использовании российских сертифицированных СКЗИ, электронные ключи JaCarta могут использоваться как средство защищённого хранения ключевой информации. Решение может быть внедрено как на небольших предприятиях, так и в крупных корпорациях с инфраструктурой сети любой сложности.

O JaCarta

Для реализации двухфакторной аутентификации и подписи в среде Windows подойдёт вся линейка электронных ключей **JaCarta PKI**, в любом форм-факторе, включая и биометрические токены, и смарт-карты, где вместо ввода PIN-кода пользователь прикладывает к специальному считывателю свой палец. Для работы с **ГОСТ** алгоритмами (включая ГОСТ 2012 года) в прикладном ПО сторонних разработчиков можно использовать электронные ключи **JaCarta2 ГОСТ**.



JaCarta PKI — USB-, MicroUSB-токен или смарт-карта для строгой двухфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам предприятия, безопасного хранения ключей, ключевых контейнеров программных СКЗИ с использованием инфраструктуры открытых ключей (PKI) на основе зарубежных криптоалгоритмов.

JaCarta FOCT — USB-, MicroUSB-токен или смарт-карта для строгой двухфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам предприятия, безопасного хранения ключей, ключевых контейнеров программных СКЗИ с использованием инфраструктуры открытых ключей (PKI) на основе отечественных криптоалгоритмов.

Системные требования и описание демостенда

Требования к серверам

Требования к программному обеспечению

Операционная система

Решение предполагает использование серверов с установленной операционной системой Windows Server. Все примеры в настоящем документе даны на основе инфраструктуры **Windows Server 2016 Standard.** Сами же решения, описанные в настоящем документе, поддерживают и более старые версии Windows Server — 2003/2008/2012.

Драйвер устройства чтения смарт-карт

В случае использования устройства чтения смарт-карт на компьютере должен быть установлен драйвер этого устройства.

1.0

Единый клиент JaCarta

На каждом компьютере, на котором используются электронные ключи JaCarta, должно быть установлено ПО Единый клиент JaCarta.

Информация, касающаяся установки и настройки Единый клиент JaCarta, представлена в документе "Единый клиент JaCarta. Руководство администратора".

Требования к аппаратному обеспечению

Сервер должен удовлетворять требованиям к аппаратному обеспечению, изложенным в документации к соответствующей редакции Windows Server.

Каждый компьютер, на котором используются смарт-карты JaCarta, должен быть оборудован устройством чтения смарт-карт.

На каждом компьютере, на котором используются **USB-токены JaCarta**, должен быть доступен хотя бы один свободный порт USB.

Требования к рабочим станциям

Требования к программному обеспечению

Операционная система

Решение предполагает использование рабочих станций с установленной операционной системой Windows. Все примеры в настоящем документе даны на основе **Windows 10 Pro.** Сами же решения, описанные в настоящем документе, поддерживают и более старые версии Windows — XP/Vista/7/8/8.1.

Драйвер устройства чтения смарт-карт

В случае использования устройства чтения смарт-карт на компьютере должен быть установлен драйвер этого устройства.

Единый клиент JaCarta

На каждом компьютере, на котором используются электронные ключи JaCarta, должно быть установлено ПО Единый клиент JaCarta.

Информация, касающаяся установки и настройки Единый клиент JaCarta, представлена в документе "Единый клиент JaCarta. Руководство администратора".

Требования к аппаратному обеспечению

Рабочие станции должны удовлетворять требованиям к аппаратному обеспечению, изложенным в документации к соответствующей версии Windows.

Каждый компьютер, на котором используются смарт-карты JaCarta, должен быть оборудован устройством чтения смарт-карт.

На каждом компьютере, на котором используются **USB-токены JaCarta**, должен быть доступен хотя бы один свободный порт USB.

Описание демо-стенда

Демо-стенд состоит из следующих компонентов.

Сервер

Windows Server 2016 Standard с установленной и настроенной ролью Active Directory и установленным программным обеспечением Единый Клиент JaCarta.

Предполагается, что Active Directory уже создана, в настоящем документе этот процесс не описывается. За помощью в настройке **Active Directory**, обратитесь к справочному руководству по Windows Server, соответствующему версии вашего Windows Server.

Далее на этот сервер будут установлены все необходимые роли и компоненты, необходимые для реализации сценариев, описанных в настоящем документе.

Клиент

Windows 10 Pro, введённая в домен с установленным программным обеспечением Единый Клиент JaCarta.

Использование цифровых сертификатов и полный отказ от паролей

Настройка доменной аутентификации в **Windows Server 2016** по сертификатам, выпущенным на USBтокены и смарт-карты **JaCarta PKI**, при условии готового вышеописанного демо-стенда, сводится к следующим шагам:

•установка роли центр сертификации Active Directory (Active Directory Certificate Services);

•настройка шаблонов выдачи сертификатов;

•выпуск сертификатов на электронные ключи JaCarta PKI;

•проверка аутентификации по электронному ключу в домене.

Опционально можно настроить автоматическую блокировку рабочей станции при отсоединении электронного ключа, а также совсем отключить парольную аутентификацию.

© "Аладдин Р.Д.", 2018

Установка центра сертификации

Необходимо добавить роль **центра сертификации** Active Directory с помощью мастера добавления ролей и компонентов сервера и сконфигурировать её. Для этого выполните следующие действия.

Нажмите Пуск -> Диспетчер серверов.



В отобразившемся окне выберите Управление -> Добавить роли и компоненты.

📥 Диспетчер серверов ٥ \times • (3) | 🚩 Панель мониторинга Vr Справ Средства Вид Добавить роли и компоненты Удалить роли и компоненты Вас приветствует диспетчер серверов 🔢 Панель мониторинга Добавление серверов Локальный сервер Создание группы серверов Все серверы Свойства диспетчера серверов Настроить этот локальный серв AD DS 🔒 DNS 2 Добавить роли и компоненты By WDS Файловые службы и сл... 🕨 3 Добавить другие серверы для управления Что нового 4 Создать группу серверов 5 Подключить этот сервер к облачным службам Скрыть Подробнее РОЛИ И ГРУППЫ СЕРВЕРОВ Роли: 4 | Группы серверов: 1 | Всего серверов: 1 AD DS 🔒 DNS 1 1 • Управляемость • Управляемость События События Службы Службы Производительность Производительность Результаты ВРА Результаты ВРА へ 🖫 ជ_象 рус 13:34 の8.09.2017 ρ [[]] e 9

Отобразится окно мастера добавления ролей и компонентов, для продолжения нажмите Далее.

Убедитесь, что учётная запись доменного администратора имеет надёжный пароль, вы находитесь под учётной записью доменного администратора, и вход в домен выполнен.

📥 Мастер добавления ролей и к	омпонентов	-		×
Перед началом р	работы	KOHE4 mos	НЫЙ СЕРЕ scow.local.t	3EP rest
Перед началом работы Тип установки	Этот мастер поможет вам установить роли, службы ролей или компоненты. Оп нужно установить, на основании потребностей своей организации, таких как о документам или размещение веб-сайта.	редели бщий д	те, что оступ к	
Выбор сервера Роли сервера	Чтобы удалить роли, службы ролей или компоненты: Запустить мастер удаления ролей и компонентов			
Компоненты Подтверждение Результаты	Прежде чем вы продолжите, убедитесь, что выполнены следующие задачи: • Учетная запись администратора защищена надежным паролем • Настроены сетевые параметры, такие как статические IP-адреса • Установлены новейшие обновления безопасности из Центра обновления Win Если вам требуется проверить, выполнены ли какие-либо предшествующие не условия, закройте мастер, выполните необходимые шаги и запустите мастер сн Чтобы продолжить, нажмите кнопку "Далее".	ndows обходин юва.	мые	
	<u>П</u> ропускать эту страницу по умолчанию			
	< <u>Н</u> азад Далее > Установ	вить	Отмен	a

В следующем окне выберите Установка ролей и компонентов.

а Мастер добавления ролей и	компонентов	-		×
Выбор типа уста	НОВКИ	KOHE mo	ЧНЫЙ СЕР scow.local.1	BEP test
Перед началом работы Тип установки Выбор сервера Роли сервера Компоненты Подтверждение Результаты	Выберите тип установки. Вы можете установить роли и компоненты на работ компьютере, на виртуальной машине или на автономном виртуальном жести	ающем (юм дискі птов. ов (VDI), ч	физическ е (VHD). чтобы	ом
	< <u>Н</u> азад <u>Далее ></u> <u>У</u> стан	овить	Отмен	ia

Выберите сервер, на который будет установлена роль, и нажмите Установить.

눰 Мастер добавления ролей и ко	омпонентов				_		×
Выбор целевого	сервера				KOHE mc	ЧНЫЙ СЕР xscow.local.	BEP .test
Перед началом работы Тип установки	Выберите серг компоненты.	зер или вирт	гуальный жесткий	диск, на котором будут устан	овлены роли	1 И	
Выбор сервера	Выберите с	сервер из пу	ла серверов				
Роли сервера	О Выберите в	зиртуальный	і жесткий диск				
Компоненты	Пул серверо	в					
Подтверждение	Фильтр:						
Результаты							
	Имя		ІР-адрес	Операционная система			
	moscow.local.	test	172.16.12.122	Майкрософт Windows Serve	er 2016 Datac	enter	
	Найдено комп	ьютеров: 1					
	На этой страни выпуска Windo диспетчере се с которых пок	ице показан ows Server, к рверов. Не в а полностью	ы серверы под уп оторые были доб выводятся автоно о не получены.	равлением Windows Server 20 авлены с помощью команды мные серверы и добавленные	12 или болес "Добавить се в новые серв	е нового :рверы" в :еры, дан	з ные
			< <u>H</u> a	зад Д <u>а</u> лее > <u>У</u>	становить	Отмен	на

В следующем окне отметьте службу сертификатов Active Directory и нажмите Далее.

Выбор ролей се Перед началом работы Тип установки Выбор сервера	ОВЕРА Выберите одну или несколько ролей для установки на этом с Роли	КОНЕЧНЫЙ СЕРВЕР moscow.local.test ервере.
Перед началом работы Тип установки Выбор сервера	Выберите одну или несколько ролей для установки на этом с Роли	ервере.
Выбор сервера		Описание
Роли сервера Компоненты Подтверждение Результаты	Веб-сервер (IIS) ▲ Доменные службы Active Directory (Установленс Режим Windows Server Essentials Сяужба опекуна узла Службы Active Directory облегченного доступа в Службы Active Directory облегченного доступа в Службы Windows Server Update Services Службы Windows Server Update Services Службы windows Server Update Services Службы печати и документов Службы политики сети и доступа Службы политики сети и доступа ✓ Службы развертывания Windows (Установлено) Службы удаленных рабочих столов Службы удаленных рабочих столов Службы удаленных рабочих столов Службы управления правами Active Directory Службы удаленных рабочих столов Факс-сервер ✓	Службы сертификатов Active Directory (AD CS) предназначены для создания центров сертификации и связанных служб ролей, которые позволяют выдавать сертификаты для различных приложений и управлять такими сертификатами.

Мастер предложит установить зависимые компоненты, нажмите Добавить компоненты.

🚘 Мастер добавления ролей и компонентов	×
Добавить компоненты, необходимые для Службы сертификатов Active Directory?	
Для управления этим компонентом требуются следующие средства. Однако их не нужно устанавливать на одном и том же сервере.	
 Средства удаленного администрирования сервера Средства администрирования ролей Средства служб сертификации Active Directory [Средства] Средства управления центра сертификац 	
< >>	
Включить средства управления (если применимо)	1
Добавить компоненты Отмена	

Обратите внимание на предупреждение, нажмите Далее.

После установки роли центра сертификации изменить имя и параметры домена будет невозможно.

Службы сертифи	катов Active Directory	KOHE	ЧНЫЙ СЕР scow.local	BE tes
Перед началом работы Тип установки Выбор сервера Роли сервера Компоненты Служба сертификации А Службы ролей Подтверждение Результаты	Службы сертификации Active Directory (AD CS) предоставляют инфрастру обеспечения работы защищенных беспроводных сетей, виртуальных час протокола IP (IPSec), защиты доступа к сети (NAP), шифрованной файлово использованием смарт-карт. На что обратить внимание: • После установки центра сертификации (ЦС) нельзя изменить имя и пар компьютера. Если вы хотите изменить имя этого компьютера, присоед повысить до контроллера домена, сделайте это перед установкой ЦС. Д сведения см. в разделе, посвященном именованию центров сертифика	иктуру сертиф стных сетей, б ой системы (Е раметры дом инить его к д Дополнитель ации.	икации, езопасн FS) и вх ена данн омену и ные	цл ос ли

В следующем окне отметьте необходимые службы ролей и нажмите **Далее,** минимально необходимая роль — центр сертификации.

ᡖ Мастер добавления ролей и к	омпонентов	- 🗆 X
Мастер добавления ролей и к Выбор служб ро. Перед началом работы Тип установки Выбор сервера Роли сервера Компоненты Служба сертификации А Службы ролей	– С Х КОНЕЧНЫЙ СЕРВЕР moscow.local.test катов Active Directory. Описание Центр сертификации (ЦС) выдает сертификаты и управляет ими. Несколько ЦС можно объединить в инфраструктуру открытых ключей.	
Подтверждение Результаты		
	< <u>Н</u> азад Д <u>а</u> лее	> Установить Отмена

Начнется процесс установки роли.

ᡖ Мастер добавления ролей и ко	мпонентов	_		Х
Ход установки		KOHE4 mos	НЫЙ СЕР scow.local.t	BEP
Перед началом работы	Просмотр хода установки			
Тип установки	установка компонента			
Выбор сервера				
Роли сервера	Начата установка на moscow.local.test			
Компоненты	Службы сертификатов Active Directory			
Служба сертификации А	Центр сертификации			
Службы ролей	Средства удаленного администрирования сервера			
Подтверждение	Средства администрирования ролей			
Результаты	Средства служо сертификации Active Directory Средства управления центра сертификации			
	 Этот мастер можно закрыть, не прерывая выполняющиеся задачи. На выполнения задачи или откройте эту страницу снова, выбрав на панел "Уведомления", а затем "Сведения о задаче". Экспорт параметров конфигурации 	и коман,	е за ходо д пункт	M
	< <u>Н</u> азад Д <u>а</u> лее > Закр	ыть	Отмен	а

По завершении установки нажмите Настроить службу сертификатов Active Directory на сервере.



В следующем окне, если вы находитесь под доменным администратором и в учётных данных всё верно отображено, нажмите **Далее.**

ᡖ Конфигурация службы сертиф	📥 Конфигурация службы сертификатов Active Directory — 🛛			\times
Учетные данные		KOHEЧHI mosco	ЫЙ CEPB w.local.t)EP est
Учетные данные	Укажите учетные данные для настройки служб ро	ли		
Службы ролей Вариант установки Тип ЦС Закрытый ключ Шифрование Имя ЦС Срок действия База данных сертификат Подтверждение Ход выполнения Результаты	Чтобы установить следующие службы роли, необходимо быть членом ло "Администраторы": • Автономный центр сертификации • Служба регистрации в центре сертификации через Интернет • Сетевой ответчик Чтобы установить следующие службы роли, необходимо быть членом гр "Администраторы предприятия": • Центр сертификации предприятия • Веб-служба политик регистрации сертификатов • Веб-служба регистрации сертификатов • Служба регистрации на сетевых устройствах Учетные данные: LOCAL\adm	укальной г	руппы	
	Дополнительные сведения о ролях серверов AD CS < <u>Н</u> азад Далее > <u>Н</u> астр	роить	Отмена	3

Выберите роли для настройки и нажмите **Далее,** минимально необходимая роль — центр сертификации.

ᡖ Конфигурация службы сертиф	икатов Active Directory	_		×
Службы ролей		KOHE4F mosc	lЫЙ CEP ow.local.	BEP test
Учетные данные Службы ролей Вариант установки Тип ЦС Закрытый ключ Шифрование Имя ЦС Срок действия База данных сертификат Подтверждение Ход выполнения Результаты	Выберите службы роли для настройки Центр сертификации Служба регистрации в центре сертификации через Интернет Сетевой ответчик Служба регистрации на сетевых устройствах Ве6-служба регистрации сертификатов Ве6-служба политик регистрации сертификатов			
	дополнительные сведения о ролях серверов AD CS			
	< <u>Н</u> азад Д <u>а</u> лее >	<u>Н</u> астроить	Отмен	a

🚡 Конфигурация службы сертификатов Active Directory — 🔲 🗙		
Вариант установ	КОНЕЧНЫЙ СЕРВЕР moscow.local.test	
Учетные данные Службы родей	Укажите вариант установки ЦС	
Служов ролеи Вариант установки Тип ЦС Закоытый ключ	Чтобы упростить управление сертификатами, центры сертификации предприятия могут использовать доменные службы Active Directory (AD DS). Автономные центры сертификации не используют доменные службы Active Directory для выдачи сертификатов или управления ими.	
Шифрование Имя ЦС Срок действия База данных сертификат Подтверждение Ход выполнения Результаты	 ЦС предприятия Чтобы центры сертификации предприятия могли выдавать сертификаты или политики сертификата, они должны входить в домен и быть подключены к сети. Автономный ЦС Автономные центры сертификации могут быть членами рабочей группы или домена. При использовании автономных центров сертификации доменные службы Active Directory и сетевое подключение не требуются. 	
	Подробнее о варианте установки < <u>Н</u> азад Далее > <u>Н</u> астроить Отмена	

В следующем окне установите тип центра сертификации, **Подчинённый** или **Корневой,** так как в настоящем примере новая настройка, выберите **Корневой.** После выбора типа ЦС нажмите **Далее.**



В следующем окне для нового центра сертификации выберите Создать новый закрытый ключ.

📥 Конфигурация службы сертиф	икатов Active Directory	_		×
Закрытый ключ		KOHE4H mosc	lЫЙ CEP ow.local.	BEP test
Учетные данные	Укажите тип закрытого ключа			
Службы ролей				
Вариант установки	Чтобы создавать сертификаты и выдавать их клиентам, центр сертифика	ции (ЦС) ,	должен	
Тип ЦС	иметь закрытый ключ.			
Закрытый ключ	Оздать новый закрытый ключ			
Шифрование	Используйте этот параметр, если у вас нет закрытого ключа или вы х закрытый ключ	отите созд	цать новы	ый
Имя ЦС				
Срок действия	Использовать существующий закрытый ключ			
База данных сертификат	Используйте этот параметр, чтобы при переустановке ЦС гарантиров ранее выданными сертификатами.	ать непре	ерывност	ъс
Подтверждение	Выбрать сертификат и использовать связанный с ним закрытый к	люч		
Ход выполнения	Выберите этот параметр, если на этом компьютере есть существук	ощий серт	гификат	
Результаты	или если вы хотите импортировать сертификат и использовать свя закрытый ключ.	занныи с	ним	
	Выбрать существующий закрытый ключ на этом компьютере			
	Выберите этот параметр, если вы сохранили закрытые ключи из п установки или хотите использовать закрытый ключ из другого ист	редыдуще очника.	ей	
	Подробнее о закрытом ключе			
	< <u>Н</u> азад Далее > <u>Н</u> аст	роить	Отмен	ia

В следующем окне укажите параметры шифрования и нажмите **Далее**. В настоящем примере в качестве криптопровайдера указан **Microsoft KeyStorage Provider** с длинного ключа **2048 бит** и алгоритмом **хэширования SHA-256**.

📠 Конфигурация службы сертификатов Active Directory			_		×
Шифрование для	а ЦС		KOHE4 mos	НЫЙ СЕР cow.local	'BEP .test
Учетные данные Службы ролей	Укажите параметры шифрования				
Вариант установки	Выберите поставщик служб <u>ш</u> ифрования:		Дли <u>н</u> а ключа:		
Тип ЦС	RSA#Microsoft Software Key Storage Provider	¥	2048		Ŷ
Закрытый ключ Шифрование Имя ЦС Срок действия База данных сертификат Подтверждение Ход выполнения Результаты	Выберите <u>х</u> эш-алгоритм для подписывания сертификатов, п SHA256 SHA384 SHA512 SHA1 MD5	с обра	емых этим ЦС: щается к закры	тому клю	учу.
	Подробнее о шифровании	_			
	< <u>Н</u> азад Д <u>а</u> лее >		<u>Н</u> астроить	Отмен	ła

В следующем окне нажмите Далее.

📥 Конфигурация службы сертификатов Active Directory				Х
Имя ЦС		KOHE4H mosc	ЫЙ CEPI ow.local.t	BEP test
Учетные данные Службы ролей Вариант установки	УКАЖИТЕ ИМЯ ЦС Введите общее имя, определяющее этот центр сертификации (ЦС). Это добавляться во все сертификаты, выдаваемые данным ЦС. Значения су) имя будет ффикса		
тип цс Закрытый ключ Шифрование	различающегося имени создаются автоматически, но могут быть изме Общее имя для этого ЦС: local-MOSCOW-CA	нены.		
Срок действия База данных сертификат Подтверждение Ход выполнения Результаты	Суффикс различающегося имени: DC=local,DC=test Предпросмотр различающегося имени: CN=local-MOSCOW-CA,DC=local,DC=test			
	Подробнее об имени ЦС < <u>Н</u> азад Д <u>а</u> лее > <u>Н</u> аз	строить	Отмен	a

В следующем окне укажите срок действия корневого сертификата, в настоящем примере - 5 лет. Нажмите **Далее.**

📥 Конфигурация службы сертиф	икатов Active Directory	_		×
Срок действия		KOHEЧH mosco	ЫЙ CEPE ow.local.t	BEP rest
Учетные данные Службы ролей Вариант установки Тип ЦС Закрытый ключ Шифрование Имя ЦС Срок действия База данных сертификат Подтверждение Ход выполнения Результаты	Укажите период действия сертификата, созданного для этого центра серт 5 г	чфикаци срок дей	и (ЦС): ствия	
	Подробнее о сроке действия			
	< <u>Н</u> азад Д <u>а</u> лее > <u>Н</u> астр	ооить	Отмена	a

На следующем окне нажмите Далее.

📥 Конфигурация службы сертиф	фикатов Active Directory	_		×
База данных ЦС		KOHE4 mose	НЫЙ СЕР cow.local	BEP .test
Учетные данные Службы ролей	Укажите расположения баз данных			
Вариант установки	Р <u>а</u> сположение базы данных сертификатов:			
Тип ЦС	C:\Windows\system32\CertLog			
Закрытый ключ Шифрование Имя ЦС Срок действия База данных сертификат Подтверждение Ход выполнения Результаты	Расположение жур <u>н</u> ала базы данных сертификатов: C:\Windows\system32\CertLog			
	Подробнее о базе данных ЦС < <u>Н</u> азад Д <u>а</u> лее >	<u>Н</u> астроить	Отмен	на

Следующее окно отобразит дайджест конфигурации, проверьте и нажмите Настроить.

ᡖ Конфигурация службы сертификатов Active Directory — 🗆 🗙					
Подтверждение			КОНЕЧН mosco	ЫЙ CEPB ow.local.t	EP est
Учетные данные Службы ролей	Чтобы настроить следующие "Настроить".	роли, службы ролей или компоненты, нажм	ите кноп	¢y	
Вариант установки	🔿 Службы сертификации	Active Directory			^
Тип ЦС	Центр сертификации				
Закрытый ключ	Тип ЦС:	Корень предприятия			
Шифрование	Поставщик служб	RSA#Microsoft Software Key Storage Provide	r		
Имя ЦС	шифрования:	014055			
Срок действия	Алгоритм хеширования:	SHA256			
База данных сертификат	длина ключа: Разрешить взаимодействие с администратором:	2048 Отключено			
Подтверждение	Срок действия сертификата:	11.09.2022 12:21:00			
Ход выполнения	Различающееся имя:	CN=local-MOSCOW-CA,DC=local,DC=test			
Результаты	Расположение базы данных сертификатов:	C:\Windows\system32\CertLog			
	Расположение журнала базы данных сертификатов:	C:\Windows\system32\CertLog			
	Служба регистрации в цент	ре сертификации через Интернет			~
		< <u>Н</u> азад Д <u>а</u> лее > <u>Н</u> астр	оить	Отмена	1

Если всё сделано верно, о	отобразятся сообщения	об успешном выполн	ении.
---------------------------	-----------------------	--------------------	-------

🚡 Конфигурация службы сертиф	икатов Active Directory		_		×
Результаты			KOHE4H mosc	НЫЙ CEP cow.local.	BEP .test
Учетные данные	Настроены следующие роли, службы р	олей и компоненты:			
Службы ролей	🔿 Службы сертификации Active Di	irectory			
Вариант установки	Пентр сертификации	🗸 Настройка вы	полнена успеш	но	
Тип ЦС	Подробнее о настройке ЦС		itomicita yenea		
Закрытый ключ	C	• 11 *			
Шифрование	служоа регистрации в центре сертификации через Интернет	Настроика вы	полнена успеш	но	
Имя ЦС	Подробнее о настройке регистрации ч	ерез Интернет			
Срок действия					
База данных сертификат					
Подтверждение					
Ход выполнения					
Результаты					
	< <u>H</u> a	азад Д <u>а</u> лее >	Закрыть	Отмен	а

Нажмите Закрыть.

Установка и конфигурация службы сертификации Active Directory на этом завершена.

Настройка шаблона выдачи сертификата

После установки и настройки роли центра сертификации Active Directory, необходимо создать шаблоны выдачи сертификатов на электронные ключи JaCarta.

Управление шаблонами происходит через консоль Центр сертификации.

Для открытия консоли выполните следующие действия.

Нажмите правой кнопкой меню Пуск выберите Выполнить -> mmc.

Корзина	
Программы и компоненты	
Управление электропитанием	
Просмотр событий	
Система	
Диспетчер устройств	
Сетевые подключения	
Управление дисками	
Управление компьютером	
Командная строка	
Командная строка (администратор)	
Диспетчер задач	
Панель управления	
Проводник	
Найти	
Выполнить	
Завершение работы или выход из системы	
Рабочий стол	
	へ 盟 d _参 ENG 13:30 11.09.2017 司

Нажмите ОК.

💷 Выполни	ть Х
۲	Введите имя программы, папки, документа или ресурса Интернета, которые требуется открыть.
<u>О</u> ткрыть:	mmc v
	ОК Отмена Об <u>з</u> ор

В отобразившемся окне выберите Добавить или удалить оснастку.

🚟 Консоль1 - [Корень консоли]	- 🗆 X
<mark>ឝ</mark> Файл Действие Вид Избранное Окно	Справка – 🗗 🗙
 Создать Создать Открыть Сохранить Сохранить как Добавить или удалить оснастку СТР Параметры Последний файл Выход 	справка trl+N trl+O RL+S L+M Дополнительн > Действия Корень консоли Дополнительн >
Позволяет добавлять оснастки в консоль или удаля	ъих.

В следующем окне выберите Центр сертификации, нажмите Добавить, нажмите ОК.

ступные оснастки:				В <u>ы</u> бранные оснастки:	
снастка	Поставщик	^		🔛 Корень консоли	Изменить рас <u>ш</u> ирени
у Телефония	Microsoft C				Verenze
Управление ТРМ	Корпораци				<u>у</u> далить
Управление груп	Корпораци				
Управление диск	Программн				Вверх
Управление комп	Microsoft C				
Управление печа	Корпораци				Вниз
Управление поли	Microsoft C		Щооавить >		
Управление сете	Корпораци				
🛚 Управляющий эл	Microsoft C				
Центр сертифик	Корпораци				
Шаблоны безопа	Корпораци				
Шаблоны сертиф	Microsoft C				
Элемент ActiveX	Microsoft C	\mathbf{v}			Дополнительно
				L	
исание:					
PROPORT NACTORNESTL	свойства цент	ha cer	отификации и упл	авлять сертификатами, издан	ными этим ПС

В следующем окне выберите локальным компьютером и нажмите Готово.

Центр сертификации	×
Выберите компьютер, которым должна управлять эта оснастка. Эта оснастка всег да управляет: 	
< Назад Готово Отмена Справка	J

Для удобства дальнейшего использования сохраните данную консоль, выбрав Файл -> Сохранить.

	Консс	ль1 - [Корень консоли\Центр сер Лействие Вид Избранное	тификации (Ло Окно Справ	кальный) ка	\local-MOSCOW	-СА\Отозванные серти	– o ×
•	С	оздать	Ctrl+N				
	0	ткрыть	Ctrl+O	проса	Дата отзыва	Дата вступления от:	Действия
~	🗸 Сохранить		CTRL+S				Отозванные серти 🔺
	C	охранить как		гэлемен	тов для отображ	ения в этом виде.	Лополнительн
	Д	обавить или удалить оснастку	CTRL+M				дополнительн у
	П	араметры					
	П	Іоследний файл					
	В	ыход					
			<			>	
Cox	ранить	текущую консоль					

Укажите имя (например, ЦентрСертификации) и место расположения (например, Рабочий стол). Нажмите **Сохранить.**

🚟 Сохранение					×
<u>П</u> апка:	Рабочий сто	л	✓ G ∅	ð 📂 🛄 -	
Б ыстрый доступ	adm	adm	этот	компьютер	
Рабочий стол	Библ	иотеки	Сеть		
Библиотеки	sc				
 Этот компьютер					
🇳 Сеть					
	<u>И</u> мя файла:	ЦентрСертификации			ить
	<u>Т</u> ип файла:	Файлы консоли управ	зления (*.msc)	~ Отме	на

Теперь запустить консоль **ЦентрСертификации** можно по созданному ярлыку, который находится на рабочем столе.

Щёлкните правой кнопкой по папке Шаблоны сертификатов и нажмите Управление.

🚟 ЦентрСертификации - [Корень консоли	\Центр сертификации (Локальный)\local-	MOSCOW-CA\Шабло —	
🚟 Файл Действие Вид Избранное	Окно Справка		_ 8 ×
🗢 🔿 📶 🖬 🖬 🖬			
Корень консоли Корень консоли Салания сертификации (Локальный) Салания сертификаты Выданные сертификаты Запросы в ожидании Неудачные запросы Шаблоны сертификатов Создать Вид Новое окно отсюда Новый вид панели за Обновить Экспортировать спис	Имя Почтовая репликация каталога Проверка подлинности контролле проверка подлинности Kerberos Агент восстановления EFS Базовое шифрование EFS Контроллер домена р р ель ный центр сертификации затор	Назначение Почтовая репликация служб Проверка подлинности клик Проверка подлинности клик Восстановление файлов Шифрующая файловая сист Проверка подлинности клик Проверка подлинности клик Шифрующая файловая сист <Все> Подписывание списка довер	Действия Шаблоны … ▲ Допо… ▶
Запуск оснастки шаблонов сертификатов			

🚇 Консоль шаблонов сертифика	атов				– 🗆 X
Файл Действие Вид Справк	ca				
🚇 Шаблоны сертификатов (mosc	Отображаемое имя шаблона	Версия схемы	Версия	Назнач ^	Действия
	🚇 Агент восстановления ключей	2	105.0	Агент в	Шаблоны сертификатов (🔺
	🚇 Агент регистрации	1	4.1		Лополнительные дей 🕨
	🚇 Агент регистрации (компьютер)	1	5.1		Дополнительное дени у
	🚇 Агент регистрации Exchange (автоном	1	4.1		Пользователь со смарт-к 🔺
	🚇 Администратор	1	4.1		Дополнительные дей 🕨
	🚇 Базовое шифрование EFS	1	3.1		
	🚇 Веб-сервер	1	4.1		
	🚇 Вход со смарт-картой	1	6.1		
	🚇 Компьютер	1	5.1		
	🚇 Контроллер домена	1	4.1		
	🚇 Корневой центр сертификации	1	5.1		
	🚇 Маршрутизатор (автономный запрос)	1	4.1		
	🚇 Перекрестный центр сертификации	2	105.0		
	🗷 Подписывание кода	1	3.1		
	🚇 Подписывание отклика OSPC	3	101.0	Подпи	
	🚇 Подписывание списка доверия сертиф.	1	3.1		
	🚇 Подчиненный центр сертификации	1	5.1		
	🚇 Пользователь	1	3.1		
	🚇 Пользователь Exchange	1	7.1		
	🛲 Пользователь со смарт-картой		11.1		
	🚇 Почтовая репликация каталога 💦 🗌	копировать шаблон	115.0	Почто	
	🚇 Проверенный сеанс Во	се задачи >	3.1		
	🚇 проверка подлинности Kerbero		110.0	Провеј	
	🚇 Проверка подлинности контро	войства	110.0	Провеј	
	🚇 Проверка подлинности рабоче С	правка	101.0	Провеј	
	🗷 Только подпись Exchange		6.1		
	🚇 Только подпись пользователя	1	4.1		
	🚇 ЦС Exchange	2	106.0	Архива	
	🖳 Шифрование СЕР	1	4.1		
				~	
< >	<			>	
При использовании данного шабло	она в качестве базового будет создан шабло	он, поддерживающий ЦС Win	dows Server 2003	Enter	

Отобразится консоль шаблонов, щёлкните правой кнопкой по **Пользователь со смарт-картой** и нажмите **Скопировать шаблон.**

Откроются свойства шаблона, содержащие 11 вкладок. На вкладке **Совместимость** можно указать совместимость с сервером центра сертификации и пользовательским рабочим местом, в настоящем примере оставлено без изменений - минимальная конфигурация.

Свойства нового шабл	она			×				
Шифрование	Аттестация ключей	Имя	субъекта	Сервер				
Требования выдачи	Устаревшие шабл	оны Раси	ирения	Безопасность				
Совместимость	Общи	e	Обработ	ка запроса				
Доступные параметрь системы указаны в па	Доступные параметры шаблонов зависят от того, какие из ранних версий операционной системы указаны в параметрах совместимости.							
Показать последук	щие							
Параметры режима Центр сертификаци	совместимости И							
Windows Server 200)3		\sim					
<u>П</u> олучатель сертиф Windows XP / Serve	иката er 2003		~					
Эти параметры не зап использовать этот ша	рещают операционным блон. ОК	и системам бол Отмена	ее ранних ве При <u>м</u> ени	ерсий 1ть Справка				

Перейдите во вкладку Общее. Здесь можно задать имя шаблона, период действия и срок обновления. Задайте Отображаемое имя шаблона, в настоящем примере JaCarta user.

войства нового шабло	она		×
Шифрование	Аттестация ключей	Имя субъекта	Сервер
Требования выдачи	Устаревшие шаблоны	Расширения	Безопасность
Совместимость	Общие	Обработ	ка запроса
Отображаемое имя ша	блона:		
JaCarta user			
Дели шеолопа. ЈаСаrtauser Период действия: 2 г. ✓ Опубликовать серти Периодиковать серти Периодиковать серти Существует в Ас	Период о <u>б</u> новлени 6 нед. 1фикат в Active Directory о автоматическую перезаявн tive Directory	ія: ✓ ку, если такой сертиф	рикат уже

Во вкладке Обработка запроса укажите цель и действие при подаче заявки, как показано на экране ниже.

Свойства нового шабл	она		×			
Шифрование	Аттестация ключей	Имя субъекта	Сервер			
Гребования выдачи	Устаревшие шаблоны	Расширения	Безопасность			
Совместимость	Общие	Обработ	ка запроса			
Цель: Подпись и шифрование ✓ Удалять отозванные или просроченные сертификаты, не архивируя Включить симметричные алгоритмы, разрешенные субъектом Архивировать закрытый ключ субъекта						
Разрешить экспорт Обновлять с исполь Если невозможно с сертификатов смар	ировать закрытый ключ зованием того же ключа (*) оздать новый ключ, то для а т-карт следует использовать	зтоматического обно существующий ключ	вления 4 (*)			
При подаче заявки для субъекта и использовани закрытого ключа его сертификата следует: О <u>П</u> одавать заявку для субъекта, не требуя ввода данных О <u>З</u> апрашивать пользователя во время регистрации						
 При регистрации выводить запрос и требовать от пользователя ответ, если используется закрытый ключ Элемент управления отключен из-за параметров совместимости. 						
	ОК О	тмена При <u>м</u> ени	справка			

Во вкладке Требования выдачи укажите Политику применения и Агент запроса сертификата.

Это не единственный возможный способ выпуска сертификата, но в настоящем примере рассматривается выпуск сертификатов Администратором от имени пользователя через агента регистрации.

Свойства нового шабло	на		×				
Шифрование	Аттестация ключей	Имя субъекта	Сервер				
Совместимость	Общие	Обработ	ка запроса				
Требования выдачи	Устаревшие шаблоны	Расширения	Безопасность				
Требовать для регистр Одобрения диспетче Указанного <u>ч</u> исла а Автоматическая ре	Требовать для регистрации: Одобрения диспетчера сертификатов ЦС Указанного числа авторизованных подписей: 						
В подлиси требуетс	я указать <u>т</u> ип политики:						
Политика примене	ния		\sim				
Политика применен	ия:						
Агент запроса сер	гификата		~				
Политики <u>в</u> ыдачи:		_					
	До <u>б</u> авить Удалить						
Требовать для повторн	ой регистрации:						
• Тех <u>ж</u> е условий, что	и для регистрации						
Подтвердить сущес	твующий сертификат						
<u>Р</u> азрешить обно	зление на основе ключей (*)						
Требует предоставлять данные о субъекте в запросе сертификата.							
*Элемент управления отключен из-за параметров совместимости.							
	ОК С	тмена При <u>м</u> ени	ить Справка				

Перейдите на вкладку Шифрование и в качестве поставщика служб шифрования (криптопровайдер) установите Athena ASECard Crypto CSP.

JaCarta PKI также поддерживает работу с криптопровайдером Microsoft Base Smard Card Crypto Provider. В этом случае для работы JaCarta PKI потребуется только minidriver.

Свойства нового шаблона							
Требования выдачи	Устаревшие шаблоны		Расширения	Безопасность			
Совместимость		Общие	Обработка	а запроса			
Шифрование	Аттестаци	я ключей	Имя субъекта	Сервер			
<u>Категория поставщика:</u> Устаревший поставщик служб шифрования							
Им <u>я</u> алгоритма:	Опреде		аляется поставщиком служб шифрования 🛛 🗸				
Минимальный размер	ключа:	2048					
Выберите поставщиков шифрования, которых можно использовать для запросов О В запросах могут использоваться любые поставщики, доступные на компьютере пользователя © В запросах могут использоваться только следующие поставщики:							
Поставщики:							
Athena ASECard Crypto CSP Microsoft Base Smart Card Crypto Provider Microsoft DH SChannel Cryptographic Provider Microsoft Enhanced Cryptographic Provider v1.0 Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider							
⊻эш запроса:	Определ	яется поставщи	ком служб шифровани	м. V			
<u>И</u> спользуйте дополнительный формат подписи							
		OK Ot	тмена При <u>м</u> енит	ь Справка			

Перейдите во вкладку Имя субъекта, выберите Строится на основе данных Active Directory. Формат имени субъекта отметьте Полное различающиеся имя.

Свойства нового шаблона Х							
Требования выдачи	Устаревшие шаблоны	Расширения	Безопасность				
Совместимост	о Общие	Обработ	ка запроса				
Шифрование	Аттестация ключей	Имя субъекта	Сервер				
О Предоставляется в запросе Использовать данные о субъекте из существующих сертификатов для запросов обновления автоматической подачи заявок (*)							
Остроится на основе данных Active Directory Выберите этот параметр для повышения согласованности имен субъектов и упрощения администрирования сертификатов. Формат имени субъекта:							
Полное различаю	Полное различающееся имя ~						
Включить <u>и</u> мя электронной почты в имя субъекта Включить эту информацию в альтернативное имя субъекта: Имя электронной почты DNS-им <u>я</u>							
✓ Имя субъекта-службы (SPN)							
*Элемент управления отключен из-за <u>параметров совместимости.</u>							
	OK	Отмена При <u>м</u> ени	пъ Справка				

Для применения всех заданных свойств шаблона нажмите **Применить.** Далее нажмите **ОК** для выхода из свойств шаблона.

Новый шаблон отобразится в списке всех шаблонов.

🗟 Консоль шаблонов сертификатов — 🗆 🗙								
<u>Файл Действие Вид Справка</u>								
🗵 Шаблоны сертификатов (mosc	Отображаемое имя шаблона	Версия схемы	Версия	Назнач ^	Действия			
	🚇 Агент регистрации	1	4.1		Шаблоны сертификатов (🔺			
	🚇 Агент регистрации (компьютер)	1	5.1		Лополнительные лей			
	🗷 Агент регистрации Exchange (автоном	1	4.1		дополнительные деи у			
	🗷 Администратор	1	4.1		JaCarta user 🔺			
	🚇 Базовое шифрование EFS	1	3.1		Дополнительные дей 🕨			
	🕮 Веб-сервер	1	4.1					
	🕮 Вход со смарт-картой	1	6.1					
	🚇 Компьютер	1	5.1					
	🚇 Контроллер домена	1	4.1					
	🚇 Корневой центр сертификации	1	5.1					
	🚇 Маршрутизатор (автономный запрос)	1	4.1					
	🚇 Перекрестный центр сертификации	2	105.0					
	🚇 Подписывание кода	1	3.1					
	🕮 Подписывание отклика OSPC	3	101.0	Подпи				
	🕮 Подписывание списка доверия сертиф	1	3.1					
	🚇 Подчиненный центр сертификации	1	5.1					
	🚇 Пользователь	1	3.1					
	🕮 Пользователь Exchange	1	7.1					
	🚇 Пользователь со смарт-картой	1	11.1					
	🚇 Почтовая репликация каталога	2	115.0	Почто				
	🚇 Проверенный сеанс	1	3.1					
	🕮 проверка подлинности Kerberos	2	110.0	Провеј				
	🚇 Проверка подлинности контроллера д	2	110.0	Провеј				
	🚇 Проверка подлинности рабочей станц	2	101.0	Провеј				
	🗷 Только подпись Exchange	1	6.1					
	🚇 Только подпись пользователя	1	4.1					
	🚇 ЦС Exchange	2	106.0	Архива				
	🚇 Шифрование СЕР	1	4.1					
	JaCarta user	2	100.3	Защиц				
				~				
< >	<			>]			

Далее этот шаблон необходимо разрешить к выдаче. Для этого в консоли **Центр сертификации** щёлкните правой кнопкой по **Шаблоны сертификатов** и выберите **Создать -> Выдаваемый шаблон сертификата.**



© "Аладдин Р.Д.", 2018
В отобразившемся окне выберите шаблон JaCarta user (ранее созданный) и Arent регистрации (существовал по умолчанию, но не был разрешён к выдаче) нажмите OK.

📧 Включение шаблонов сертификатов	×
Выберите один шаблон сертификата для использовани: Примечание. Если созданный шаблон сертификата не о время, пока информация о шаблоне не будет реплициро	я в этом центре сертификации (ЦС). отображается в списке, подождите некоторое ована на все контроллеры домена.
Пе все шаолоны сертификатов в организации могут сы	ть доступны для вашего цс.
Имя	Назначение
R IPSec	IKE-посредник IP-безопасности
🚇 IPSec (автономный запрос)	IKE-посредник IP-безопасности
🖳 JaCarta user	Вход со смарт-картой, Проверка подлинности (
🗷 RAS-и IAS-серверы	Проверка подлинности клиента, Проверка под
🚇 Агент восстановления ключей	Агент восстановления ключей
🕮 Агент регистрации	Агент запроса сертификата
🚇 Агент регистрации (компьютер)	Агент запроса сертификата
🖳 🖳 Агент регистрации Exchange (автономный запрос)	Агент запроса сертификата
🚇 Вход со смарт-картой	Проверка подлинности клиента, Вход со смарт 🗸
A 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	- >
	ОК Отмена

Разрешённые шаблоны должны появиться в разделе Шаблоны сертификатов в консоли Центра сертификации.

🚟 ЦентрСертификации - [Корень консоли\Центр) сертификации (Локальный)\local-MOSCO	W-CA∖Шаблоны	серти — 🗆 🗙
\overline Файл <u>Д</u> ействие <u>В</u> ид <u>И</u> збранное <u>О</u> кно	<u>С</u> правка		_ 5 ×
🗢 🌩 🖄 📰 🔍 🗟 📑			
Корень консоли Корень консоли Сан-МоSCOW-СА Сотозванные сертификаты Выданные сертификаты Запросы в ожидании Неудачные запросы Шаблоны сертификатов	Имя Агент регистрации ЈаСата user Почтовая репликация каталога Проверка подлинности контролле проверка подлинности Кеrberos Агент восстановления EFS Базовое шифрование EFS Контроллер домена Веб-сервер Компьютер Пользователь Подчиненный центр сертификации Администратор	Назначение Агент запроса Вход со смарт- Почтовая репу Проверка под, Проверка под, В сос- Сос- Сос- Сос- Сос- Сос- Сос- Сос-	Действия Шаблоны сертификатов ▲ Дополнительные дей ↓

Подготовка шаблонов завершена.

Можно создать и разрешить к выдаче несколько шаблонов, если это требуется, например, с разными криптопровайдерами или разным сроком действия сертификата.

Выдача сертификатов

После настройки шаблонов можно перейти к непосредственному выпуску сертификата и записи его в память USB-токена или смарт-карты JaCarta PKI. Для этого необходимо, по аналогии с Центром Сертификации, открыть консоль Сертификаты.

Для этого выполните следующие действия.

Нажмите правой кнопкой меню Пуск выберите Выполнить -> mmc.



Файл Действие Вид Избранное Окно Справка Создать Ctrl+N Действия Открыть Ctrl+O Действия	- 8 ×
Создать Ctrl+N Открыть Ctrl+O	
Сохранить как Сохранить как Добавить или удалить оснастку Параметры Последний файл Выход	оли 🔺

В отобразившемся окне выберите Добавить или удалить оснастку.



	Поставшик	~		Корень консоли	Изменить расширения
	поставщик				rishening pacampennis
2 маршрутизация	Microsoft C				<u>У</u> далить
Монитор IP-безо	Microsoft C				
Общие папки	Microsoft C				
Папка	Microsoft C				Rebx
Планировщик за	(с) Корпора				Вниз
Просмотр событий	(с) Корпора		Добавить >		DING
Редактирование	. Microsoft C		-		
🛿 Редактор GPO ин	. Корпораци				
🛿 Редактор объек	Microsoft C				
🕻 Редактор управл	. Корпораци				
Результирующа	Microsoft C				
Сертификаты	Корпораци				
	(c) Koppop				

В следующем окне выберите моей учетной записи пользователя и нажмите Готово.

Оснастка диспетчера сертификатов	×
Эта оснастка всегда будет управлять сертификатами для: моей учетной записи пользователя учетной записи службы учетной записи компьютера 	
< <u>Н</u> азад Готово Отмена	3

Для удобства дальнейшего использования консоль можно сохранить по аналогии с консолью **Центр сертификации.**

÷.

Откройте консоль **Сертификаты,** которую сохранили ранее, щёлкните правой кнопкой по папке **Личное,** далее выберите **Все задачи -> Запросить новый сертификат.**

🚟 Консоль1 - [Корень консоли]	– 🗆 X
🚟 Файл Действие Вид Избранное Окно Справка	_ & ×
	,,
📔 Корень консоли Имя	Действия
Сертификаты - текущий пользователь	Корень консоли 🔺
>	Дополнительн 🕨
> 🛅 Все задачи > Поиск сертификатов	
Новое окно отсюда Запросить новый сертификат	
Обновить Импорт	
Справка Дополнительные операции >	
> 🧰 Доверенные лица	
> 📔 Поставщики сертификатов проверки под	
Доверенные корневые сертификаты сма	
Запросить новый сертификат от центра сертификации (ЦС) в этом домене	

Нажмите Далее.

	_		\times
🔄 Регистрация сертификатов			
Перед началом работы			
Следующие шаги помогут установить сертификаты, являющиеся цифровыми уч используемыми для подключения к беспроводным сетям, защиты контента, иден задач безопасности.	етными, нтифика	данными ции и ини	I, ЫХ
Прежде чем запрашивать сертификат, убедитесь, что:			
этот компьютер подключен к сети; имеются учетные данные, которые могут быть использованы для подтверждения получение сертификата.	і права н	a	
Да	лее	Отме	на

Выберете Агент регистрации и нажмите Заявка.

		_		×
🔄 Регистрация сертификатов				
Запрос сертификатов				
Вы можете запросить следующие т запросить, и нажмите кнопку "Заяв	типы сертификатов. Выберите сертифи зка".	каты, которые x	отите	
Политика регистрации Active I	Directory			^
🗌 JaCarta	🤨 Состояние: Доступно	Подробн	ости 👻	
Требуется больше данн для параметры парамет	ых для подачи заявки на этот сертифик ров.	ат. Щелкните зд	есь	
Aгент восстановления EFS	🤃 Состояние: Доступно	Подробн	ости 💙	
🖂 Агент регистрации	Остояние: Доступно	Подробн	ости 💙	
Д Администратор	Остояние: Доступно	Подробн	ости 💙	
				*
<u>П</u> оказать все шаблоны				
		<u>З</u> аявка	Отм	ена

		_		×
🔄 Pe	егистрация сертификатов			
	Выбор политики регистрации сертификатов			
	Политика регистрации сертификатов позволяет регистрировать сертификаты на заранее шаблонов сертификатов. Политика регистрации сертификатов уже могл	основан 1а быть н	ии заданн астроена	ных
	Настраиваемые администратором			
	Политика регистрации Active Directory			~
	Настраиваемые пользователем		Добави	пъ
		лее	Отме	на

Нажмите Готово.

			_		×
📮 Pei	гистрация сертификатов				
F	Результаты установки сертифик	атов			
	Следующие сертификаты были получені	ы и установлены на данном компьютере.			
	Политика регистрации Active Directo	ry			
	🖂 Агент регистрации	🗸 Состояние: Успешно	Подро	бности 🗸	
				<u>Г</u> отов	D

Сертификат Агента регистрации выпускается 1 раз. На том месте, где будут в дальнейшем выпускаться сертификаты, если мест (рабочих станций) будет несколько, на каждой необходимо выпустить сертификат Агента регистрации.

Выпуск сертификата на электронный ключ JaCarta

Откройте консоль сертификатов, которую сохранили ранее, щёлкните правой кнопкой по папке **Личное,** далее выберите **Все задачи -> Дополнительные операции -> Зарегистрироваться от имени.**

🚟 Консоль1 - [Корень консоли\Сертификаты - текуц	ций пользователь\Личное]	– 🗆 X
🚟 Файл Действие Вид Избранное Окно Сг	правка	_ 8 ×
🔶 🧼 🖄 📰 📋 🧔 🕞 🛛 🗾		· · · · · · · · · · · · · · · · · · ·
Корень консоли Сертификаты - текущий пользователь Сертификаты - текущий пользователь Сертификатов Сертификатов - Сертификатов - се	Гип объекта Сертификаты Поиск сертификатов Запросить новый сертификат	Действия Личное ▲ Дополнительн ▶
> 🧰 До Новое окно отсюда	Импорт	
Создать настраиваемый запрос	Дополнительные операции >	
Зарегистрироваться от имени		
Управление политиками регистрации		
Справка		
<		>
З&арегистрироваться от имени		

Нажмите Далее.

	_		×
🔄 Регистрация сертификатов			
Перед началом работы			
Следующие шаги помогут установить сертификаты, являющиеся цифровыми уче используемыми для подключения к беспроводным сетям, защиты контента, иден задач безопасности.	≞тными нтифика	даннымі ции и ин	и, ых
Прежде чем запрашивать сертификат, убедитесь, что:			
этот компьютер подключен к сети; имеются учетные данные, которые могут быть использованы для подтверждения получение сертификата.	права н	ia	
Дал	1ee	Отме	ена

Нажмите Далее.

	—	
Регистрация сертификатов		
Выбор политики регистрации сертификатов		
Политика регистрации сертификатов позволяет регистрировать заранее шаблонов сертификатов. Политика регистрации сертиф	сертификаты на основа икатов уже могла быть	нии заданны настроена.
Настраиваемые администратором		
Политика регистрации Active Directory		*
Настраиваемые пользователем		Добавить
	Лалоо	Отмена

В следующем окне нажмите Обзор.

	_		\times
🙀 Регистрация сертификатов			
Выберите сертификат агента регистрации			
Сертификат агента регистрации необходим для подписи запроса на сер пользователей. Нажмите кнопку "Обзор", чтобы найти сертификат под "Далее".	этификат от име писи, а затем щ	ени других целкните	
Consultance account			
Сертификат подписи:		<u>О</u> бзор	
		Отме	на

Выберите сертификат Агента регистрации, нажмите ОК.

Безопасн	ость Windows		×	
Подте	Подтверждение сертификата			
Подтвердите этот сертификат, нажав кнопку "ОК". Если это неправильный сертификат, нажмите кнопку "Отмена".				
<u>e</u> =	adm adm			
لـــــا	Издатель: local-MOS	COW-CA		
	Действителен с: 11.09.2017 по 11.09.2019			
	Просмотреть свойст	ва сертификата		
	ОК	Отмена		

Выберите шаблон, который ранее создали и разрешили к выдаче.

Запрос сертификатов			
Вы можете запросить следующие ти запросить, и нажмите кнопку "Дале	ппы сертификатов. Выберите сертифи e".	ікаты, которые хотите	
Политика регистрации Active Di	rectory		1
◉ JaCarta	Остояние: Доступно	Подробности 💙	
О Агент восстановления EFS	Остояние: Доступно	Подробности 💙	
Агент регистрации	Остояние: Доступно	Подробности 💙	
🔿 Администратор	Остояние: Доступно	Подробности 🗸	
🔿 Базовое шифрование EFS	Остояние: Доступно	Подробности 🗸	ł
0.7	() Состояния: Лостияно	Подробности 🗙	

Укажите пользователя, для которого сертификат будет выпущен и записан на электронный ключ. Для этого нажмите **Обзор.**

_]	×
🗐 Регистрация сертификатов			
Выберите пользователя			
Чтобы запросить сертификат от имени другого пользователя, введите его формальное доменное имя. Например, используйте формат "имя фамилия", "имя_пользователя" и "домен\имя_пользователя".	: имя ил ли	и	
Прежде чем запрашивать сертификат пользователя, убедитесь, что устройство, на кото должен быть установлен, подключено.	ором он	H	
Имя пользователя или псевдоним:			
	<u>0</u> 6	зор	
	(Отмена	1

В поле Введите имена выбираемых объектов укажите имя или часть имени пользователя, после чего нажмите Проверить имена.

Выбор: "Пользователь"		×
<u>В</u> ыберите тип объекта:		
"Пользователь"		<u>Т</u> ипы объектов
В с <u>л</u> едующем месте:		
local.test		<u>Р</u> азмещение
Введите <u>и</u> мена выбираемых объектов (<u>примеры)</u> :		
jsn		Проверить имена
Дополнительно	OK	Отмена

Если есть совпадения, система подставит полное имя пользователя, нажмите ОК.

Выбор: "Пользователь"	×
<u>В</u> ыберите тип объекта:	
"Пользователь"	<u>Т</u> ипы объектов
В с <u>л</u> едующем месте:	
local.test	<u>Р</u> азмещение
Введите имена выбираемых объектов (примеры):	
john snow (jsnow@local.test)	Проверить имена
Дополнительно	ОК Отмена

В следующем окне нажмите Заявка.

		_		×
🗐 P	регистрация сертификатов			
	Выберите пользователя			
	Чтобы запросить сертификат от имени другого пользователя, введите его форма доменное имя. Например, используйте формат "имя фамилия", "имя_пользоват "домен\имя_пользователя".	льное им еля" или	ия или	
	Прежде чем запрашивать сертификат пользователя, убедитесь, что устройство, н должен быть установлен, подключено.	на которо	м он	
	Имя пользователя или псевдоним:			
	LOCAL\jsnow		<u>О</u> бзор	
	<u>3</u> a	явка	Отме	на

Далее система запросит вставить электронный ключ и ввести PIN-код. Введите PIN-код пользователя и нажмите **Подтвердить.**

JaCarta: проверка доступа	<
JaCarta	
Введите пароль пользователя	
Сменить после проверки	
Отмена Подтвердить	

Если всё сделано верно, система отобразит Состояние: Успешно.

		—		\times
🔄 Регистрация сертификатов				
Результаты установки о	сертификатов			
Следующие сертификаты бы.	ли получены и установлены на данном компьюте	epe.		
Политика регистрации Ас	tive Directory			
JaCarta	У Состояние: Успешно	Подр	обности	•
	<u>С</u> ледующий пользов	ватель	<u>З</u> акры	ыть

Сразу же можно выпустить сертификат следующему пользователю на следующий электронный ключ.

Заводить таким образом тысячи и даже сотни сотрудников крайне неудобно, для решения этой задачи компания **"Аладдин РД"** разработала специальное программное обеспечение — систему управления USB-токенами и смарт-картами **JMS (JaCarta Management System)** — сертифицированная корпоративная система управления жизненным циклом средств аутентификации и электронной подписи. Подробная информация и документация доступна на сайте компании https://www.aladdin-rd.ru/catalog/jms/index

Проверка работоспособности

В качестве проверки выполните просмотр содержимого электронного ключа и совершите вход в домен по сертификату на электронном ключе.

Просмотр сертификата через Единый Клиент JaCarta

Запустите **Единый Клиент JaCarta**, подсоедините смарт-карту или USB-токен с сертификатом, введите PIN-код и убедитесь, что **сертификат и закрытый ключ** успешно выпущены и находятся на электронном ключе **JaCarta**.

🔗 Единый Клиент JaCarta		– 🗆 X
Единый Клие	нт JaCarta	Аладдин
	JaCarta	
JaCarta	Информация о токене РКІ	
	Операции с приложением	
	Установить PIN-код пользователя Сменить PIN-код администратора Создать запрос на сертификат Разблокировать PIN- код пользователя Q Инициализировать	
	Ключи и сертификаты	ĽO
	 ¥ Le-JaCarta-238749ba-40b1-4af9-845-40381 ☐ john snow 1.6 Кбайт 3акрытый ключ 	
🔅 Настройки		
С Переключиться в режим пользователя		

Дважды щёлкнув по сертификату, можно получить его общие свойства (для чего предназначен, срок действия), состав (серийный номер, используемые алгоритмы и т.д.), путь сертификации (строится ли цепочка доверия) и статус (действителен или не действителен).

🙀 Сертификат	Х	🖬 Сертификат 🛛 🗙
Общие Состав Путь сертификации		Общие Состав Путь сертификации
Сведения о сертификате Этот сертификат предназначается для: • Защищает сообщения электронной почты • Подтверждает удаленному компьютеру идентификацию вашего компьютера • Вход со смарт-картой	-	Путь сертификации
Кому выдан: john snow		
Кем выдан: local-MOSCOW-CA		Просмотр сертификата
Действителен с 12.09.2017 по 12.09.2019		<u>С</u> остояние сертификата:
<u>Установить сертификат</u> Заявление поставщика		Этот сертификат действителен.
ОК		ОК

Вход в домен по сертификату на электронном ключе

Перейдите на пользовательскую рабочую станцию под управлением операционной системы Windows 10, подключите USB-токен или смарт-карту и загрузите ОС. Далее выберите Параметры входа (Sign-in options) вход по смарт-карте и введите PIN-код.

Данная клиентская рабочая станция должна входить в домен, согласно описанию демо-стенда.



По завершении аутентификации вы попадёте в операционную систему, используя только смарт-карту и зная её PIN-код.



Парольная аутентификация в настоящем примере не используется, более того её можно вообще отключить, оставив только один вариант аутентификации — аутентификация по смарт-карте.



На этом настройка двухфакторной аутентификации в домен Windows завершена.

После аутентификации в домен смарт-карты или USB-токены можно использовать внутри операционной системы в различных сценариях с различным программным обеспечением которое поддерживает работу с электронными ключами. На сайте "Аладдин Р.Д." есть серия интеграционных инструкций по взаимодействию электронных ключей с различным прикладным ПО.

Дополнительные возможности

Опционально, для повышения общего уровня безопасности, можно полностью или выборочно (для конкретного пользователя) отключить аутентификацию в домене по паролям, а также настроить автоматическую блокировку рабочей станции или выход из операционной системы при отсоединении электронного ключа JaCarta PKI.

Отключение возможности аутентификации по паролям

Отключение аутентификации по паролям может быть произведено в рамках конкретного пользователя или всех машин в домене.

После выполнения данных настроек войти в систему можно будет только с использованием сертификата, выпущенного на электронный ключ JaCarta PKI.

Запрет аутентификации по паролю для пользователя

Запустите консоль управления Пользователи и компьютеры Active Directory.

Для этого нажмите Пуск -> Средства администрирования.



1	.0

🎼 🛃 📄 🖛	Средства работы с ярлыками Администри	ирование	– 🗆 X				
Файл Главная	Поделиться Вид Управление		~ 🕐				
 							
3 F - X	Имя	Дата изменения	Тип				
🖈 Быстрый доступ	Terminal Services	16.07.2016 16:23	Папка с файлами				
📃 Рабочий стол	🖈 🔜 Active Directory - домены и доверие	16.07.2016 16:20	Ярлык				
👆 Загрузки	🖈 Active Directory — сайты и службы	16.07.2016 16:19	Ярлык				
🚆 Документы	🖈 🍰 DNS	16.07.2016 16:19	Ярлык				
📰 Изображения	Брандмауэр Windows в режиме повышенной безопасн	16.07.2016 16:18	Ярлык				
sc	🚋 Диспетчер серверов	16.07.2016 16:19	Ярлык				
🔜 выдача на карт	у 💦 Диспетчер служб IIS	16.07.2016 16:19	Ярлык				
- seide is is web.	👧 Инициатор iSCSI	16.07.2016 16:18	Ярлык				
💻 Этот компьютер	🌇 Источники данных ODBC (32-разрядная версия)	16.07.2016 16:18	Ярлык				
🔿 Сеть	🌇 Источники данных ODBC (64-разрядная версия)	16.07.2016 16:18	Ярлык				
	🔝 Конфигурация системы	16.07.2016 16:18	Ярлык				
	📠 Локальная политика безопасности	16.07.2016 16:19	Ярлык				
	🎦 Модуль Active Directory для Windows PowerShell	16.07.2016 16:19	Ярлык				
	🛞 Монитор ресурсов	16.07.2016 16:18	Ярлык				
	🎦 Оптимизация дисков	16.07.2016 16:18	Ярлык				
	🔚 Очистка диска	16.07.2016 16:19	Ярлык				
	😥 Планировщик заданий	16.07.2016 16:18	Ярлык				
	📔 Пользователи и компьютеры Active Directory	16.07.2016 16:20	Ярлык				
	🌆 Просмотр событий	16.07.2016 16:18	Ярлык				
	📝 Редактирование ADSI	16.07.2016 16:19	Ярлык				
		16.07.2016.16-10	0				
Элементов: 34 🛛 Выбран 1 элемент: 1,13 КБ 🖉 📰							

Откройте Пользователи и компьютеры Active Directory.

Находясь в лесу домена, откройте Users, выберите пользователя, щёлкнув на нём правой кнопкой.

Откройте вкладку **Учётная запись** и в параметрах учётной записи отметьте **Для интерактивного входа в сеть нужна смарт-карта**, нажмите **Применить**, нажмите **ОК**.

Файл Действие Вид Справка Фользователи и компьютеры Сокраненные запросы Сокраненные запросы Сокраненные запросы Сокраненные запросы Соспрантея Сокраненные запросы Сопользователь Сокраненные запросы Сопользователь Сокраненные запросы Сокраненные учетная запись Среда Сеансы Удаленное управление Сокраненные управление Сокраненные управление Сокраненные управление Сокраненные учетная запись Среда Сеансы Удаленное управление Сокраненные управление Сокраниенные сакрами не кожет быть делегирована Сокраниенные учетной записи: Сокраненные учетной записи Сокраненные учетной записи Сокраненные учетной записи Сокраненные учетные запись Сокрана Сокраненные учетной записи Сокраненные учетной записи Сокраненные учетное важная и не может быть делегирована Сокранентыя учетной записи Сокраненты интерактивного входа в сеть нужна смарт карта Сокранентые учетной записи Сок действия учетной записи Сок Сотмена Применить Справка	📔 Active Directory - пользователи и ко	🚽 Active Directory - пользователи и компьютеры							
	Файл Действие Вид Справка	Файл Действие Вид Справка							
Пользователи и компьютеры Сохраненные запросы Вultin Вultin CorriginSecutityPrincipal: Managed Service Accour Users Managed Service Accour Users Managed Service Accour Users Managed Service Accour Users Managed Service Accour Users Managed Service Accour Cocure Appec Verman samues Pro Ada Managed Service Accour Doduue Appec Verman samues Pro Ada Managed Service Accour Doduue Appec Verman samues Pro Cocure Appec Verman samues Pro Ada Managed Service Accour Doduue Appec Verman samues Pro Ada Managed Service Accour Doduue Appec Verman samues Pro Ada Managed Service Accour Cocure Appec Verman samues Pro Ada Managed Service Accourt Pro Ada Managed Service Accourt Cocure Appec Verman samues Pro Ada Managed Service Accourt Cocure Appec Verman samues Pro Ada Managed Service Accourt Managed Service Accourt Ada Managed Service Accourt Pro Ada Managed Service Accourt Pro Ada Managed Service Accourt Pro Ada Managed Service Accourt Pro Ada Managed Service Accourt Managed Service Accourt Managed Service Accourt Pro Ada Managed Service Accourt Pro Ada Managed Service Accourt Pro Ada Managed Service Accourt Pro Ada Managed Service Accourt Pro Ada Ada Managed Service Accourt Pro Ada Managed Service Accourt Pro Ada Managed Service Accourt Pro Ada Ada Managed Service Accourt Pro Ada Ada Managed Service Accourt Pro Ada Ada Managed Service Accourt Pro Ada Ada Managed Service Accourt Pro Ada Ada Ada Managed Service Accourt Pro Ada Ada Ada Managed Service Accourt Ada Ada Ada Ada Ada Ada Ada Ada	🗢 🔿 🙍 🔂 😽 🔯	⇐ ⇒ 2 💼 🖌 🗈 🗙 🖼 @ 🕞 🛛 🖬 🖏 📚 🏗 🍸 💆 🎘							
С С С С С С С С С С С С С С С С С С С	Image: Second secon	Ima Тип Описание adm adm Пользователь Учетная запись пользо Dof Свойства: john snow ? Drs Свойства: john snow ? Drs Свойства: john snow ? Drs Свойства: john snow ? Pro Общие Адрес Учетная запись Профиль Солов Профиль служб удаленных рабочих столов СОМ+ Общие Адрес Учетная запись Профиль Телефоны Организация Ада Имя входа пользователя: [snow @local.test Ада Имя входа пользователя (пред-Windows 2000): LOCAL\ [snow LOCAL\ [snow @local.test ~ Ада Время входа Вход на Bxод на Гос Гос Разблокировать учетную запись _ Гру Параметры учетной записи: _ _ Иза Энн интерактивного входа в сеть нужна смарт карта _ Учетная запись важна и не может быть делегирована _ _ Учетная запись _ _ _ _ Ког Оск. действия учетной записи<							
	< >								

Теперь вход по паролюдля этого пользователя будет невозможен, всегда будет требоваться смарткарта или USB-токен.



Запрет аутентификации по паролю всем компьютерам домена

Для выполнения этой настройки необходимо отредактировать групповые политики домена. Для этого откройте консоль **Редактор управления групповыми политиками.**

Нажмите правой кнопкой меню Пуск, выберите Выполнить -> mmc.

a			
Программы и компоненты			
Управление электропитанием			
Просмотр событий			
Система			
Диспетчер устройств			
Сетевые подключения			
Управление дисками			
Управление компьютером			100
Командная строка			
Командная строка (администратор)			
Диспетчер задач			
Панель управления			
Проводник			
Найти			
Выполнить			
Завершение работы или выход из системы			
Defermit con			

Нажмите ОК.

💷 Выполни	ть Х
	Введите имя программы, папки, документа или ресурса Интернета, которые требуется открыть.
<u>О</u> ткрыть:	mmc ~
	ОК Отмена Об <u>з</u> ор

	Консоль1 - [Корень консоли]			– 🗆 ×
-	Файл Действие Вид Избранное	Окно Справк	a	_ 8 ×
	Создать	Ctrl+N		
	Открыть	Ctrl+O		Действия
	Сохранить	CTRL+S ұля отображения в этом виде.	Корень консоли 🔺	
	Сохранить как		Дополнительн 🕨	
	Добавить или удалить оснастку	CTRL+M		
	Параметры			
	Последний файл			
	Выход			
Поз	воляет добавлять оснастки в консоль ил	и удалять их.		

В отобразившемся окне выберите Добавить или удалить оснастку...

В следующем окне выберите **Редактор управления групповыми политиками,** нажмите **Добавить,** нажмите **ОК.**

Добавление и удаление	соснасток			×		
Вы можете выбрать осна расширяемых оснасток м	Вы можете выбрать оснастки для этой консоли из доступных на компьютере оснасток и затем настроить их. Для расширяемых оснасток можно настроить требуемое расширение.					
Доступные <u>о</u> снастки:			В <u>ы</u> бранные оснастки:			
Оснастка	Поставщик	۸	🔛 Корень консоли	Изменить рас <u>ш</u> ирения		
🚊 Маршрутизация 🜏 Монитор IP-безо	Microsoft C Microsoft C			<u>У</u> далить		
👸 Общие папки 🧰 Папка	Microsoft C Microsoft C			Вверх		
Планировщик за Просмотр событий	(с) Корпора (с) Корпора		Добавить >	В <u>н</u> из		
Редактирование Редактор GPO ин Водоктор GPO ин	Місгозоft С Корпораци					
Редактор оовек	Корпораци					
🗐 Сертификаты	Корпораци					
🖗 Система архивац	(с) Корпора	¥		Допо <u>л</u> нительно		
Описание:	Описание:					
Эта оснастка позволяет редактировать объекты групповой политики, которые могут ссылаться на сайт, домен или подразделение в Active Directory либо храниться на компьютере.						
			Γ	ОК Отмена		

Нажмите Обзор и выберите объект групповой политики.

Выбор объекта групповой политики	×
Мастер групповой политики	
	Объекты групповой политики могут храниться как в Active Directory, так и на локальном компьютере. Для выбора объекта воспользуйтесь кнопкой "Обзор". Объект групповой политики:
	< <u>Н</u> азад Готово Отмена

Укажите Default Domain Policy и нажмите OK.

Если указать Domain Controller, изменения отработают только для контроллера домена.

Поиск объекта групповой политики	?	×
Домены/Подразделения Сайты Все		
Поиск в: 🛐 local.test 🗸 🖉	" 📑 📰 🔻	
Домены, подразделения и связанные объекты групповой поли	тики:	
Имя Домен		
Controllers local test		
	ОКО	тмена

Выбор объекта групповой политики	×
Мастер групповой политики	
	Объекты групповой политики могут храниться как в Active Directory, так и на локальном компьютере. Для выбора объекта воспользуйтесь кнопкой "Обзор". Объект групповой политики:
	Default Domain Policy
	<u>О</u> бзор
	Разрешить изменение фокуса "Оснастки групповой политики" при запуске из командной строки. Применяется только при сохранении консоли.
	< Назад Готово Отмена

Нажмите ОК.

Добавление и удаление	соснасток			×	
Вы можете выбрать оснастки для этой консоли из доступных на компьютере оснасток и затем настроить их. Для расширяемых оснасток можно настроить требуемое расширение.					
Доступные <u>о</u> снастки:			В <u>ы</u> бранные оснастки:		
Оснастка	Поставщик	^	Корень консоли	Изменить расширения	
🚊 Маршрутизация	Microsoft C		📕 Политика Default Domain Polic	Vasauti	
Монитор IP-безо	Microsoft C			<u>у</u> далить	
👸 Общие папки	Microsoft C				
📔 Папка	Microsoft C			Вверх	
🕑 Планировщик за	(с) Корпора			During	
🛃 Просмотр событий	(с) Корпора		Лобавить Х	В <u>н</u> из	
📝 Редактирование	Microsoft C		Foodpiller		
🧾 Редактор GPO ин	Корпораци				
🧾 Редактор объек	Microsoft C				
🗾 Редактор управл	Корпораци				
📕 Результирующа	Microsoft C				
🔄 Сертификаты	Корпораци				
🚻 Система архивац	(с) Корпора	~	< >	Допо <u>л</u> нительно	
-					
Описание:					
Эта оснастка позволяет редактировать объекты групповой политики, которые могут ссылаться на сайт, домен или					
подразделение в Астіче	Directory Judo 3	ран	иться на компьютере.		
				01/	
				ОК Отмена	

Открывшуюся консоль можно сохранить. Нажав **Файл -> Сохранить как.** В качестве имени укажите **Default Domain Policy.**

🚟 Консоль1 - [Корень консоли]	– 🗆 X
🚟 Файл <u>Д</u> ействие <u>В</u> ид <u>И</u> збранное <u>О</u> кно <u>С</u> правка	_ & ×
Корень консоли Имя	Действия
> 🧃 Политика Default D 🔲 Политика Default Domain Poli	Корень консоли 🔺
	Дополнительн 🕨

Далее разверните политику и перейдите в параметры безопасности:

Политика Default Domain Policy -> Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности

Дважды щёлкните по Интерактивный вход в систему: Требовать смарт-карту.

 Действие Вид Избранное Окно Справка Действия Де	🚟 Консоль1 - [Корень консоли\Политика Defa	ılt Domain Policy [moscow.local.test]\Конфигурация компьютера	\Политики\К	– 🗆 🗙
 Политика Default Domain Policy [mosc Политика Default Domain Policy [mosc Конфигурация компьютера Контерактивный вход в систему: пороговое число неудачи. Контерактивный вход в систему: пребевать комарт-карту Контерактивный вход в систему: пороговое число неудачи. Контерактивный вход в систему: пребевать смарт-карту Контерактивный вход в систему: требовать смарт-карту Контера	🚟 <u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>И</u> збранное <u>О</u> кно	о <u>С</u> правка		_ & ×
 Политика Default Domain Policy [mosc Конфигурация компьютера Конфигурация программ Конфигурация программ Конфигурация программ Конфигурация windows Политика разрешения и Конфигурация Windows Политика зудита Политика учетных за Параметры безопа Конфигурация windows Политика зудита Политика зудита Политика зудита Параметры безопа Митерактивный вход в систему: поведение при извлечен Не опре Интерактивный вход в систему: количество предыдущих Не опре Интерактивный вход в систему: поведения при извлечен Не опре Интерактивный вход в систему: поведения дл Не опре Интерактивный вход в систему: порсовать соедения дл Не опре Интерактивный вход в систему: порсовать соедения для по Не опре Интерактивный вход в систему: пребовать сомпьют Не опре Интерактивный вход в систему: пребовать пороверки на к Не опре Интерактивный вход в систему: пребовать сомпьют Не опре Интерактивный вход в систему: пребовать сомпьют Не опре Интерактивный вход в систему: пребовать сомпьют Не опре Интерактивный вход в систему: пребовать пороверки на к Не опре Интерактивный вход в систему: пребовать сомпьют Не опре Интерактивный вход в систему: пребовать сомпьют Не опре Интерактивный вход в систему: пребовать сомпьют Не опре Интерактивный вход в систему: пребовать пороверки на к Не опре Интерактивный вход в систему: пребовать пороверки дадиниистратора Конслоь восстановления: разрешить ватоматический вход ададиниистратора Конслоь восстановления: разрешить измора уч	← → 2 □ × □ × □ ↓ 2 □			Land Carlos Carl
 Конфигурация компьютера Политики Конфигурация программ Конфигурация программ Конфигурация программ Конфигурация программ Конфигурация и программ Конфигурация Vindows Политика разрешения и Сценарии (запуск/завер Нараметры безопасност Параметры безопасност Политики учетных за Конфигурация и интерактивный вход в систему: заголовок сообщения для. Не опре Не опре Параметры безопасност Параметры безопасност Митерактивный вход в систему: половокать пользовате. Не опре Параметры безопасност Митерактивный вход в систему: пороговое число неудач. Не опре Митерактивный вход в систему: предоларогов компьют. Митерактивный вход в систему: требовать проверки на к	🗸 🗐 Политика Default Domain Policy [mosc 🔺	Политика	Парамет ^	Действия
🗧 п ¥ 🛛 🤤 Контроллер домена: требование цифровой подписи для Не опре, ¥	 Политика Default Domain Policy [mosc Конфигурация компьютера Конфигурация программ Конфигурация программ Конфигурация Windows Конфигурация Windows Конфигурация Windows Конфигурация Windows Конфигурация Windows Конфигурация Windows Сценарии (запуск/завері Параметры безопасност Политики учетных за Политики учетных за Политики учетных за Политики учетных за Политика аудита Политика аудита Параметры безоп Журнал событий Конфигуриние службы Реестр Файловая система Брандмаузр Windows Политики открытого Политики открытого 	Политика Доступ к сети: Разрешить трансляцию анонимного SID в Завершение работы: очистка файла подкачки виртуальн Завершение работы: разрешить завершение работы сис Интерактивный вход в систему: поведение при извлечен Интерактивный вход в систему: заголовок сообщения дл Интерактивный вход в систему: количество предыдущих Интерактивный вход в систему: напоминать пользовател Интерактивный вход в систему: напоминать пользовател Интерактивный вход в систему: не отображать последне Интерактивный вход в систему: пе отображать сведения о п Интерактивный вход в систему: пребовать нажатия СТ Интерактивный вход в систему: пребовать нажатия СТ Интерактивный вход в систему: пребовать проверки на к Интерактивный вход в систему: пребовать проверки на к Интерактивный вход в систему: требовать проверки на к Интерактивный вход в систему: требовать проверки на к Интерактивный вход в систему: требовать проверки на к Кинет сети Microsoft: использовать цифровую подпись Клиент сети Microsoft: использовать цифровую подпись Клиент сети Microsoft: отправлять незащифрованный па Консоль восстановления: разрешить автоматический вход Консоль восстановления: разрешить копирование диске Контроллер домена: запретить изменение пароля учетн Контроллер домена: требование цифровой подписи для	Парамет ^ Отключи Не опре, Не опере, Не опере, Не опере, Не опере, Не опере,	Действия Параметры безопа ▲ Дополнительн ▶ Интерактивный вхо ▲ Дополнительн ▶

В отобразившемся окне отметьте **Определить следующий параметр политики**, укажите **Включён**. Нажмите **Ок**.

Свойства: Интерактивный вход в о	истему: требовать с	?	×
Параметр политики безопасности	Объяснение		
Интерактивный вход в сис	тему: требовать смарт-ка	рту	
Определить следующий парам	етр политики:		
Включен			
<u>О</u> тключен			
	ОК Отмена	Прим	енить

Для того, чтобы обновлённая политика начала действовать немедленно, необходимо её обновить.

Для этого выполните следующее.

Откройте командную строку. Пуск -> Выполнить -> cmd

💷 Выполни	ть Х
	Введите имя программы, папки, документа или ресурса Интернета, которые требуется открыть.
<u>О</u> ткрыть:	<mark>cmd</mark> ~
	ОК Отмена Обзор

В открывшемся окне введите gpupdate /force.



Командную строку можно закрыть.

Перейдите на рабочую станцию и проверьте статус службы **Политика удаления смарт-карт** (ScPolicySvc).

Пуск -> Панель управления -> Администрирование -> Службы

Служба должна быть в статусе Автоматически.

Если всё настроено верно, и политика уже обновлена, вход по паролю будет невозможен, всегда будет требоваться смарт-карта или USB-токен.



1.0

Автоматическое блокирование рабочей станции и выход из операционной системы при отсоединении JaCarta PKI

Существует возможность настроить автоматическое блокирование рабочей станции или автоматический выход из системы при отсоединении **JaCarta PKI**. То есть, отходя от рабочего места и забирая с собой токен или смарт-карту, пользователь автоматически заблокирует систему или вообще выйдет из системы.

Для настройки этой политике выполните следующее.

Откройте ранее сохранённую консоль (Default Domain Policy).

Далее разверните политику и перейдите в параметры безопасности:

Политика Default Domain Policy -> Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности

Дважды щёлкните по Интерактивный вход в систему: поведение при извлечении смарт-карты.

В отобразившихся свойствах выберите **Блокировка рабочей станции** или **Принудительный выход из** системы, в зависимости от желаемого сценария. Далее нажмите **Применить**, нажмите **ОК**.

Свойства: Интерактивный вход в систему: поведение п ? 🛛 🗙	
Параметр политики безопасности Объяснение	
Интерактивный вход в систему: поведение при извлечении смарт-карты	
Определить следующий параметр политики	
Нет действия 🗸	
Нет действия	
Блокировка рабочей станции Принулительный выход из системы	
Отключение в случае удаленного сеанса служб удаленных рабочи	
ОК Отмена При <u>м</u> енить	

Для того, чтобы обновлённая политика начала действовать немедленно, необходимо её обновить.

Для этого выполните следующее.

Откройте командную строку. Пуск -> Выполнить -> cmd

🖅 Выполни	пь Х
	Введите имя программы, папки, документа или ресурса Интернета, которые требуется открыть.
<u>О</u> ткрыть:	cmd ~
	ОК Отмена Обзор

В открывшемся окне введите gpupdate /force.



Командную строку можно закрыть.

Перейдите на рабочую станцию и проверьте статус службы Политика удаления смарт-карт (ScPolicySvc).

Пуск -> Панель управления -> Администрирование -> Службы

Служба должна быть в статусе Автоматически.

Если всё настроено верно, и политика уже обновлена, при отсоединении **JaCarta PKI** от рабочей станции произойдет автоматическая блокировка или выход из системы (в зависимости от настройки политики).

Организация VPN-соединения для доступа к информационным ресурсам

VPN (Virtual Private Network) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений).

Компания Microsoft имеет свою реализацию VPN-технологии в рамках Windows Server, а компания "Аладдин Р.Д." предоставляет реализацию двухфакторной аутентификации на VPN-шлюзе. Это обеспечивает дополнительную безопасность пользователей, работающих в виртуальной сети. Сотрудники, желающие использовать личные устройства (такие как ноутбуки, портативные ПК и планшеты) для подключения к корпоративным сетям, когда они не присоединены к домену, представляют высокий интерес для современного бизнеса. Возможность подключения к виртуальной частной сети (VPN), открывающей удалённый доступ к корпоративной сети, предусмотрена для всех устройств на базе Windows. Настоящий документ в полном объёме описывает настройку VPN-шлюза и доступа в защищённую сеть с использованием электронного ключа JaCarta PKI.

Описание демо-стенда

Демо-стенд состоит из следующих компонентов.

Сервер

Windows Server 2016 Datacenter с установленным программным обеспечением Единый Клиент JaCarta и настроенными ролями серверов Active Directory и Active Directory Certificate Services.

Роль шлюза VPN будет настроена на этом же сервере в рамках настоящего документа. Опционально можно установить на отдельный от AD и CS сервер.

Подробное руководство об установке и настройке Active Directory Certificate Services доступно в документе — "JaCarta PKI для аутентификации в домене Windows Server 2016", который размещён на официальном сайте "Аладдин Р.Д.", в разделе "Интеграционные инструкции" — https://www.aladdin-rd.ru/support/guides.

Клиент

Не входящая в домен рабочая станция — Windows 10 с установленным программным обеспечением Единый Клиент JaCarta.

Ход настройки

Настройка происходит на сервере и клиенте, делится на следующие этапы.

На сервере:

•установка роли IIS (Web-сервер);

- •запрос сертификата для IIS сервера;
- •установка и настройка компонента Удалённый доступ, Маршрутизация;
- •назначение прав на удалённый доступ для пользователей.

На клиенте:

создание VPN-подключения;проверка работоспособности.

Установка роли IIS (Web-сервер) и запрос сертификата для IIS сервера

Для организации VPN-соединения с аутентификацией по смарт-картам необходима роль Webсервера и сертификат для этого сервера.

Важно, чтобы сертификат был выпущен до установки и настройки маршрутизации, политик сети и доступа.

Установка роли IIS (Web-сервер)

Если ранее на сервере была установлена роль IIS, перейдите к следующему разделу. В противном случае, установите компонент. Для этого выполните следующие действия.

Нажмите Пуск -> Диспетчер серверов.



В отобразившемся окне выберите Управление -> Добавить роли и компоненты.



Отобразится окно мастера добавления ролей и компонентов, для продолжения нажмите Далее.

ᡖ Мастер добавления ролей и компонентов				×
Перед началом р	работы	KOHE4H mosc	НЫЙ СЕРВ cow.local.te	EP est
Перед началом работы Тип установки	Этот мастер поможет вам установить роли, службы ролей или компоненты. Опр нужно установить, на основании потребностей своей организации, таких как об документам или размещение веб-сайта.	оеделит ощий до	е, что оступ к	
Выбор сервера Роли сервера	Чтобы удалить роли, службы ролей или компоненты: Запустить мастер удаления ролей и компонентов			
Компоненты Прежде чем вы продолжите, убедитесь, что выполнены следующие задачи: Подтверждение • Учетная запись администратора защищена надежным пародем.				
Результаты	 Настроены сетевые параметры, такие как статические IP-адреса Установлены новейшие обновления безопасности из Центра обновления Win Если вам требуется проверить, выполнены ли какие-либо предшествующие нес условия, закройте мастер, выполните необходимые шаги и запустите мастер сни Чтобы продолжить, нажмите кнопку "Далее". Пропускать эту страницу по умолчанию 	dows обходим ова.	лые	
	< <u>Н</u> азад <u>Далее ></u> <u>У</u> станов	ить	Отмена	a

В следующем окне выберите Установка ролей и компонентов.

re-	Мастер добавления ролей и к	сомпонентов	_		×
	Выбор типа уста	НОВКИ	KOHE4 mos	НЫИ СЕРВ cow.local.t	est.
	Перед началом работы	Выберите тип установки. Вы можете установить роли и компоненты на работак компьютера, на виртиальной машине или на автономном виртиальном устгол	ощем ф	изическа	ом
	Тип установки	компьютере, на виртуальной машине или на автономном виртуальном жестком	и диске	(viib).	
	Выбор сервера	Установка ролей или компонентов			
	Роли сервера	Настроите один сервер путем добавления ролеи, служб ролеи и компоненто	в.		
	Компоненты	🔘 Установка служб удаленных рабочих столов			
	Полтвержление	Установите службы ролей для инфраструктуры виртуальных рабочих столов	(VDI), ч	тобы	
		создать развертывание на основе виртуальных компьютеров или сеансов.			
		< <u>Н</u> азад <u>Далее ></u> <u>У</u> станов	ить	Отмен	a

Отобразится окно добавления новых ролей, выберите Веб-сервер (IIS) и нажмите Далее.

ᡖ Мастер добавления ролей и ко	мпонентов	_		×
Выбор ролей сер	вера	KOHE4 bravo	IНЫЙ CEPE s.westeros.)EP loc
Перед началом работы	Выберите одну или несколько ролей для установки на этом сервере.			
Тип установки	Роли Описание			
Выбор сервера Роли сервера Компоненты Подтверждение Результаты	DHCP-сервер DNS-сервер DNS-сервер Hyper-V Arrecтация работоспособности устройств Be6-сервер (IIS) Aomenhale службы Active Directory Pexum Windows Server Essentials Ceresoй контроллер Cлужбы опекуна узла Cлужбы Active Directory oблегченного доступа к Cлужбы MultiPoint Cлужбы MultiPoint Cлужбы печати и документов Cлужбы печати и доступа Cлужбы печати и доступа Cлужбы печати и доступа Cлужбы печати и доступа Cлужбы сертификатов Active Directory Cлужбы сертификатов Active Directory Cлужбы удаленных рабочих столов Cлужбы управления правами Active Directory	предос: ввляемул ю инфр ій.	тавляет ю и аструкту	у
	< <u>Н</u> азад Д <u>а</u> лее > Устано	БИТЬ	Отмен	a

В отобразившемся окне нажмите Добавить компоненты.



В отобразившемся окне нажмите Далее.

📥 Мастер добавления ролей и к	сомпонентов	-		×
Роль веб-сервер	ba (IIS)	KOHE4 bravo	IНЫЙ CEPE s.westeros.	BEP loc
Перед началом работы Тип установки Выбор сервера Роли сервера Компоненты	Веб-серверы устанавливаются на компьютерах, которые позволяют совместно информацию в Интернете, а также получать доступ через интрасети и экстрасе сервера включает службы IIS 10.0 с улучшенной безопасностью, диагностикой администрированием, унифицированную веб-платформу, которая объединяет платформу WCF.	исполь ти. Ролг и IIS 10.0	зовать ь веб- , ASP.NET	Ги
Роль веб-сервера (IIS) Службы ролей Подтверждение Результаты	 The default installation for the Web Server (IIS) role includes the installation of ro enable you to serve static content, make minor customizations (such as default d errors), monitor and log server activity, and configure static content compression 	le servic ocumen	es that ts and H	ТТР
	Дополнительные сведения о веб-сервере IIS			
	< <u>Н</u> азад Далее > Установ	вить	Отмен	a

В отобразившемся окне **Службы ролей** выбранные параметры можно оставить по умолчанию. Нажмите **Далее.**

📥 Мастер добавления ролей и к	сомпонентов		-		×
Выбор служб ро	ЛЕЙ Выберите службы ролей для установки для Веб-сервер (IIS).		KOHE4 bravos	НЫЙ СЕРЕ s.westeros.	BEP loc
Перед началом расоты Тип установки Выбор сервера	Службы ролей	Описание			
Роли сервера Компоненты	 ✓ Веб-сервер ▲ ✓ Безопасность ✓ Фильтрация запросов □ Редлес и огланичения домена 	вео-сервер пред поддержку веб-с дополнительно г расширений ASP	оставля айтов І поддеря NET, А	^{нет} HTMLи кку SPивеб	-
Роль веб-сервера (IIS) Службы ролей Полтверж ление	Авторизация URL-адреса Дайджест-проверка подлинности Обычная проверка подлинности	сервера. Этот ве использовать для внутреннего или сайта либо для п	б-серве я разме внешн редоста	ер можно ещения его веб- авления	D
Результаты	Проверка подлинности к пооказ Проверка подлинности с сопоставление Проверка подлинности с сопоставление Централизованная поддержка SSL-серти	разработчикам с приложений на с технологий.	реды с основе	оздания веб-	
	 С Исправность и диагностика Ведение журнала НТТР Ведение журнала ODBC Монитор запросов Настраиваемое ведение журнала Средства ведения журнала Трассировка 				
	 К. Ортика фолктики Н.П.Б. К. С. С.				
	< <u>Н</u> азад Д <u>а</u> лее з	> Установ	ить	Отмен	a

Отметьте Автоматический перезапуск конечного сервера и нажмите Установить.

📥 Мастер добавления ролей и ко	мпонентов	_		×
Подтверждение у	становки компонентов	KOHE4H bravos.	НЫЙ СЕРВІ .westeros.le	EP DC
Перед началом работы Тип установки	Чтобы установить на выбранном сервере следующие роли, службы ролей или нажмите кнопку "Установить".	компоне	енты,	
Выбор сервера	Автоматический перезапуск конечного сервера, если требуется			
Роли сервера	На этой странице могут быть отображены дополнительные компоненты (напри администрирования) так как они были выбраны автоматически. Если вы не хот	мер, сре ите уста	едства навлива	ть
Компоненты	эти дополнительные компоненты, нажмите кнопку "Назад", чтобы снять их флах	кки.		
Роль веб-сервера (IIS) Службы ролей	Веб-сервер (IIS)			^
Подтверждение	Средства управления Консоль управления службами IIS			
Результаты	Веб-сервер Общие функции НТТР Документ по умолчанию Обзор каталога Ошибки НТТР Статическое содержимое Испозвность и визсчостика Экспорт параметров конфигурации Указать альтернативный исходный путь			>
	< <u>Н</u> азад Д <u>а</u> лее > <u>У</u> станов	ить	Отмена	3

Окно мастера теперь можно закрыть.
Запрос сертификата для сервера IIS

Откройте **диспетчер служб IIS,** через Пуск -> Средства администрирования. В основном меню, в центре, выберите Сертификаты сервера.



В меню Действия, справа, выберите Создать сертификат домена.



В полном имени укажите имя будущего VPN-соединения и заполните остальные поля так, как это требуется.

Создать сертификат		?	×
Свойства различ	нающегося имени		
Укажите данные, необходимы указаны полные официальны	е для сертификата. В полях "Область, край" и "Город" должны быть е названия без сокращений.		
Полное <u>и</u> мя:			
Органи <u>з</u> ация:			
<u>П</u> одразделение:			
Г <u>о</u> род			
О <u>б</u> ласть, край:			
С <u>т</u> рана или регион:	RU ~		
	<u>Н</u> азад <u>Да</u> лее <u>Г</u> отово	Отмена	

В поле центр сертификации нажмите **Выбрать** и укажите центр сертификации. В поле **Понятное имя** укажите короткое имя сертификата, которое будет отображаться в поле имя в диспетчере IIS. В настоящем примере имя — VPN.

Создать сертификат	?	×
Локальный центр сертификации		
Задайте в том же домене центр сертификации, который подпишет сертификат. Рекомендуе запоминающееся понятное имя.	ется легко	
<u>Л</u> окальный центр сертификации:		
	Выбрать	
Пример: ИмяЦентраСертификации\ИмяСервера		
<u>Н</u> азад Д <u>а</u> лее <u>Г</u> отово	Отме	на

Убедитесь, что сертификат создан.



Установка и настройка компонентов Удалённый доступ и Маршрутизация

Установка роли удалённый доступ и службы политики сети и доступа

Нажмите Пуск -> Диспетчер серверов.



В отобразившемся окне выберите Управление -> Добавить роли и компоненты.



Отобразится окно мастера добавления ролей и компонентов, для продолжения нажмите Далее.

🛓 Мастер добавления ролей и компонентов — 🛛 🔿			×
Перед началом работы	KOHE4 mosc	НЫЙ СЕРВ cow.local.te	EP Ist
Перед началом работы Этот мастер поможет вам установить роли, службы ролей или компоненты. Опр нужно установить, на основании потребностей своей организации, таких как об документам или размещение веб-сайта. Выбор сервера Роли сервера Компоненты Подтверждение Результаты Чтобы удалить роли, службы ролей или компоненты: Запустить мастер удаления ролей и компонентов Прежде чем вы продолжите, убедитесь, что выполнены следующие задачи: Учетная запись администратора защищена надежным паролем Частроены сетевые параметры, такие как статические IP-адреса Установлены новейшие обновления безопасности из Центра обновления Win Если вам требуется проверить, выполнены ли какие-либо предшествующие настер сни Чтобы продолжить, нажмите кнопку "Далее".	оеделит бщий до dows обходим ова.	е, что эступ к ње	
Пропускать эту страницу по умолчанию			
< <u>Н</u> азад <u>Далее</u> > <u>У</u> станов	ИТЬ	Отмена	1

В следующем окне выберите Установка ролей и компонентов.

ᡖ Мастер добавления ролей и к	сомпонентов	_		×
Выбор типа уста	НОВКИ	KOHE4 mos	НЫЙ СЕРВ cow.local.te	EP est
Перед началом работы Тип установки Выбор сервера Роли сервера Компоненты Подтверждение Результаты	Выберите тип установки. Вы можете установить роли и компоненты на работаю компьютере, на виртуальной машине или на автономном виртуальном жестком • Установка ролей или компонентов Настройте один сервер путем добавления ролей, служб ролей и компоненто • Установка служб удаленных рабочих столов Установите службы ролей для инфраструктуры виртуальных рабочих столов создать развертывание на основе виртуальных компьютеров или сеансов.	ощем ф и диске в. (VDI), ч	изическо (VHD). тобы	DM
	< <u>Н</u> азад Далее > Установ	ить	Отмена	а

Отобразится окно добавления новых ролей, выберите **Удаленный доступ** и **Службы политики сети и доступа** (если не установлено ранее) и нажмите **Далее.**

🚡 Мастер добавления ролей и компонентов — 🗆 🗙					
Мастер добавления ролей и ко Выбор ролей сере Тип установки выбор сервера Роли сервера Компоненты Удаленный доступ Службы ролей Подтверждение Результаты	Выберите одну или несколько ролей для установки на этом о Роли Аттестация работоспособности устройств Алтестация работоспособности устройств Аспужбы опекуна узла Службы Windows Server Essentials Службы Windows Server Update Services Службы иполитики сети и доступа (Установлено) Службы политики сети и доступа (Установлено) Службы политики сети и доступа (Установлено) Службы политики сети и доступа (Установлено) Службы развертывания Windows Службы удаленных рабочих столов Службы удаленных рабочих столов Службы управления правами Active Directory	- С Х КОНЕЧНЫЙ СЕРВЕР логи. westeros.loc Сервере. Службы удаленного доступа обеспечивают легкое подключение через DirectAccess, VPN и прокси веб-приложения. DirectAccess обеспечивает высокий уровень доступности и управляемости. RAS предоставляет традиционные службы VPN, включая подключения типа "сеть — сеть" (для филиала или облака). Прокси веб-приложения позволяет публиковать HTTP- и HTTPS-приложения из корпоративной			
	 Службы федерации Active Directory Удаленный доступ Файловые службы и службы хранилища (Устанс Факс-сервер 	сети на клиентских устройствах за ее пределами. Служба маршрутизации обеспечивает традиционные возможности маршрутизации, включая			
Казад Далее > Установить Отмена					

В отобразившемся окне нажмите Далее.

ᡖ Мастер добавления ролей и н	сомпонентов	-		×
Удаленный дост	уп	KOHE4 north	НЫЙ СЕРВ h.westeros.	IEP loc
Перед началом работы Тип установки Выбор сервера Роли сервера Компоненты Удаленный доступ Службы ролей Подтверждение Результаты	Удаленный доступ объединяет DirectAccess, VPN и прокси-службу веб-прилож консоли управления. Разверните DirectAccess, чтобы разрешить управляемым компьютерам, присо- домену, подключаться к внутренней корпоративной сети в качестве клиентов Бесперебойное подключение всегда доступно клиентским компьютерам, обна Интернете. Администраторы DirectAccess могут удаленно управлять клиентами на мобильных компьютерах всегда используются актуальные политики безопа выполняются корпоративные требования. Разверните VPN, чтобы разрешить клиентским компьютерам, работающим по операционных систем, не поддерживающих DirectAccess, или настроенным в р удаленно подключаться к корпоративным сетям через VPN-соединение. Разверните прокси-службу веб-приложения, чтобы публиковать отдельные пр базе HTTP и HTTPS из вашей корпоративной сети на клиентские устройства, н этой сети. Это средство может использовать AD FS для проверки подлинности перед предоставлением им доступа к опубликованным приложениям. Прокси также предоставляет функциональность прокси вашим AD FS-серверам.	ения в е адиненн DirectAct руженни 1, благод існости и д управл забочей риложен аходящи пользов веб-при	диной ым к cess. ым в аря чему 1 тением группе, ия на tecя вне saтелей иложени	^ Y
	Настройте функции RRAS-маршрутизации с помощью консоли удаленного дос маршрутизации.	тупа и		~
	< <u>Н</u> азад Д <u>а</u> лее > Устано	вить	Отмен	a

В отобразившихся службах ролей выберите DirectAccess VPN и Маршрутизация, нажмите Далее.

🚡 Мастер добавления ролей и компонентов — 🗆 🗙					×
Выбор служб ро.	лей		KOHE ^L nort	НЫЙ CEP h.westeros	BEP .loc
Перед началом работы	Выберите службы ролей для установки для Удаленный доступ	ь.			
Тип установки	Службы ролей	Описание			
Выбор сервера	✓ DirectAccess и VPN (RAS)	Маршрутиз	ация обеспе	ечивает	
Роли сервера	Маршрутизация	поддержку	маршрутиза	аторов N	AT,
Компоненты	Прокси-сервер веб-приложений	с протокол	ами BGP, RIP	и и	
Удаленный доступ		маршрутиз	аторов с под сной рассыл	цдержко ки (IGMI	й)_
Службы ролей		прокси).	спои рассыл	KA (IOIMI	
Подтверждение					
Результаты					
	< <u>Н</u> азад Д <u>а</u> лее >	• <u>y</u> c	тановить	Отмен	a

Отметьте Автоматический перезапуск конечного сервера и нажмите Установить.

淕 Мастер добавления ролей и компонентов			×
Подтверждение установки компонентов	KOHEHH north.	IЫЙ CEPB westeros.I	EP loc
Перед началом работы Тип установки Выбор сервера Роли сервера Компоненты Компоненты Натобы установить на выбранном сервере следующие роли, службы ролей или на чажмите кнопку "Установить". Матоматический перезапуск конечного сервера, если требуется На этой странице могут быть отображены дополнительные компоненты (напри администрирования), так как они были выбраны автоматически. Если вы не хот эти дополнительные компоненты, нажмите кнопку "Назад", чтобы снять их флаз	компоне мер, сре ите устан кки.	нты, дства навлива	ать
Удаленный доступ Службы ролей Подтверждение Результаты Веб-сервер (IIS) Средства управления Наборы символов и средства управления службами IIS Веб-сервер Безопасность IP-адрес и ограничения домена Внутренняя база данных Windows Пакет администрирования диспетчера RAS-подключений (СМАК)		>	< >
Экспорт параметров конфигурации Указать альтернативный исходный путь <u>Казад</u> Д <u>а</u> лее > <u>У</u> станов	ить	Отмена	a

На этом мастер добавления ролей можно закрыть.

Настройка маршрутизации

Откройте оснастку **Маршрутизация и удаленный доступ,** через **Пуск -> Средства** администрирования.

🎼 🛃 🔚 🖛	Средства работы с ярлыками Администриров	зание	– 🗆 X		
Файл Главная	Поделиться Вид Управление		~ 🕐		
← → * ↑ ₩ «	с Система и безопасность 🔸 Администрирование 🗸 🗸	🖸 Поиск: Админ	истрирование 🔎		
	Имя	Дата изменения	Тип		
🖈 Быстрый доступ	Terminal Services	16.07.2016 16:23	Папка с файлами		
Рабочии стол	📕 Active Directory - домены и доверие	16.07.2016 16:20	Ярлык		
🕂 Загрузки	📌 👷 Active Directory — сайты и службы	16.07.2016 16:19	Ярлык		
🔮 Документы	🖈 💼 DNS	16.07.2016 16:19	Ярлык		
📰 Изображения	🖈 😚 Брандмауэр Windows в режиме повышенной безопасности	16.07.2016 16:18	Ярлык		
🖵 E	🚘 Диспетчер серверов	16.07.2016 16:19	Ярлык		
2	🗎 Диспетчер служб IIS	16.07.2016 16:19	Ярлык		
при во	👧 Инициатор iSCSI	16.07.2016 16:18	Ярлык		
💣 Сеть	📷 Источники данных ODBC (32-разрядная версия)	16.07.2016 16:18	Ярлык		
	📷 Источники данных ODBC (64-разрядная версия)	16.07.2016 16:18	Ярлык		
	🔁 Конфигурация системы	16.07.2016 16:18	Ярлык		
	📇 Локальная политика безопасности	16.07.2016 16:19	Ярлык		
	🔁 Маршрутизация и удаленный доступ	16.07.2016 16:19	Ярлык		
	🔝 Модуль Active Directory для Windows PowerShell	16.07.2016 16:19	Ярлык		
	🔊 Монитор ресурсов	16.07.2016 16:18	Ярлык		
	🎽 Оптимизация дисков	16.07.2016 16:18	Ярлык		
	🔚 Очистка диска	16.07.2016 16:19	Ярлык		
	🎁 Пакет администрирования диспетчера подключений	16.07.2016 16:19	Ярлык		
	😥 Планировщик заданий	16.07.2016 16:18	Ярлык		
	🛜 Пользователи и компьютеры Active Directory	16.07.2016 16:20	Ярлык		
		16.07.2016.16.10	Q		
Элементов: 36 Выбр	Элементов: 36 Выбран 1 элемент: 1,11 КБ				

В отобразившейся оснастке в левом меню кликните правой кнопкой нужный сервер и нажмите Настроить и включить маршрутизацию и удалённый доступ.

9	Маршрутизация	и удаленный доступ
---	---------------	--------------------

🗢 🔿 📶 💢 🗒 🙆 🔢 🗔	
 Маршрутизация и удаленный NORTH (локально) Состояние сервера 	
NORIH Настроить и включить маршрутизацию и удаленный доступ	і удаленного
Отключить маршрутизацию и удаленный доступ	упа к сети выберите в меню "Действие"
Все задачи >	шрутизации и удаленного доступа.
Вид >	
Удалить	
Обновить	
Свойства	
Справка	

Настройка маршрутизации и удаленного доступа для выбранного сервера.

Отобразится мастер установки сервера маршрутизации и удалённого доступа. Нажмите Далее.

Мастер настройки сервера маршрутизации и удаленного доступа	
	Мастер установки сервера маршрутизации и удаленного доступа
	Этот мастер помогает настроить сервер так, чтобы вы могли подключаться к другим сетям и разрешать подключения удаленных клиентов.
	Для продолжения нажмите кнопку "Далее".
	< <u>Н</u> азад Далее > Отмена

 \times

_

Выберите Доступ к виртуальной частной сети (VPN) и NAT.

Мастер настройки сервера маршрутизации и удаленного доступа Конфигурация Вы можете включить указанные службы в любом из этих сочетаний или выполнить настройку данного сервера.
 Удаденный доступ (VPN или модем) Позволяет удаленным клиентам подключаться к этому серверу через удаленное подключение или безопасное подключение виртуальной частной сети (VPN) Преобразование сетевых адресов (NAT) Позволяет внутренним клиентам подключаться к Интернету, используя один общий IP-адрес. Доступ к виртуальной частной сети (VPN) и NAT Позволяет удаленным клиентам подключаться к данному серверу через Интернет и внутренним клиентам подключаться к данному серверу через Интернет и внутренним клиентам подключаться к Интернету, используя один общий IP-адрес. Еезопасное соединение между двумя частными сетями Позволяет подключить данную сеть к удаленной сети, например, к сети филиала. Особая комбинация возможностей маршрутизации и удаленного доступа.
< <u>Н</u> азад Далее > Отмена

Выберите интерфейс сети, который подключает данный шлюз к сети.

Для (реализации VPN	I на сервере должно быть	, как миниму	м, 2 сетевых и	інтерфейса.	
Мастер	Мастер настройки сервера маршрутизации и удаленного доступа					
Соед Ч ме	инение по VPN тобы разрешить VPN енее одного интерфе	√клиентам подключаться к данно айса сети должно быть подключен	му серверу не ю к Интернету.			
Выбер	рите интерфейс сети Интерфейсы <u>с</u> ети:	1, который подключает данный се	рвер к Интернету	r.		
	Имя	Описание	IP-адрес			
	Ethernet0	Intel(R) 82574L Gigabit	172.16.12.125			
		inter(n) 62974L Gigabit	132.166.10.123	Uncr)		
		< <u>Н</u> азад	Далее >	Отмена		

В следующем окне выберите способ назначения IP-адресов — автоматически или из заданного диапазона.

Мастер настройки сервера маршрутизации и удаленного доступа
Назначение IP-адресов Вы можете выбрать способ назначения IP-адресов удаленным клиентам.
Выберите способ назначения IP-адресов удаленным клиентам:
О Двтоматически
При использовании DHCP-сервера для назначения IP-адресов, убедитесь, что он настроен правильно. Если DHCP-сервер не используется, то этот сервер будет сам создавать IP-адреса. Уз заданного диапазона адресов
< <u>Н</u> азад Далее > Отмена

В настоящем примере используется заданный диапазон.

Новый диапазон IPv4-ад	?	×					
Введите начальный IP-адрес и либо конечный IP-адрес, либо количество адресов в непрерывном диапазоне.							
<u>Н</u> ачальный IP-адрес:	0.0.0.0						
<u>К</u> онечный IP-адрес:	0.0.0.0						
Количество адресов:	0						
	OK	Отмена					

Выберите, требуется ли данному серверу работать с RADIUS. В настоящем примере это не требуется - выберите **Нет.**

Мастер настройки сервера маршрутизации и удаленного доступа
Управление несколькими серверами удаленного доступа Запросы на подключения могут быть проверены локально или переадресованы на удаленный сервер доступа, совместимый с протоколом RADIUS.
Хотя маршрутизация и удаленный доступ могут выполнять проверку подлинности запросов на подключение, большие сети с множеством серверов удаленного доступа часто используют RADIUS-сервер для централизованной проверки подлинности.
Если вы в своей сети используете RADIUS-сервер, то на текущем сервере можете настроить переадресацию запросов проверки подлинности на RADIUS-сервер.
Вы хотите настроить данный сервер для работы с RADIUS-сервером? Не <u>т</u> , использовать службу маршрутизации и удаленного доступа для проверки подлинности запросов на подключение
С Да, настроить данный сервер для работы с RADIUS-сервером
< Назад Далее > Отмена

По завершении нажмите Готово.

Мастер настройки сервера маршрутизации и удаленного доступа						
	Завершение мастера сервера маршрутизации и удаленного доступа					
	Успешно завершена работа мастера сервера маршрутизации и удаленного доступа					
	Сводка:					
	VPN-клиенты подключаются к следующему общедоступному интерфейсу: Ethemet0	^				
	RAS-и VPN-клиентам для адресации назначается следующая сеть: Ethemet1.					
	При установке и проверке клиентских	~				
	Чтобы клиенты могли подключаться, необходимо добавить учетные записи пользователей на локаль компьютере или через Active Directory.	ном				
	Для закрытия мастера нажмите кнопку "Готово".					
< <u>Н</u> азад Готово Отмена						

Перейдите в оснастку Маршрутизация и удалённый доступ, откройте свойства сервера.

🚊 Маршрутиз	ация и удаленный доступ		– 🗆 ×
Файл Действ	ие Вид Справка		
🌩 📄 🗖			
Маршрутиза Состояни	ация и удаленный NORTH (локально) ие сервера		_
> 🔂 NORTH	Настроить и включить маршрутизацию и удаленный доступ		го доступа 🔷
	Отключить маршрутизацию и удаленный доступ		беспечивает безопасный удаленный доступ
	Использовать DirectAccess		эзволяет настраивать следующие
	Все задачи	>	лными сетями;
	Вид	>	
	Удалить		
	Обновить		
	Свойства		
	Справка		ного доступа, выберите в меню "Действие"
<			
Открытие окна с	войств выбранного объекта.		

÷.

Перейдите во вкладку Безопасность -> методы проверки подлинности, отметьте Протокол ЕАР, остальное оставьте пустым. Нажмите ОК, нажмите Применить.

IKEv2	PPP	Ведени	е журнал	в
Общие	Безопасность	IPv4	IP۱	6
Иетоды прове	рки подлинности		?	>
Сервер произв выбранных мет	одит проверку удаленной годов в порядке их указа	і системы испо. ния.	льзуя од	ин и
🔽 Протокол Е	AP			
Если испол Для настро NPS.	ьзуется защита доступа йки остальных параметр	к сети (NAP), вы ов NAP исполь	ыберите I зуйте сер	ЕАР вер
🗌 Шифрованн	ая проверка (Microsoft, ве	ерсия 2, MS-CH	AP v2)	
🗌 Шифрованн	ая проверка подлинност	и (СНАР)		
Незашифро	ванный пароль (РАР)			
Разрешить компьютера	проверку подлинности с а для IKEv2	помощью серт	ификата	
Доступ без пр	оверки			
П Разрешит	ъ подключение удаленны	х систем без п	роверки	
		ОК	Отмен	a
⊢ Привязка сег	отификата SSL			
Привязка сер	ртификата SSL ивать HTTP			
Привязка сер Использо Выберите сег	отификата SSL ивать HTTP отификат, который лолже	ен использоват	ъ	
Привязка сер Использо Выберите сер SSTP-сервер	ртификата SSL рвать HTTP ртификат, который долже для привязки SSL (веб-т	ен использоват прослушиватель	ь)	
Привязка сеј Использо Выберите сеј SSTP-сервер Сертификат:	отификата SSL вать HTTP отификат, который долж для привязки SSL (веб-п По умолчанию	ен использоват прослушиватель	ъ 5) Просмотр	,

1.0

В оснастке Маршрутизация и удалённый доступ выберите **Сервер-> IPv4 -> Преобразование сетевых** адресов (NAT). В отобразившемся окне откройте свойства сетевого интерфейса, который ранее указывался в мастере настройки маршрутизации.

🚊 Маршрутизация и удаленный доступ				- 0	×
Файл Действие Вид Справка					
🗢 🔿 🙍 🔜 🗶 🖬 🖉 🗄					
 	разование сетевых адресов фейс утренний ernet1 Отображение сопоста Удалить Обновить Свойства Справка	в (NAT) Всего сопоставлений 0 0 влений	Прибывших пак 0 0 119	етов переве;	(EHO
					>

В отобразившемся окне перейдите во вкладку Службы и порты, отметьте **Безопасный веб-сервер** (HTTPS), нажмите **Применить**, нажмите **ОК**.

Свойства: Ethernet0	?	×				
Преобразование сетевых адресов (NAT)						
Пул адресов	Службы и порты					
Выберите службы в частной сети, к которым вы хотите перенаправлять пользователей Интернета. Будут созданы правила перенаправления портов NAT. <u>С</u> лужбы:						
 ☐ FTP-сервер ☐ Протокол Internet Mail Access ☐ Протокол Internet Mail Access ☐ Почтовый сервер Интернета ☑ IP-безопасность (IKE) ☑ IP-безопасность (прослежие) ☐ Протокол Post-Office Protocol 	s Protocol, версия 3 (IMAP3) s Protocol, версия 4 (IMAP4) a (SMTP) вание IKE NAT) I, версия 3 (POP3)	^				
Удаленный рабочий стол Безопасный веб-сервер (НТ	трс)					
	11-3)	v				
<		>				
Добавить Из <u>м</u> енить	<u>Удалить</u>					
(ОК Отмена Пр	ри <u>м</u> енить				

Назначение пользователю прав на использование VPNподключения

Подключаться к сети через VPN-соединения могут только те пользователи, учётные записи которых настроены для таких подключений. Для назначения пользователю таких прав выполните следующие действия.

Откройте оснастку Active Directory — Пользователи и компьютеры. Откройте свойства пользователя, которому необходимо назначить права на VPN-соединения. Во вкладке **Входящие звонки** выберите **Разрешить доступ**, нажмите **Применить**, нажмите **ОК**.



Проверка работоспособности

Для того чтобы подключаться к сети через VPN-соединение, необходимо настроить соответствующее подключение на рабочей станции и осуществить это подключение с использованием электронного ключа JaCarta.

Создание подключения

Перейдите на клиентскую рабочую станцию.

Откройте Центр управления сетями и общим доступом, выберите Создание и настройка нового подключения к сети.



			—		×
← 🔮	🛛 Set U	p a Connection or Network			
		•			
0	Choose	e a connection option			
		Connect to the laternat			
		Set up a broadband or dial-up connection to the Internet.			
		Set up a new network			
	3	Set up a new router or access point.			
		Connect to a workplace			
		Set up a dial-up or VPN connection to your workplace.			
	L				
		-			
		L	<u>N</u> ext	Can	cel

Выберите Использовать моё подключение к Интернету (VPN).



В отобразившемся окне выберите Подключение к рабочему месту.

Отобразится следующее окно, выберите Настроить.

	_	_		×
~	Connect to a Workplace			
	Do you want to set up an Internet connection before continuing?			
	An Internet connection is necessary for using a VPN connection.			
	\rightarrow <u>S</u> et up an Internet connection			
	\rightarrow I'll set up an Internet connection later			
			Canc	el

В следующем окне укажите **адрес, имя подключения.** Отметьте пункт **использовать смарт-карту.** Нажмите **Создать.**

			_		×
←	🔚 Connect to a Workplace				
	lype the Internet addre	ess to connect to			
	Your network administrator c	an give you this address.			
	Internet address:	vpn.westeros.loc			
	Destination name:	VPN Westeros			
	✓ Use a <u>s</u> mart card				
	✓ <u>R</u> emember my creder	itials			
	💡 🗌 <u>A</u> llow other people to	use this connection			
	This option allows any	yone with access to this computer to use this connection	on.		
			eate	Cano	:el



Если всё настроено верно, соединение произойдет успешно. Статус Connected.

Settings			-		×	
🔅 Home	VPN					
Find a setting	VPN					
Network & Internet	+ Add a VPN con	nection				
🗇 Status	VPN Connectio No Internet	n				
記 Ethernet	VPN Westeros					
ଳି Dial-up	Connected					
% VPN		Advanced options	Disco	onnect	1	
🕒 Data usage						
A Provy	Advanced Option	IS				
	Allow VPN over metered networks					
	On On					
	Allow VPN while roami	ing				
	On On					

Также и в свойствах подключения отображено успешное подключение.

鞋 Network and Sharing Center		- 🗆 X
← → ∨ ↑ 🚆 « Network and	Internet > Network and Sharing Center	✓ ט Search Control Panel
Control Panel Home	View your basic network information	n and set up connections
Change adapter settings	View your active networks	
Change advanced sharing settings	VPN Westeros Public network	Access type: No Internet access Connections: VPN Westeros
	Unidentified network Public network	Access type: No network access Connections:
	Change your networking settings	
	Set up a new connection or network Set up a broadband, dial-up, or VPN of	connection; or set up a router or access point.
	Troubleshoot problems Diagnose and repair network problem	ns, or get troubleshooting information.
See also		
HomeGroup		
Infrared		
Windows Firewall		

На этом настройка и проверка окончена.

Подключение к удалённому рабочему столу (RDP)

RDP (Remote Desktop Protocol) — протокол **Remote Desktop** создан компанией **Microsoft** для обеспечения удалённого доступа к серверам и рабочим станциям Windows. Протокол **RDP** может использоваться как для администрирования, так и для повседневной работы на удалённой рабочей станции. В настоящее время **RDP** является основным протоколом удалённого доступа для систем семейства Windows, а клиентские приложения существуют как для OC от Microsoft, так и для Linux, FreeBSD, MAC OS X и различных тонких клиентов для терминального доступа.

Описание демо-стенда

Демо-стенд состоит из следующих компонентов.

Сервер

Windows Server 2016 Datacenter с установленным программным обеспечением Единый Клиент JaCarta и настроенными ролями серверов Active Directory и Active Directory Certificate Services.

Настройка удалённого доступа, в рамках настоящего документа, будет настроена на этот же сервер. Можно реализовать на любой сервер или клиентскую редакцию Windows.

Настоящий пример показывается простое RDP-соединение клиент-сервер, без участия сервиса терминалов **Remote Desktop Services.**

Подробное руководство об установке и настройке Active Directory Certificate Services доступно в документе — "JaCarta PKI для аутентификации в домене Windows Server 2016", который размещён на официальном сайте "Аладдин Р.Д.", в разделе "Интеграционные инструкции" — https://www.aladdin-rd.ru/support/guides.

Клиент 1

Рабочая станция — Windows 10 с установленным программным обеспечением Единый Клиент JaCarta.

Ход настройки

Настройка происходит на сервере и клиенте, делится на следующие этапы.

На сервере:

включение удалённого доступа;
назначение прав пользователей для удалённого доступа;

В качестве "сервера" может выступать любая ОС Windows, не обязательно серверная редакция.

На клиенте:

создание RDP-подключения;проверка работоспособности.

Подключение к удалённому рабочему столу

Электронные ключи JaCarta PKI могут использоваться для двухфакторной аутентификации в сессию удалённого рабочего стола (RDP). Также с ключом можно работать после установки сессии с прикладным ПО, поддерживающим работу со смарт-картами.

Настройка рабочих станций и серверов

Для того чтобы к рабочему столу компьютера можно было подключаться удалённо, выполните следующее.

Выберите Пуск, щёлкните правой кнопкой на Компьютер и выберите Свойства.

В открывшемся окне Система щёлкните на ссылке Настройка удалённого доступа.



.....

Отобразится окно **Свойства системы**. В секции **Удалённый рабочий** стол выберите **Разрешить удалённое подключение к этому компьютеру.**

Опционально выбор **Разрешить подключаться только с компьютеров, на которых работает удалённый рабочий стол с проверкой подлинности на уровне сети (NLA).** Зависит от требований, решение будет работать и без NLA.

Свойства системы Х					
Имя компьютера	Оборудование	Дополнительно	Удаленный достуг	1	
Удаленный помощник					
компьютеру					
		L	1 <u>о</u> полнительно		
Удаленный раб	очий стол				
Выберите вариа	ант и укажите, ко	му разрешено под	аключение.		
() <u>Н</u> е разрешат	ъ удаленные под	ключения к этому	компьютеру		
Разрешить у	даленные подкл	очения к этому ко	мпьютеру		
Разрешить подключения только с компьютеров, на которых работает удаленный рабочий стол с проверкой подлинности на уровне <u>с</u> ети (рекомендуется)					
Помочь выбрать пользователей					
	(ОК Отме	ена При <u>м</u> енит	ь	

Если вы хотите, чтобы к компьютеру могли подключаться пользователи, не имеющие полномочий локального администратора, нажмите **Выбрать пользователей** и выберите этих пользователей или (и) группы.

Пользователи удаленного рабочего стола	?	×				
Пользователи из списка ниже, а также члены групп "Администраторы", могут подключаться к этому ко	ны мпьютеру.					
S WESTEROS \jsnow						
Добавить Удалить						
Чтобы создать новую учетную запись или добавить другие группы, откройте панель управления <u>Учетны</u> пользователей.	пользоват іе записи	елей в				
ОК	Отме	на				

Далее окна настройки можно закрыть, нажав ОК.

Действия пользователя

Для того чтобы подключиться к удалённому рабочему столу, выполните следующее.

Убедитесь в том, что электронный ключ JaCarta PKI с сертификатом пользователя, имеющего право на подключение к удалённому рабочему столу подключён к рабочей станции, на которой будет настроено подключение.

Щёлкните Пуск > Все программы > Стандартные > Подключение к удалённому рабочему столу.

퉋 Подключение к удаленному рабочему столу		_		×
Подключение к удаленн рабочему столу	юму			
<u>К</u> омпьютер: 172.16.12.125 Пользователь: Не задано При подключении необходимо будет указать учетные данные.	~			
Показать параметры	Подкл <u>ю</u> чить		<u>С</u> правка	

В окне **Подключение к удалённому рабочему столу** в поле **Компьютер** введите имя или IP-адрес компьютера, к рабочему столу которого вы хотите подключиться.

Нажмите Параметры.

Откройте вкладку Локальные ресурсы.

🎚 Подключение к удаленному рабочему столу — 🗆 🗙						
Подключение к удаленному рабочему столу						
Общие Экран Локальные ресурсы Взаимодействие Дополнительно Звук удаленного рабочего стола						
Клавиатура Использовать сочетания клави <u>ш</u> Windows: Только в полноэкранном режиме Пример: ALT+TAB						
Покальные устройства и ресурсы Выберите устройства и ресурсы, которые вы хотите использовать во время удаленного сеанса. ☑ Пр <u>и</u> нтеры ☑ Буфер обмена Подробнее						
Скрыть параметры Подключить Справка						

1.0

В секции Локальные устройства и ресурсы нажмите Подробнее.

퉋 Подключение к удаленному рабочему столу	×
Подключение к удаленному рабочему столу	
Локальные устройства и ресурсы	
Выберите устройства и ресурсы этого компьютера, которые вы хотите использовать во время удаленного сеанса.	
☐Смарт-карты	1
Ш Порты	
Другие поддерживаемые PnP-устройства	
	-
ОК Отмена	3

Убедитесь, что флажок Смарт-карты установлен, и нажмите ОК.

Нажмите Подключить.

Если система сразу не определила смарт-карту и не предложила ввести PIN-код, нажмите **Больше** вариантов и выберите смарт-карту. После чего откроется окно ввода PIN-кода.

Безопасность Windows	×						
Введите учетные данные							
Эти учетные данные будут использоваться при подключении к 172.16.12.125.							
john snow							
Учетные данные смарт-карты							
•••••	0						
Запомнить меня							
Больше вариантов							
WESTEROS\A							
john snow							
OK C	Отмена						

Нажмите **ОК,** после чего произойдет подключение к удалённому рабочему столу и аутентификация в сессию **RDP.**

Доступ к информационным ресурсам по HTTPS

Общие сведения

Существует возможность аутентифицироваться с использованием электронного ключа JaCarta при получении доступа к информационным ресурсам по протоколу HTTPS. Аутентификация по протоколу HTTPS может использоваться не только для доступа к защищённому Web-сайту, но и в следующих технологиях доступа к различным службам, например, Outlook Web Access, Microsoft Exchange, Шлюз служб терминалов. А также к Web-сервисам других вендоров, например, Citrix XenApp/XenDesktop.

Подробное руководство об установке и настройке **Citrix Xen Desktop** доступно в документе — "**JaCarta для аутентификации в XenDesktop/XenApp 7.x. Руководство по настройке**", который размещён на официальном сайте "Аладдин Р.Д.", в разделе "Интеграционные инструкции" — https://www.aladdin-rd.ru/support/guides.

Внедрение аутентификации пользователя с использованием сертификата в памяти **JaCarta** позволит усилить защищённость указанных служб и предотвратить несанкционированный доступ.

Примечание:

В качестве примера в настоящем документе рассматривается доступ к защищённому сайту.

Настройка сервера

Общие рекомендации и последовательность действий

При настройке Web-сервера для исключения несанкционированного доступа к нему рекомендуется максимально ограничить возможности аутентификации пользователя, исключив анонимную аутентификацию, а также другие стандартные способы аутентификации.

В целях безопасности развёртывать центр сертификации на Web-сервере не рекомендуется.

Общие настройки сервера

Для того чтобы настроить Web-сервер, выполните следующую последовательность действий.

Убедитесь в том, что сервер удовлетворяет системным требованиям. В частности, на нём должна быть установлена роль **Веб-сервер (IIS)**.

Запустите Диспетчер служб IIS.

В дереве консоли выберите имя сервера — в центральной части окна отобразятся доступные возможности.

🎕 Диспетчер служб IIS		– 🗆 X
← → ● BRAVOS ►		🔯 🗵 🟠 🔞 🗸
<u>Ф</u> айл <u>Р</u> ежим <u>С</u> правка		
Подключения		Действия
🔍 - 🕞 🖄 😽	Пачальная страница вкахоз	Управление сервером
Начальная страница ВВАУОS (WESTEROS) Алмини	Фильтры: 🔹 🐺 Перейти 🤟 🕁 Показать <u>в</u> се 🗧	Перезапустить
	IIS A	Остановить
		Просмотреть пулы
	Ведение Документ по Заголовки Кэширова Модули Проверка	приложений Просмотреть сайты
	журнала умолчанию ответов выводимы подлинно	Получить новые
		компоненты веб-платформы
	Просмотр Рабочие Сертифик Сжатие Сопостав Страницы	W Справка
	J	
	Типы МІМЕ Фильтрация запросов	
	Управление	
	Стала Ста Shared Лелегиро Релактор	
	Configurat компонента конфигур	
	I ПП Просмотр возможностей 💦 Просмотр содержимого	1
Готовность		€ <u>1</u> .:

В секции **IIS** сделайте двойной щелчок на Сертификаты сервера.

Центральная область окна будет выглядеть следующим образом.

Consult.						
Сертифі	икаты сервера		Импортировать			
Используйте эту фун может использовать Фильтры:	кцию для запроса и обработки сертифик с веб-сайтами, где настроено использов:	атов, которые веб-сервер ание SSL. <u>в</u> се	Создать запрос сертификата Запрос установки сертификатов			
Имя	Получатель сертификата	Поставщик	Создать сертификат домена			
vpn	vpn.westeros.loc	westeros-NORTH-CA	Создать самозаверенный сертификат			
	north.westeros.loc westeros-NORTH-CA	westeros-NORTH-CA westeros-NORTH-CA	Вид Экспортировать Обновить Удалить Включить автоматическую повторную привязку обновленных сертификатов			
< Просмотр возможи	ностей ह Просмотр содержимого	>	Справка			
			• <u>=</u>			

В колонке Действия справа щёлкните на ссылке Создать сертификат домена.

Отобразится окно мастера создания сертификата.

В окне мастера создания сертификата заполните необходимые поля и нажмите Далее.

Примечание:

Значение в поле Полное имя должно совпадать с адресом сайта, который пользователь будет вводить в браузере.

На следующей странице мастера создания сертификата в поле **Локальный центр сертификации** выберите используемый центр сертификации (при необходимости воспользуйтесь кнопкой **Обзор**), в поле **Понятное имя** введите дополнительное имя сертификата.

Нажмите Готово, чтобы закрыть окно мастера создания сертификата.

Снова выберите Web-сервер, щёлкнув на его имени в окне диспетчера служб IIS.

В центральной части окна в секции IIS сделайте двойной щелчок на значке Проверка подлинности.

Отключите все способы проверки подлинности, кроме **Проверка подлинности клиента Active Directory с помощью сертификата**. Для этого, выбрав способ проверки подлинности, в колонке **Действия** щёлкните на ссылке **Отключить** или **Включить**.

Настройка сайта

В окне диспетчера служб IIS разверните ветвь с именем сервера и выберите сайты > Default Web Site. В правой части окна щёлкните на ссылке Привязка.

Отобразится следующее окно.

Іривязки	сайта				? ×
Тип	Имя узла	Порт	IP-адреса	Сведения о при	Добави <u>т</u> ь
http		80	*		Из <u>м</u> енить
					<u>У</u> далить
					О <u>б</u> зор
					 <u>З</u> акрыть

Нажмите Добавить.

Отобразится следующее окно.

обавление п	ривязки	сайта			?	×
<u>Т</u> ип: http	~	IP- <u>ад</u> рес: Все неназначенные	~	П <u>о</u> рт: 80		
Имя у <u>з</u> ла:]				
Пример: ww	w.conto	so.com или marketing.contoso.con	ı			
Пример: ww	w.conto:	so.com или marketing.contoso.con	ו			
Пример: ww	w.conto	so.com или marketing.contoso.con	ı			
Пример: ww	w.conto	so.com или marketing.contoso.con	ı			

В списке Тип выберите https, и в списке Сертификаты SSL выберите сертификат сервера.

Нажмите ОК.

1.0

В окне диспетчера служб IIS щёлкните на сайте или виртуальном каталоге, доступ к которому вы хотите сделать защищённым (например, сайты > Default Web Site > site).

В центральной части окна станут доступны настройки данного сайта.



Сделайте двойной щелчок на иконке Параметры SSL.

Страница примет следующий вид.

	Действия		
🥶 Параметры SSL	🛃 Применить		
Эта страница позволяет изменять параметры SSL для содержимого веб-сайта или	Стмена		
приложения.	😢 Справка		
✓ Требовать SSL			
Сертификаты клиента:			
🔿 Игнорировать			
🔿 Принимать			
Требовать			

Установите флажок Требовать SSL, и в секции Сертификаты клиента выберите Требовать.

В колонке Действия нажмите Применить.

Действия пользователя

Для получения доступа к защищённому сайту выполните следующее.

Запустите Microsoft Internet Explorer.

1.0

Убедитесь в том, что ваш электронный ключ JaCarta с сертификатом, дающим право на доступ к сайту, подсоединён к компьютеру.

Введите адрес защищённого сайта, начинающийся с https.

В окне Безопасность Windows выберите сертификат пользователя и нажмите ОК.

При необходимости введите PIN-код пользователя JaCarta.

Признаком установления защищённого соединения служит появление значка 💻 рядом с адресной строкой Internet Explorer.

Hастройка Mozilla Firefox и проверка входа на защищенный Web-сайт

Помимо браузера Internet Explorer, для доступа к защищённому Web-сайту существует возможность использовать браузер Mozilla Firefox, для этого потребуется небольшая настройка.

Чтобы использовать электронные ключи JaCarta с Mozilla Firefox, в настройках браузера необходимо указать путь к библиотеке PKCS11 из состава Единый клиент JaCarta. Если браузер Mozilla Firefox был установлен на компьютер до установки Единый клиент JaCarta и, если при установке Единый клиент JaCarta была отмечена соответствующая опция, путь к библиотеке прописывается в настройках Mozilla Firefox автоматически.

Чтобы указать путь к **PKCS11** из состава **Единый клиент JaCarta** вручную, выполните следующие действия.

Запустите Mozilla Firefox, щёлкните на значке **Глебох** и выберите Настройки > Настройки, как показано на изображении ниже.



В отобразившемся окне щёлкните на значке **ССР** (**Дополнительные**), выберите вкладку Шифрование и нажмите Устройства защиты.

Отобразится следующее окно.

🕙 Управление устройствами			
Модули и устройства защиты	Подробности	Значение	На <u>ч</u> ать сеанс
▷NSS Internal PKCS #11 Module	Модуль	Athena PKCS#11	Закончить сеанс
Athena PKCS#11 Module	Путь	C:\Windows\syst	Sengir and Seene
◊ Модуль встроенных корневых се			Сменить пароль
			Загрузить
			В <u>ы</u> грузить
			Использовать <u>F</u> IPS
			ОК

Если путь к библиотеке PKCS11 был прописан автоматически в процессе установки **Единый клиент** JaCarta, в списке Модули и устройства защиты будет значиться Athena PKCS#11 Module. В противном случае нажмите Загрузить.

Отобразится следующее окно.

🕹 Загрузка устройства РКСЅ#11	_ 🗆 ×	
Введите информацию о модуле, который вы хот	ите добавить.	
Имя модуля: New PKCS#11 Module		
Имя файла модуля:	О <u>б</u> зор	
OK	Отмена	

В поле Имя модуля введите имя нового модуля (например, JaCarta), в поле Имя файла модуля укажите путь к библиотеке PKCS11 из состава Единый клиент JaCarta (при необходимости воспользуйтесь кнопкой Обзор).

Файл библиотеки PKCS11 из состава Единый клиент JaCarta находится по следующему пути:

C:\Windows\System32\asepkcs.dll

Нажмите ОК.

Добавленная библиотека отобразится в списке Модули и устройства защиты.

🕙 Управление устройствами			<u>_</u> D×
Модули и устройства защиты ▷ NSS Internal PKCS #11 Module ▷ Модуль встроенных корневых се □JaCarta JaCarta	Подробности Модуль Путь	Значение JaCarta c:\Windows\Syst	На <u>н</u> ать сеанс Закончить сеанс Сменить пароль Загрузить Выгрузить Использовать <u>F</u> IPS
			ОК

Настройка конфигурации Mozilla Firefox

Чтобы обеспечить SSL-доступ к защищённому сайту с использованием цифрового сертификата в памяти JaCarta, необходимо включить соответствующую настройку в конфигурации Mozilla Firefox. Для этого выполните следующие действия.

Примечание:

Данные действия необязательны для Firefox версий до 4.0.

Запустите Mozilla Firefox.

В адресной строке наберите about: config и нажмите клавишу Enter.

В окне браузера отобразится предупреждающее сообщение.

Нажмите Я обещаю, что буду осторожен.

Окно браузера примет следующий вид:

Firefox 🔻						
about:config	+					
♦ → about:config				r.		
Фидьтр:						
Имя настройки		Состояние	Тип	Значение		
accelerometer.enabled		по умолчанию	логическ	true		
accessibility.accesskeycausesactivation		по умолчанию	логическ	true		
accessibility.blockautorefresh		по умолчанию	логическ	false		
accessibility.browsewithcaret		по умолчанию	логическ	false		
accessibility.browsewithcaret_shortcut.enabled		по умолчанию	логическ	true		
accessibility.mouse_focuses_formcontrol		по умолчанию	логическ	false		
accessibility.tabfocus		по умолчанию	целое	7		
accessibility.tabfocus_applies_to_xul		по умолчанию	логическ	false		

Двойным щелчком измените значение настройки

security.ssl.allow_unrestricted_renego_everywhere__temporarily_available_pref

на true (истина).

(Для быстрого поиска настройки введите или скопируйте ее в поле Фильтр).

Действия пользователя

Чтобы получить доступ к защищённому сайту с использованием браузера Mozilla Firefox и электронного ключа JaCarta, выполните следующие действия.

Убедитесь в том, что к компьютеру подключён электронный ключ JaCarta. На USB-токене JaCarta должен гореть световой индикатор.

Запустите браузер Mozilla Firefox, в адресной строке введите адрес защёщенного сайта (адрес должен начинаться с https://) и нажмите клавишу ВВОД.

Отобразится следующее окно.


Введите пароль пользователя JaCarta и нажмите **ОК**.

После этого вы попадёте на защищённый сайт.

Защита документов Microsoft Office

Пакет программ **Microsoft Office** является наиболее популярным в мире офисным и домашним инструментом для работы с различными типами документов (текстами, электронными таблицами, базами данных и др.).

Используя цифровой сертификат, записанный на USB-токен или смарт-карту **JaCarta PKI**, пользователь может с лёгкостью подписать документ электронной подписью, тем самым обеспечив защиту документа.

Для чего нужна электронная подпись в MS Office?

Электронная подпись — это цифровая зашифрованная печать, удостоверяющая подлинность цифровых данных, таких как сообщения электронной почты, макросы или электронные документы. Подпись подтверждает, что сведения предоставлены подписавшим их создателем и не были изменены.

Электронная подпись позволяют организациям снизить риск при обмене данными в электронном виде, а также оптимизировать обработку контрактов и других соглашений. Цифровые подписи предоставляют сведения о том, что именно было подписано, и могут быть проверены в будущем.

Одновременно с видимой подписью в документ добавляется и цифровая подпись для удостоверения личности подписавшего. После того как в документе появилась цифровая подпись, он становится доступен только для чтения.

Сертификат подписи и центр сертификации

Сертификат подписи

Для создания цифровой подписи необходим сертификат подписи, удостоверяющий личность. При отправке макроса или документа, подписанного цифровой подписью, также отправляется сертификат и открытый ключ. Сертификаты выпускаются Центром сертификации и могут быть отозваны.

Центр сертификации

Центр сертификации выпускает цифровые сертификаты, подтверждает их достоверность с помощью подписей, а также отслеживает сертификаты, которые истекли или были отозваны.

Что подтверждает цифровая подпись?

• Подлинность.

•Цифровая подпись подтверждает личность подписавшего.

• Целостность.

•Цифровая подпись подтверждает, что содержимое документа не было изменено или подделано после заверения.

• Неотрекаемость.

•Цифровая подпись подтверждает происхождение заверенного содержимого. Подписавший не может отрицать свою связь с подписанным содержимым.

Изависимо от времени получения сертификата подписи и состояния его отзыва считается, что подписанные документы с действующей отметкой времени содержат действительные подписи.

Какие приложения Microsoft Office поддерживают ЭП?

•документы Word;

•книги Excel;

•презентации PowerPoint.

Хранение цифрового сертификата на электронном ключе

Электронный ключ, в отличии от других известных способов хранения, обеспечивает неизвлекаемость ключевой информации на USB-токене или смарт-карте. Неизвлекаемое хранение подразумевает, что ключ из токена или карты не попадает никуда извне, например, на жёсткий диск компьютера или в оперативную память. А при обращении к информации на электронном ключе требуется знание PIN-кода, неправильный ввод которого приведёт к блокировке. Это в свою очередь защищает от подбора комбинации PIN-кода, сводя количество попыток к определённому значению, например, 3.

Добавление подписи к документу Microsoft Word 2016

ර බා

Главная

🔏 Вырезать

🕞 Копировать

Буфер обмена

Файл

ĥ

^

еобхо,	дим	١ый	доку	умен	4T.							
и Рассы	лки	Реце	нзирова	ние	Вид	Q	Что вы хотите	е сделать?				
Aa - & ª⊻ - <u>A</u> -		• <u>}</u> = =	*== ↓ ≡ \$		∎ ậ↓ ⊵ - ⊞	¶ •	АаБбВвГг; 11 Обычный	АаБбВвГг; 1 Без инте	АаБбВ Заголово	АаБбВе Заголово	Аас Заголовок	АаБб Подзаго
G			Абза	зц		Fai I						
			_									
	-	□ ×										
	\$	D		H	аз	Ba	ани	e				

Для подписания документа откройте необходимый документ.

Trebuchet M + 32

Word 2016 справка

📀 🏵 🟠 Поиск

Вставить • Формат по образцу • Формат по образцу

F₂₄

Ссыл

- A A

Шрифт

Популярные разделы справки

ВАЖНО: Данная статья переведена с помощью машинного перевода, см. Отказ от ответственности. Используйте английский вариант этой статьи, который находится здесь, в качестве справочного материала.

Выбор альбомной или книжной ориентации страницы

Вставка объекта WordArt

Исправления в Word

Изменение регистра текста

Добавление диаграммы в документ

Заголовок Хотите сделать дизайн этого шаблона еще лучше? Загляните в коллект

«Главная». Вы можете изменить оформление заголовков или подчерки помощью таких привлекательных стилей, как «Выделение» и «Выделе подходят друг к другу и помогут вам раскрыть свои идеи.

Попробуйте! Это легко.

Перейдите в меню Файл -> Сведения и в отобразившемся окне нажмите Защита документа.

¢			До	кумент7 - Word
Сведения	Сведен	ЯИН		
Создать		Защита документа	Свойства -	
Открыть	С Защита	Все могут открывать, копировать и изменять любую часть этого документа.	Размер	Еще не сохранено
Сохранить	документа -		Число страниц Число слов	1 50
Сохранить как			Общее время правки Название	8 мин Добавить название
Печать	Поиск	ИНСПЕКТОР ДОКУМЕНТОВ Перед публикацией этого файла не забудьте, что он содержит:	Теги Примечания	Добавить тег Добавить примечания
Общий доступ	проблем -	 своиства документа, сведения о типе контента, имя шаолона и имя автора Настраиваемые XML-данные 	Связанные даты	
Экспорт			Изменено	
Закрыть		Управление документом	Создано	Сегодня, 10:29
	Управление	Возврат, извлечение файла и восстановление несохраненных изменений. Нет несохраненных изменений.	Напечатано	
Учетная	Acidimenticia		Связанные пользо	ователи
Запись			Автор	Dmitry Shurale
Параметры				Добавить автора
			Кем изменено	Еще не сохранен
			Показать все свойства	

В отобразившемся меню выберите Добавить цифровую подпись.

¢		Документ7 - Word
Сведения	Сведения	
Создать	2	
Открыть	Защита документа Все могут открывать, копировать и изменять любую часть этого документа	Свойства * Размер Еще не сохранено
Сохранить	Защита документа *	Число страниц 1 Число слов 50
Сохранить как	Пометить как окончательный Пометка документа как окончательного и	Общее время правки 8 мин Название Добавить название
Печать	нередактируемого	Теги Добавить тег Примечания Добавить примечания
Общий доступ	Защита документа паролем та, имя шаблона и имя авт	ора примечания добавно примечания
Экспорт	Ограничить редактирование	Связанные даты Изменено
Закрыть	вносить пользователям	Создано Сегодня, 10:29
	Ограничить доступ Ограничить доступ Опредоставление пользователям доступа с ограничением Опредоставление пользователям доступа с ограничением Опредоставление колиподация и рецати	Напечатано
Учетная запись	Соможности изисления, конкрования и нечати	Связанные пользователи
Параметры	Обеспечение целостности документа путем добавления невидимой цифровой подписи	Автор Dmitry Shuralev
Парамстры		Добавить автора
		сем изменено Еще не сохранен
		і юказать все своиства

Если документ ещё не сохранён, Microsoft Office предложит его сохранить. Нажмите Да.

Microsof	ft Word	×				
	Прежде чем добавлять цифровые подписи, необходимо сохранить документ в формате, который их поддерживает. Вы хотите сохранить документ в таком формате?					
	<u>Да</u> Н <u>е</u> т					

Укажите Имя файла, Тип файла и путь, куда необходимо сохранить документ.

関 Сохранение документа				×
🔶 🚽 👻 🛧 🌗 » Этот компьютер » М	Лузыка >	*	ට Поиск: Музыка	م
Упорядочить 🔻 Создать папку				== - ?
💽 Microsoft Word	№ Название	Исполнители Альбом		
🝊 OneDrive				
💻 Этот компьютер				
🚽 main (aladdin.ru				
Документы				
👃 Загрузки				
📰 Изображения				
👌 Музыка				
📃 Рабочий стол				
🖕 Локальный дис 🗡				
<u>И</u> мя файла: Название.docx				~
<u>Т</u> ип файла: Документ Word (*.docx)				~
Авторы: Dmitry Shuralev	Теги: Добавьте ключевое с	Название: Добавьте наз	вание	
🗌 Сохранять эскизы	<u>З</u> аголовок:			
	Из <u>м</u> енить			
 Скрыть папки 		С <u>е</u> рвис	• <u>С</u> охранить	Отмена

Для формирования ЭП в MS Office 2016 по средствам JaCarta PKI, на компьютере должны быть установлены драйверы и утилиты для работы с JaCarta PKI, са ма JaCarta PKI должна иметь цифровой сертификат и быть подсоединена к компьютеру. На экране появится окно **Подписание**. Выберите необходимый **Тип подтверждения и Цель подписания,** нажмите **Подписать**.

Подписание	?	×
П Дополнительные сведения о том, что подписывается		
В документ будет добавлена цифровая подпись. Эта подпись не будет видна при содержимого документа. –	просмот	rpe
<u>Т</u> ип подтверждения:		~
Нет Создал и утвердил данный документ Утвердил данный документ Создал данный документ		
Чтобы добавить сведения о подписавшем, нажмите кнопку «Подробности».	С <u>в</u> едени	19
Тема сертификата: Dmitry Shuralev Кем выдан: Aladdin Private Root(3.15)	И <u>з</u> менит	гь
Подписат <u>ь</u>	Отм	ена

В настоящем примере используется тип **"Создал и утвердил документ",** а **Цель подписания** не указывается. В поле **Тема сертификата** указывает, кому выдан сертификат, которым будет осуществлена подпись.

Подписание	?	×
Дополнительные сведения о том, что подписывается		
В документ будет добавлена цифровая подпись. Эта подпись не будет видна при содержимого документа.	і просмо	rpe
<u>тип подтверждения:</u>		
Создал и утвердил данный документ		\sim
Цель подписания документа:		
Чтобы добавить сведения о подписавшем, нажмите кнопку «Подробности».	С <u>в</u> едени	49
Тема сертификата: Dmitry Shuralev Кем выдан: Aladdin Private Root(3.15)	И <u>з</u> мени	ть
Подписат <u>ь</u>	Отм	іена

В следующим окне введите **PIN-код** от подключённого токена или смарт-карты, нажмите **OK**.

Безопасн	Безопасность Windows							
Смар	Смарт-карта							
Введит	Введите имя пользователя, пароль и ПИН-код.							
	ПИН-код							

Далее произойдёт выработка ЭП и появится сообщение об удачном завершении операции.



Документ подписан.

Существует возможность проверить подпись, для этого перейдите в меню **Файл -> Сведения** и в отобразившемся окне нажмите **Просмотр подписей.**



1.0

В следующем окне, справа, отобразятся все подписи, которыми подписан документ. В настоящем примере используется одна подпись.

I ІОДПИСИ Действительные подписи:					
Dmitry Shur	31.03.2017				

Щёлкните по нужной подписи, далее в отобразившемся меню выберите Состав подписи...



Чтобы просмотреть сертификат пользователя, подписавшего документ, и убедиться в его достоверности, нажмите **Просмотр...**

Состав подписи	?	\times
Подпись действительна — подписанное содержимое не изменял сертификат действителен. Тип подписи: XAdES-EPES	ось и	
<u>Т</u> ип подтверждения:		
Создал и утвердил данный документ		
<u>Ц</u> ель подписания документа:		
Тема сертификата: Dmitry Shuralev Кем выдан: Aladdin Private Root(3.15)	<u>П</u> росмо ⁻	гр
Дополнительные Просмотр сведений о сведения, которые будут подписавшем включены в подпись	Закј	оыть

Отобразится окно свойств сертификата.

戻 Сертификат	Х
Общие Состав Путь сертификации	
Сведения о сертификате	
Этот сертификат предназначается для:	-
 Подтверждает удаленному компьютеру идентификацию вашего компьютера 	
 Защищает сообщения электронной почты Вхол со смарт-картой 	
Кому выдан: Dmitry Shuralev	-
Кем выдан: Aladdin Private Root(3.15)	
Действителен с 01.02.2017 по 01.02.2019	
💡 Есть закрытый ключ для этого сертификата.	
<u>З</u> аявление поставщика	
OK	

Так же можно посмотреть **Состав** сертификата (используемые алгоритмы, серийный номер, срок действия) и **Путь сертификации.**

На этом проверка окончена.

Добавление подписи к документу Microsoft Excel 2016

Для подписания документа откройте необходимый документ.

Перейдите в меню **Файл -> Сведения** и в отобразившемся окне нажмите **Защита книги.** Далее в отобразившемся меню выберите **Добавить цифровую подпись.**

¢				Книга1 - Excel
Сведения	Сведения			
Создать	Защита книги		Свойства -	
Открыть Сохранить	Контролируйте типы изменений, котор Защита вносить в эту книгу. книги *	ые пользователи могут	Размер Название Теги	Еще не сохранено Добавить название Добавить тег
Сохранить как	Пометить как окончательный Пометка книги как окончательной и нередактируемой.		Категории	Добавить категорию
Печать	Зашифровать с использованием пароля Настройка пароля, который требуется для открытия	дьте, что он содержит:	Связанные д Изменено	аты
Общий доступ Экспорт	данной книги.		Создано Напечатано	Сегодня, 11:26
Опубликовать	Эправление типами изменении, которые разрешено вносить в текущий лист.	тение несохраненных	Связанные п	ользователи
Закрыть	Предотвращение нежелательных изменений структуры книги, таких как добавление листов.		мырр	Добавить автора
Учетная запись	Ограничить доступ Предоставление пользователям доступа с ограничением возможности изменения, копирования и печати	браузере	Кем изменено Показать все све	Еще не сохранен ойства
Параметры	Добавить цифровую подпись Обеспечение целостности книги путем добавления невидимой цифровой подписи.	»зователи при просмотре этой		

Дальнейшие шаги полностью совпадают с подписанием документа Word, описанном выше.

Добавление подписи к документу Microsoft Power Point 2016

Для подписания документа откройте необходимый документ.

Перейдите в меню **Файл -> Сведения** и в отобразившемся окне нажмите **Защита презентации**. Далее в отобразившемся меню выберите **Добавить цифровую подпись**.

E		Презентация1 - PowerPoint
Сведения	Сведения	
Создать		(BOĂCTRA *
Открыть	Контролируйте презестнации Контролируйте илы изменений, которые пользователи могут внос	ить в эту Размер Еще не сохранено
Сохранить	презентации т	Число слайдов 1 Число скрытых слайдов 0
Сохранить как	Пометить как окончательный Сметка презентации как окончательной и	Название Добавить название Теги Добавить тег
Печать	нередактируемой.	Категории Добавить категорию
Общий доступ	Назначение пароля, который требуется для открытия презентации. люди с ограниченнь	Связанные даты
Экспорт	Ограничить доступ Предоставление пользователям доступа с ограничением ▶	Изменено Создано Сегодня, 11:23
Закрыть	возможности изменения, копирования и печати <u> </u>	Напечатано
	Собеспечение целостности презентации путем есохраненных измен добавления невидимой цифровой подписи.	ений. Связанные пользователи
Учетная запись		Astop Dmitry Shuralev
Параметры		Добавить автора Кем изменено Била на соуганам
		Показать все свойства

Дальнейшие шаги полностью совпадают с подписанием документа Word, описанном выше.

Защита электронной почты Outlook

Программное обеспечение Microsoft Outlook на протяжении многих лет является наиболее популярным офисным и домашним инструментом в мире для работы с электронной почтой. По сути является полноценным органайзером, предоставляющим функции календаря, планировщика задач, записной книжки и менеджера контактов. Кроме того, MS Outlook позволяет отслеживать работу с документами пакета Microsoft Office.

В настоящем документе показаны примеры на базе Outlook 2016, но его можно использовать и для других более старых версий.

Используя цифровой сертификат, записанный на электронный ключ **JaCarta PKI**, пользователь может с лёгкостью подписать и зашифровать электронное сообщение, тем самым обеспечить защиту сообщения и вложения.

Требования к инфраструктуре

Серверная часть

Windows Server с ролью контроллера домена (AD DC).

Windows Server с ролью центра сертификации (AD CA).

Windows Server с ролью почтового сервера Microsoft Exchange.

⚠ Указанные роли могут быть развёрнуты в рамках одного физического или виртуального сервера Windows. Настоящий документ не рассматривает настройку указанных серверных ролей.

Клиентская часть

Любая клиентская версия Windows сустановленным ПО Microsoft Outlook и Единый Клиент JaCarta.

Принцип работы

Шифрование электронных писем и выработка \проверка электронной подписи играют важную роль при обеспечении информационной безопасности. У пользователей есть электронный ключ JaCarta PKI с цифровым сертификатом и ключевой парой (открытый и закрытый ключ). Третья сторона (Центр сертификации или Удостоверяющий центр) удостоверяет по цифровому сертификату его законного владельца.

Электронная подпись почтовых сообщений производится отправителем почтового сообщения с использованием своего закрытого ключа. При помощи открытого ключа можно проверить правильность цифровой подписи, а также посмотреть информацию об отправителе.

Для **шифрования почтовых сообщений** два пользователя сначала должны обменяться подписанными сообщениями. Почтовое сообщение шифруется отправителем при помощи открытого ключа получателя. Таким образом, любой может зашифровать сообщение для пользователя при помощи открытого ключа, но только владелец закрытого ключа может расшифровать сообщение.

Для надёжной сохранности сертификат и ключ необходимо хранить на USB-токене или смарт-карте JaCarta PKI. При использовании JaCarta PKI только легальный пользователь сможет прочесть зашифрованное для него сообщение. Центр сертификации и почтовый сервер необходимы в инфраструктуре, но настройка электронной подписи и шифрования почтовых сообщений не зависит от них. Настройка ЭП и шифрования почтовых сообщений сводится к настройке программы почтового клиента.

Электронный ключ JaCarta PKI, в отличии от других известных способов хранения, обеспечивает неизвлекаемость ключевой информации на USB-токене или смарт-карте. Неизвлекаемое хранение подразумевает, что ключ из токена или карты не попадает никуда извне, например, на жёсткий диск компьютера или в оперативную память. А при обращении к информации на электронном ключе требуется знание PIN-кода, неправильный ввод которого приведёт к блокировке. Это в свою очередь защищает от подбора комбинации PIN-кода, сводя количество попыток к определённому значению, например, 3.

Для чего нужно шифровать сообщения?

Если вам нужно защитить конфиденциальность сообщения электронной почты, защитить сам текст письма и все вложения, то можно зашифровать это письмо. Шифрование сообщения в Outlook означает, что читаемый обычный текст преобразуется в зашифрованные данные. Расшифровать сообщение для прочтения может только получатель, у которого есть закрытый ключ, соответствующий открытому ключу, использованному для его шифрования. Для получателей, которые не имеют соответствующего закрытого ключа, будет отображаться искажённый текст.

Что подтверждает цифровая подпись?

• Подлинность.

•Цифровая подпись подтверждает личность подписавшего.

• Целостность.

•Цифровая подпись подтверждает, что содержимое документа не было изменено или подделано после заверения.

• Неотрекаемость.

•Цифровая подпись подтверждает происхождение заверенного содержимого. Подписавший не может отрицать свою связь с подписанным содержимым.

А Независимо от времени получения сертификата подписи и состояния его отзыва считается, что подписанные документы с действующей отметкой времени содержат действительные подписи.

Настройка и проверка шифрования и подписи

Настройка параметров безопасности

В главном окне Outlook 2016 выберите Файл -> Параметры.



В отобразившемся окне, в левом меню выберите Центр управления безопасностью и справа нажмите Параметры центра управления безопасностью.

Параметры Outlook		?	×
Общие Почта	Обеспечение безопасности документов, а также защиты и работоспособности компьютера.		
Календарь	Безопасность и другие сведения		
Люди	Дополнительные сведения о защите конфиденциальности и безопасности приведены на сайте Office.com.		
Задачи	Создание защищенных информационных систем		
Поиск	Центр управления безопасностью Microsoft Outlook		
Язык Дополнительно	Центр управления безопасностью содержит параметры безопасности и конфиденциальности. Эти параметры помогают обеспецият безопасность колцьютела. Изменить и не	ностью	
Настроить ленту	рекомендуется.		_
Панель быстрого доступа			
Надстройки			
центр управления безопасностью			
L [ОК	Отме	на

В окне **Центр управления безопасностью** выберите **Защита электронных писем**, отметьте пункт **Добавлять цифровую подпись к исходящим сообщениям**.

Центр управления безопасностью		?	×					
Надежные издатели Шифр	ованная электронная почта							
Параметры конфиденциальности								
Защита электронных писем 🄏	шифровать содержимое и вложения исходящих сооощении							
Обработка вложений	✓ Отправлять подпи <u>с</u> анные сообщения открытым текстом							
Автоматическое скачивание	Запрашивать уведомление S/MIME для всех подписанных сообщений S/MIME							
Параметры макросов	По у <u>м</u> олчанию: Установки S/MIME (D.Shuralev@aladdin-rd.ru) 🔽 Параметр <u>ы</u>							
Программный доступ Цифровые удостоверения (сертификаты)								
	Цифровые удостоверения или сертификаты являются документами, которые обеспечивают безопас ваших электронных транзакций.	ность						
	Опуб <u>л</u> иковать в глобальном списке адресов Импорт/ <u>э</u> кспорт <u>П</u> олучить удостоверение	e						
Читат	ь как обычный текст							
	итать обычные письма как обычный текст							
] Читат <u>ь</u> письма с цифровой подписью как обычный текст							
Сцена	рии в папках							
	азрешить сценарии в общих папках							
P	азрешить сценарии в общедоступных папках							
	ОК	Отм	ена					

Нажмите **Параметры.**

Центр управления безопасностью		?	×
Надежные издатели Параметры конфиденциальности Защита электронных писем Обработка вложений	Шифрованная электронная почта		
Автоматическое скачивание Параметры макросов	Запрашивать уведомление S/MIME для всех подписанных сообщений S/MIME По у <u>м</u> олчанию: Параметр <u>ы</u>		
Программный доступ	Цифровые удостоверения (сертификаты) Ши фровые удостоверения или сертификаты являются документами, которые обеспечивают безопаса ваших электронных транзакций. Опубдиковать в глобальном списке адресов Импорт/экспорт Получить удостоверения Читать как обычный текст Цифровые письма как обычный текст Цитать обычные письма как обычный текст Цитать письма с цифровой подписью как обычный текст Дитать сценарии в общих папках Разрешить сценарии в общедоступных папках	HOCT5	
	ОК	Отм	ена

В отобразившемся окне выберите **сертификат подписи и алгоритм хэширования.** В случае если необходимо выполнить еще и шифрование, то укажите **сертификат шифрования** и **алгоритм шифрования**. В настоящем примере для подписи и шифрования используется один сертификат пользователя, находящийся на **USB-токене JaCarta PKI**.

Изменение настройки безопасности							
Настройка безопасности —— <u>И</u> мя конфигурации:							
Установки S/MIME (D.Shura	lev@aladdin-rd.ru)		~				
Ф <u>о</u> рмат криптографии:	S/MIME		\sim				
✓ <u>Н</u> астройка безопасности	по умолчанию для	і этого формат	a				
✓ Настро <u>й</u> ка по умолчаник	о для всех сообщен	ий					
<u>М</u> етки безопасности	<u>С</u> оздать	Удалит <u>ь</u>					
Сертификаты и алгоритмы							
Сертификат подписи:	Dmitry Shuralev		<u>В</u> ыбрать				
<u>А</u> лгоритм хеширования:	SHA1	~					
Сертификат шифрования:	Dmitry Shuralev		В <u>ы</u> брать				
А <u>л</u> горитм шифрования:	AES (256-bit)	~					
Передавать сертификать	і с сообщением						
		OK	Отмена				

В открывшемся окне можно выбрать нужный сертификат и посмотреть его свойства.

Нажмите ОК.

Безопа	сность Windows		\times			
Выб	ор сертификата					
	Dmitry Shuralev					
	Издатель: Aladdin					
	Действителен с: 01.02.2017 по 01.02.2019					
	Просмотреть свойст	ва сертификата				
			_			
	ОК	Отмена				

Отправка и получение подписанного сообщения

Перейдите в главное меню Outlook 2016 и создайте новое письмо для произвольного получателя.

Заполните необходимые поля для отправки, выберите Параметры -> Подпись.

Нажмите Подпись.

И Кнопки **Подписать** и **Шифровать** доступны только после настроек параметров электронной цифровой подписи и шифрова ния почтовых сообщений. При нажатии кнопки **Подписать** или **Шифровать** не происходит подписи или шифрования сообщения, подпись и шифрова ние происходит непосредственно перед отправкой сообщения, после ввода PIN-кода.

🖬 🔊 🗟 🕆 🤚 = пример подписи - Сообщение (HTML)								
Файл Сообщение Встаяха Параметры Формат техста Рецензирование Q Что сы холите сделять? Параметры Цвета - Дишифты - темы Параметры Дарафиты - состраниць - темы Дарафиты - состраниць - сострани - сострани - сострани - сострани - сострани - сострани - состр				~				
Kong Demity Ichia принер подписи								
Пример подлиси								
Суважением, 340 "Аладдин Р.Д." <u>www.aladdin-rd.ru</u>								

В предыдущем окне нажмите **Отправить,** отобразится окно ввода PIN-кода.

Введите PIN-код и нажмите **ОК.**

	Безопасность Wind	lows		×			
	Смарт-карт						
	Введите имя по						
	E ПИН-	юд					
	пин						
Щелкните здесь для получения дополнительных сведений							
	0	к	Отмена				

Полученное письмо с подписью будет иметь специальную пометку в виде печати 🕇 и дополнительное поле **Подписано.**

. 5	(5 👖 🤟 🗧 пример подписанного сообщения Сообщение (HTML)	• –	□ ×
Файл Со	общение 🛛 🖓 Что вы хотите сделать?		
Г Хдалить Удалить	С Ответить С Ответить всем С Переслать Переслать Ответить всем Переслать Пересла Переслать Пересла Пересла Пересла Пересла Пересла Переслать Пересла	о Масштаб	
Кому @aladdir Копия @aladdir Подписано	Dmitry пример подписанного сообщения. I-rd.ru @aladdin-rd.ru		8
Пример под	писанного сообщения.		
С уважение	м, ЗАО "Аладдин Р.Д." <u>www.aladdin-rd.ru</u>		
Для просмо	ра свойств подписи щелкните значок 😫.		
Цифровая	подпись: правильная Х		
Тема:	c		
От: Полликано:	[D.Shuralev@aladdin.ru		
	Цифровая подпись сообщения является действительной и доверенной.		
	Для просмотра сведений о сертификате, применяемом в цифровой подписи сообщения, нажмите кнопку "Сведения".		
	Сведения		
<u>Предупр</u>	еждать об ошибках в подписанных сообщениях до открытия.		
	<u>З</u> акрыть		

Отправка и получение зашифрованного сообщения

Перейдите в главное меню Outlook 2016 и создайте новое письмо для произвольного получателя.

Заполните необходимые поля для отправки, выберите Параметры -> Подпись.

Нажмите Подпись, нажмите Шифрование.

В письмо вложите произвольный документ, например .txt файл.

B	চ ত	Ŷ									пример подписанн	ого и зашифр	рованного пи	сьма - Сообщени
Файл	Сообщение	Встав	ka 🛛 🗖	Іараметры	Форма	т текста Р	ецензировани	2 Что вы х	отите сделат	ь?				
Темы	Цвета т А. Шрифты т Эффекты т ст Темы	↓ Цвет раницы *	& СК Показа	от Р	Разрешени • Раз	 Шифрова Подписат подписат 	ть Кнопк голосова	И Уведоми И Уведоми ния т Отслеживание	ть о доставк пь о прочтен	е нии	Сохранить отправленнь элемент ~ Дополнительнь	ў 3адержка доставки не параметры	направлять ответы в	
₹	Кому	Dmit												
Отправи	ить						_							
	Тема	при	мер подп	писанного и	и зашифров	анного письма	3							
	Вложение		111.txt 18.5	t	Ŧ									
Это пр С влож	оимер подписа кением.	нного и з	ашифро	званного г	письма.									
С уваж	кением,													
	111 (000000))3).txt — Б.	локнот					-		×				
	Файл Правка	Формат	Вид (Справка										
	это простой	текст								\sim				
	<									>				

И Кнопки **Подписать** и **Шифровать** доступны только после настроек параметров электронной цифровой подписи и шифрования почтовых сообщений. При нажатии кнопки **Подписать** или **Шифровать** не происходит подписи или шифрования сообщения, подпись и шифрование происходит непосредственно перед отправкой сообщения, после ввода PIN-кода.

🚍 🐬 🕐 Работа с вложениями	пример подп	исанного и зашифрованного письма - Сообщение (HTML)	63	– 🗆 🗙
Файл Сообщение Вложения 💡 Что вы хо	отите сделать?			
Открыть Быстрая Отправить Сохранить Сохранить Удалить	Копировать Показать			
Действия	Выделение Сообщение			~
Cp 05.07.2017 16:04				
Dmitry Shuralev				
пример подписанного и зашифрован	ного письма			
Кому Dmitry Shuralev				
111.bxt				
Это пример подписанного и зашифрованного письма.				
С вложением.				
CVRDWOHMOM				
Дмитрий Шуралев				
<u>d.shuralev@aladdin-rd.ru</u> ЗАО "Аладдин Р.Д."	www.aladdin-rd.ru			

Полученное зашифрованное письмо будет иметь специальную пометку в виде замка 📫 ,нажав на который, можно посмотреть свойства безопасности сообщения, в том числе алгоритм шифрования.

Свойства безопасности сообщения	×					
К Тема: пример подписанного и зашифрованного письма						
Сообщения могут шифроваться и содержать слои цифровых подписей. Каждый слой допускает наличие нескольких подписей.						
Слои безопасности						
<u>В</u> ыберите слой для просмотра его описания.						
Уровень шифрования Уровень цифровых подписей Подписано: D.Shuralev						
Описани <u>е</u> :						
ОК: защищено 168-разрядным шифрованием 3DES.						
Следующие кнопки позволяют просмотреть дополнительные сведения или внест изменения в выбранный слой:	ги					
Из <u>м</u> енить доверие Подро <u>б</u> ности Доверие к центру сертификации						
Предупре <u>ж</u> дать об ошибках в подписанных сообщениях <u>З</u> акрыть						

Если это письмо будет перехвачено злоумышленником или даже сам легитимный пользователь откроет его из стороннего места, без сертификата, то ничего кроме темы ему доступно не будет, так как письмо надёжно зашифровано алгоритмом 3DES.



smime.p7m

На этом настройка и проверка шифрования и подписи электронных писем в **Microsoft Outlook 2016** завершена.

Шифрование данных EFS

Во всех операционных системах Microsoft, семейства NT, начиная с Windows 2000 и выше (кроме домашних (home) версий) существует встроенная технология шифрования данных EFS (Encrypting File System). EFS-шифрование основано на возможностях файловой системы NTFS и архитектуре CryptoAPI и предназначено для быстрого шифрования файлов на жёстком диске компьютера.

Система EFS использует шифрование с открытым и закрытым ключом. Для шифрования в EFS используется личный и публичный ключи пользователя, которые генерируются при первом использовании пользователем функции шифрования. Данные ключи остаются неизменными всё время, пока существует его учётная запись. При шифровании файла EFS случайным образом генерирует уникальный номер, так называемый File Encryption Key (FEK) длиной 128 бит, с помощью которого и шифруются файлы. Ключи FEK зашифрованы мастер-ключом, который зашифрован ключом пользователей системы, имеющего доступ к файлу. Закрытый ключ пользователя защищается хэшем пароля этого самого пользователя.

Данные, зашифрованные с помощью EFS, могут быть расшифрованы только с помощью той же самой учётной записи Windows с тем же паролем, из-под которой было выполнено шифрование. А если хранить сертификат шифрования и закрытый ключ на USB-токене или смарт-карте, то для доступа к зашифрованным файлам потребуется еще и этот USB-токен или смарт-карта, что решает проблему компрометации пароля, так как будет необходимо наличие и дополнительного устройства в виде электронного ключа.

1.0

Одна из важных отличительных особенностей **EFS** от других средств шифрования в Windows - это возможность локальной (stand alone) работы. То есть пользователь создает новый самозаверенный сертификат, записывает его на **JaCarta PKI**, настраивает **EFS** и в дальнейшем получает доступ к необходимым каталогам или файлам только при наличии электронного ключа и знания его PIN-кода.

Ход настройки

Ход настройки делится на 3 этапа

выпуск сертификата шифрования;
настройка директорий шифрования;

•проверка работоспособности.

Выпуск сертификата шифрования

Вначале необходимо выпустить и записать сертификат и закрытый ключ в память JaCarta PKI, для этого выполните следующие действия.

Для OC Windows 8 и выше:

Щёлкните правой кнопкой меню Пуск,



выберите Панель управления.



Для OC Windows 7 и ниже:

Нажмите Пуск, выберите Панель управления.

Корзина		
Google Chrome		
Google Chrome		
Подключение к удаленному рабочему столу	dshuralev	
🧊 Paint	Документы •	
Приступая к работе	Изображения	
indows Media Center		
JaCarta Manager	игры Компьютер	
🦓 Ножницы	Панель управления	
Калькулятор	Устройс Изменение параметров и настройка функциональных возможнос компьютера.	тей
Даписки	Программы по умолчанию	
	Справка и поддержка	
• Все программы		
Найти программы и файлы	Завершение работы	
🚳 😂 🚞 🛛		RU 🔺 🛱 🌓 14:12 29.06.2017

Далее настройка идентична для всех версий OC Windows.

В открывшемся окне выберите Учётные записи пользователей.

📴 Все элементы панели управления					
$\leftarrow \to \ \cdot \ \uparrow$ 🔝 > Панель управлени	🗧 🔿 🗹 🛉 📴 > Панель управления 🔸 Все элементы панели управления				
Настройка параметров компью	тера		Просмотр: Мелкие значки 🔻		
🖌 Flash Player (32 бита)	🏪 Windows To Go	📑 Автозапуск	ا Администрирование		
🔗 Брандмауэр Windows	🐼 Восстановление	💕 Графика и медиа Intel(R)	🔐 Дата и время		
🛢 Дисковые пространства	🔊 Диспетчер Realtek HD	📇 Диспетчер устройств	Диспетчер учетных данных		
• Домашняя группа	🖶 Защитник Windows	🖷 Звук	🗊 Инфракрасная связь		
🕢 История файлов	🔤 Клавиатура	🕼 Мышь	🖳 Панель задач и навигация		
🚨 Параметры индексирования	🔄 Параметры Проводника	🚅 Персонализация	🐻 Подключения к удаленным рабоч		
🥘 Почта	👩 Программы и компоненты	🐻 Программы по умолчанию	🔋 Рабочие папки		
	🔗 Региональные стандарты	🐌 Резервное копирование и восстан	😪 Свойства браузера		
🔜 Система	🏢 Телефон и модем	💶 Управление цветом	📧 Устранение неполадок		
🔚 Устройства и принтеры	🎎 Учетные записи пользователей	🏲 Центр безопасности и обслуживан	🔇 Центр синхронизации		
 Центр специальных возможностей Центр управления сетами и общи Учетные записи пользователе Экран Электр Изменечие параметров учетно записи и паролей пользователе совместно использующих это- компьютер. 		Шифрование диска BitLocker ей ой Язык елей, от	<mark>д</mark> Шрифты		

В открывшемся окне выберите Управление сертификатами шифрования файлов.

82	Учетные записи пользователей		-		×
÷	- 🔶 👻 🛧 🤱 > Панель упра	авления > Все элементы панели управления > Учетные записи пользователей 🗸 🗸	Поиск	в пане	P
	Панель управления — домашняя страница	Внесение изменений в учетную запись пользователя			?
	Администрирование учетных записей	Изменение учетной записи в окне "Параметры компьютера"			
_	<u>Управление сертификатами</u> шифрования файлов	Изменить параметры контроля учетных записей Изменить параметры контроля учетных записей Dmitry Shuralev			
•	Управление профилями пользователей	Управление учетными записями пользователей			
	Изменение переменных среды	Чтобы изменить пароль, нажмите клавиши CTRL+ALT+DELETE и выберите "Сменить пароль".			

Нажмите Далее.

		\times
~	碞 Шифрующая файловая система (EFS)	
	Управление сертификатами шифрования файлов	
	Шифрованная файловая система (EFS) позволяет хранить информацию на жестком диске в зашифрованном формате и выбирать, какие пользователи смогут получать к ней доступ. Шифрование защищает файлы от несанкционированного доступа.	
	Чтобы получить доступ к зашифрованным файлам, требуется сертификат шифрования и ключ расшифровки на компьютере или смарт-карте. Этот инструмент можно использовать для обновления файлов, уже зашифрованных с помощью другого сертификата и ключа.	
	Далее Отмен	9

Выберите самозаверяемый сертификат с сохранением его на смарт-карте и нажмите Далее.

Перед продолжением убедитесь, что JaCarta PKI подсоединена к компьютеру, а на компьютере установлено ПО Единый Клиент.

		\times
←	🔁 Шифрующая файловая система (EFS)	
	Создать сертификат	
	О Создать новый самозаверяющий сертификат и сохранить его на моем компьютере	
	Создать сертификат, чтобы защитить файлы в случае потери компьютера	
	Создать новый самозаверяющий сертификат и сохранить его на моей смарт-карте	
	Создайте сертификат, чтобы защитить файлы в случае потери компьютера. При доступе к файлам, зашифрованным с помощью этого сертификата, необходимо использовать смарт-карту. Вставьте смарт-карту, если применяется этот вариант.	
	Получить сертификат, выданный центром сертификации моего домена Сертификат этого типа использует параметры шифрования, выбранные системным администратором. Подключитесь к домену и в случае использования смарт-карты вставьте ее.	
	<u>Д</u> алее Отм	ена

Введите PIN-код вставленной карты.

Корзина	🚽 Шифрующая файлова	ия система (EFS)		
Google Chrome	Какой тип сертифик Выберите подходящий сертификата шифров	ката вы хотите создать? й вариант для автоматического с ания файлов.	создания и хранения	pted
	 Самозаверяющий с Использу сертифик Самозаве Вставьте Сертифик Убедитеся хранится н 	ертификат на этом компьютере щая файловая система (EFS) Подождите, пока будет созда самозаверяющий сертификат шифрования файлов.	н новый для Отмена	
	Какой тип сертифика	та следует использовать?	ЈаСагtа: проверка доступа 111 Введите пароль пол	ьзователя Отмена Подтвердить
				RU 🔺 🍢 🖶 🌒 15:08

На следующем шаге укажите директории, которые будут связаны с новым сертификатом, при необходимости можно указать все логические диски.

🔁 Шифрующая файловая система (EFS)
Обновить ранее зашифрованные файлы
Выберите папки, содержащие зашифрованные файлы, которые следует связать с новым сертификатом и ключом. Немедленное обновление позволяет избежать потери доступа к зашифрованным файлам в случае утраты прежнего сертификата или ключа.
Папки:
Все логические диски
Отложить перешифрование файлов
Обновление файлов может занять значительное время, которое зависит от количества обновляемых файлов. Если выполнить выход или извлечь смарт-карту в процессе обновления, файлы не будут обновлены.
Далее Отмена

Введите PIN-код ещё раз.

		×
종 📶 💷	фрующая файловая система (EFS)	
Обно Выбер связа позво	рвить ранее зашифрованные файлы оите папки, содержащие зашифрованные файлы, которые следует ть с новым сертификатом и ключом. Немедленное обновление од Безопасность Windows	
утрат <u>П</u> апки — V	ы 1: Новые учетные данные: вставьте смарт-карту, которую вы хотите использовать для шифрования файлов.	
	dshuralev Учетные данные смарт-карты dshuralev@WIN-CAC80KR51PG ріN-код	
LITO 🛄	ОК Отмена	_
Обнов колич смарт	зление файлов может занять значительное время, которое зависит от нества обновляемых файлов. Если выполнить выход или извлечь -карту в процессе обновления, файлы не будут обновлены.	
	Далее От	мена

Сертификат выдан и записан на JaCarta PKI. Нажмите Закрыть.

	X
🚽 Шифрующая файловая система (EFS)	
Ваши зашифрованные файлы были обновлены	
<u>С</u> ведения о сертификате:	
Кому выдан: dshuralev	Просмотр сертификата
Кем выдан: dshuralev	
Действителен до: 05.06.2117	Пр <u>о</u> смотр журнала
	2
	Закрыть

Настройка директорий шифрования

Далее необходимо указать директорию, которая будет зашифрована со всем содержимым, можно зашифровать весь диск со всеми вложенными директориями. В настоящем примере используется директория **encrypted**, находящаяся на **диске С.** Щёлкните правой кнопкой по директории и выберите **Свойства**.



Нажмите Д	Другие.
------------------	---------

)). Свойства: enc	rypted	×
Предыду	ицие версии	Настройка
Общие	Доступ	Безопасность
	encrypted	
Тип:	Папка с файлами	
Расположение	: C:\	
Размер:	109 ME (115 269 35	1 байт)
На диске:	109 ME (115 281 92)) байт)
Содержит:	Файлов: 7; папок: 0)
Создан:	29 июня 2017 г., 15:	06:51
Атрибуты:	Только для чтен (применимо толь)	ия жо к файлам в папке)
	Скр <u>ы</u> тый	Другие
	ок	Отмена Применить

Отметьте флаг Шифровать содержимое для защиты данных.

Дополни	тельные атрибуты
<u> </u>	Установите подходящие параметры для этой папки. При изменении этих параметров будет задан вопрос, следует ли затрагивать вложенные папки и файлы.
Атриб	уты индексирования и архивации
<u></u> a	пка готова для архивирования
<mark>⊽</mark> <u>Р</u> а до	зрешить индексировать содержимое файлов в этой папке в полнение к свойствам файла
Атриб	уты сжатия и шифрования
<u> </u>	кимать содержимое для экономии места на диске
<u> Ш</u>	ифровать содержимое для защиты данных Подробно
	ОК Отмена

Нажмите ОК, нажмите Применить.

В отобразившемся окне выберите **К данной папке и ко всем вложенным папкам и файлам.** И нажмите **ОК.**

Выбор пункта Применение только к этой папке не зашифрует все вложенные ниже директории и файлы в них.

Подтверждение изменения атрибутов
Выбраны следующие изменения атрибутов:
зашифровать
Применить эти изменения только к данной папке или также ко всем вложенным папкам и файлам?
🔘 Применение изменений только к этой папке
К данной папке и ко всем вложенным папкам и файлам
ОК Отмена

Нажмите ОК.

После завершения процесса шифрования зашифрованная директория будет подсвечена другим цветом.


Проверка работоспособности

Сразу после завершения настройки отключите JaCarta PKI, выполните выход из системы или перезагрузку ПК, далее снова войдите в систему без JaCarta PKI.

Перейдите в папку encrypted и попробуйте открыть какой-либо файл из неё. Если все настройки сделаны верно, отобразится предложение вставить смарт-карту.



1.0

🕞 💽 т 📗 🕨 Компью	тер 🕨 Локалы	ный диск (С	:) • encrypted				•	49	Поиск: encrypted		- 0	× Q
Упорядочить 👻 🔝	Открыть 🔻	Печать	Записать на ог	птиче	ский диск Новая	я папка				1		0
🔆 Избранное	Имя	_			Дата изменения	Тип	Размер					
脉 Загрузки 强 Недавние места 💻 Рабочий стол	1 1.rar				25.04.2017 15:27 22.06.2017 18:29 15.03.2017 16:46	Документ Office Файл "RAR" Chrome HTML Do	4 539 KG 94 619 KG 1 077 KG					
🧊 Библиотеки 🛃 Видео	 ∃ 3 ↓ 4 ↓ 5 	G			24.03.2017 14:24 24.03.2017 14:31	Документ Office Документ Office	4 990 KG 4 106 KG					
📄 Документы 📄 Изображения 🎝 Музыка	t t	6e	зопасность Wind Шифрующая Идет шифрован файлу с помощ	iows я фай ие фа ью см	йловая система йла или получение д арт-карты. Введите Г	(EFS) доступа к зашифрованн ПИН-код смарт-карты.	10МУ					
№ Компьютер				dshu Учетн dshura PIN-к	ralev ые данные смарт-ка slev@WIN-CAC80KR5	рты 1PG ОК Отм	ена					
5 Документ Offi	Д ce Open XML	ата изменен Разм	ния: 24.03.2017 16: тер: 3,16 МБ	:46	Дата создания	: 29.06.2017 15:06						
🚱 🥭 [9	<i>ब</i>						RU 🔺 🖞	•	15: 29.06	52 2017

Вставьте смарт-карту, щёлкните по документу ещё раз и введите PIN-код.

Если всё сделано верно, документ откроется и доступ будет получен.



На этом настройка **EFS-шифрования** закончена, доступ к файлам теперь возможен только при наличии **JaCarta PKI и PIN-кода**.

Шифрование данных BitLocker

Во всех операционных системах Microsoft, начиная с Windows Vista и выше, существует встроенная технология шифрования разделов жёстких дисков — BitLocker (BitLocker Drive Encryption). Позже в Windows 7 появилась возможность шифровать ещё и внешние носители (внешние жёсткие диски или USB-накопители).

Шифрование осуществляется симметричным алгоритмом AES (Advanced Encryption Standard). При этом шифруется не весь диск, а размеченные разделы (тома) по отдельности. Ключ шифрования должен безопасно храниться на защищённом носителе. Это может быть TPM (Trusted Platform Module) — специальная микросхема для реализации функций безопасности встроенная, например, в материнскую плату ПК. Другой вариант — хранение ключа на смарт-карте или USB-токене JaCarta PKI, именно этот сценарий рассматривается в настоящем документе. Этот способ один из самых безопасных, пользователю для доступа потребуется наличие смарт-карты и знание PIN-кода. Еще есть возможность получать доступ по паролю и каждый раз ключ будет вырабатываться из пароля, но это и самый небезопасный способ, так как если кто-то узнает ваш пароль, то узнает и ключ.

В случае утери, безвозвратной блокировки или физической поломки смарт-карты, существует механизм восстановления. Для этого создается специальный 48-значный ключ восстановления,

который необходимо хранить отдельно от защищённого ПК, например, в сейфе в виде распечатанного документа.

BitLocker в отличии от **EFS-шифрования** работает по клиент-серверной модели. Требуется наличие сервера и локальная работа технологии невозможна.

EFS-шифрование и доступ к защищённым данным с использованием электронных ключей JaCarta **PKI** рассмотрен в документе — "JaCarta PKI и EFS-шифрование в Microsoft Windows»".

Описание демо-стенда

Демо-стенд состоит из следующих компонентов.

Сервер

Windows Server 2016 Datacenter с установленным программным обеспечением Единый Клиент JaCarta и настроенными ролями сервера Active Directory и Active Directory Certificate Services.

Компонент шифрование **BitLocker** в рамках настоящего документа будет установлена на этот же сервер.

Подробное руководство об установке и настройке Active Directory Certificate Services доступно в документе — "JaCarta PKI для аутентификации в домене Windows Server 2016".

Клиент

Windows 10, введённый в домен с установленным программным обеспечением Единый Клиент JaCarta.

Логический диск этой рабочей станции будет защищён шифрованием **BitLocker** в рамках настоящего документа.

Ход настройки

Настройка происходит на сервере и клиенте, делится на следующие этапы.

На сервере:

•установка компонента шифрования BitLocker;
•редактирование шаблона сертификата пользователя;
•настройка групповых политик для BitLocker на взаимодействие со смарт-картой.

На клиенте:

включение шифрования\защиты диска на клиенте;проверка работоспособности.

Установка компонента шифрования BitLocker

Если ранее на сервере был установлен компонент шифрования BitLocker, перейдите к следующему разделу. Если ранее установлен не был, установите компонент. Для этого выполните следующие действия.

Нажмите Пуск -> Диспетчер серверов.



В отобразившемся окне выберите Управление -> Добавить роли и компоненты.



Отобразится окно мастера добавления ролей и компонентов, для продолжения нажмите Далее.

📥 Мастер добавления ролей и ко	омпонентов	_		×
Перед началом р	работы	KOHE4H mosc	НЫЙ СЕРВ cow.local.te	EP est
Перед началом работы Тип установки	Этот мастер поможет вам установить роли, службы ролей или компоненты. Опр нужно установить, на основании потребностей своей организации, таких как об документам или размещение веб-сайта.	оеделит ощий до	е, что оступ к	
Выбор сервера Роли сервера	Чтобы удалить роли, службы ролей или компоненты: Запустить мастер удаления ролей и компонентов			
Компоненты Подтверждение	Прежде чем вы продолжите, убедитесь, что выполнены следующие задачи: • Учетная запись администратора защищена надежным паролем			
Результаты	 Настроены сетевые параметры, такие как статические IP-адреса Установлены новейшие обновления безопасности из Центра обновления Win Если вам требуется проверить, выполнены ли какие-либо предшествующие нес условия, закройте мастер, выполните необходимые шаги и запустите мастер сни Чтобы продолжить, нажмите кнопку "Далее". Пропускать эту страницу по умолчанию 	dows обходим ова.	лые	
	< <u>Н</u> азад <u>Далее ></u> <u>У</u> станов	ить	Отмена	a

В следующем окне выберите Установка ролей и компонентов.

ᡖ Мастер добавления ролей и к	омпонентов	-		×
Выбор типа установки		КОНЕЧНЫЙ СЕРВЕР moscow.local.test		EP est
Перед началом работы Тип установки Выбор сервера Роли сервера Компоненты Подтверждение Результаты	Выберите тип установки. Вы можете установить роли и компоненты на работаю компьютере, на виртуальной машине или на автономном виртуальном жестком • Установка ролей или компонентов Настройте один сервер путем добавления ролей, служб ролей и компоненто • Установка служб удаленных рабочих столов Установите службы ролей для инфраструктуры виртуальных рабочих столов (создать развертывание на основе виртуальных компьютеров или сеансов.	щем фи і диске і в. (VDI), чт	ізическо (VHD).	ĐM
	< <u>Н</u> азад Далее > Установ	ить	Отмена	a

Отобразится окно добавление новых ролей, нажмите Далее.

🔁 Мастер добавления ролей и ко	омпонентов	- 🗆 X
Мастер добавления ролей и ко Выбор ролей сере Перед началом работы Тип установки Выбор сервера Роли сервера Компоненты Подтверждение Результаты	 Эмпонентов ЭВЕРА Выберите одну или несколько ролей для установки на этом со Роли DHCP-сервер ✓ DNS-сервер (Установлено) Нурег-V Аттестация работоспособности устройств Веб-сервер (IIS) Доменные службы Active Directory (Установленс Режим Windows Server Essentials Службы Active Directory облегченного доступа к Службы Active Directory облегченного доступа к Службы Active Directory of Arterses Службы активации корпоративных лицензий Службы политики сети и доступа Службы политики сети и доступа Службы политики сети и доступа Службы сертификатов Active Directory (Установися) © Службы сертификатов Астиче Directory (Установися) © Службы сертификатов Active Directory (Установися) © Остака сертификатов Active Directory (Установися) © Службы сертификатов Acti	— П Х Конечный сервер north.westeros.loc ервере. Описание DHCP-сервер позволяет централизованно настраивать временные IP-адреса и связанные с ними данные, предоставлять их клиентским компьютерам, а также управлять ими.
	Службы управления правами Active Directory Службы федерации Active Directory <	> Установить Отмена

В отобразившемся окне выбора компонентов отметьте Шифрование диска BitLocker.

ᡖ Мастер добавления ролей и к	омпонентов	– 🗆 X
Выбор компонен	ТОВ	КОНЕЧНЫЙ СЕРВЕР north.westeros.loc
Перед началом работы	Выберите один или несколько компонентов для установки н	а этом сервере.
Тип установки	Компоненты	Описание
Выбор сервера	Cryx6a SNMP Cryx6a Windows Search	Шифрование диска BitLocker позволяет защитить данные на
Роли сервера Компоненты Подтверждение Результаты	 Служба икпвации процессов Windows Служба активации процессов Windows Служба беспроводной локальной сети Соединитель MultiPoint Средства защиты виртуальной машины для упр Средства задиты виртуальной машины для упр Средство просмотра XPS Стандартизированное управление хранилищам Удаленное разностное сжатие Удаленный помощник Управление групповой политикой (Установленс Фильтр Windows TIFF IFilter Фоновая интеллектуальная служба передачи (Bl Функции .NET Framework 3.5 	утерянных, украденных или неверно списанных компьютерах путем шифрования целого тома и проверки целостности компонентов ранней загрузки. Для расшифровки данных эти компоненты должны успешно пройти проверку, а зашифрованный диск должен находиться в исходном компьютере. Для проверки целостности требуется совместимый доверенный платформенный модуль (ТРМ).
	 Функции .NET Framework 4.6 (Установлено 2 из Функции Защитника Windows (Установлено) Шифрование диска BitLocker 	> Установить Отмена

В следующем окне нажмите Добавить компоненты.



Далее нажмите Установить.

눰 Мастер добавления ролей и ко	мпонентов	—		×
Подтверждение у	/становки компонентов	KOHE4H north.	ЧЫЙ CEPB! .westeros.le	EP oc
Перед началом работы Тип установки	Чтобы установить на выбранном сервере следующие роли, службы ролей или нажмите кнопку "Установить".	компоне	≥нты,	
Выбор сервера	Автоматический перезапуск конечного сервера, если требуется			
Роли сервера	На этой странице могут быть отображены дополнительные компоненты (напри администрирования) так как они были выбраны автоматически. Если вы не хот	мер, сре ите уста	едства навлива	ть
Компоненты	эти дополнительные компоненты, нажмите кнопку "Назад", чтобы снять их фла:	жки.		
Подтверждение Результаты	Enhanced Storage Средства удаленного администрирования сервера Средства администрирования компонентов Средства администрирования программы шифрования дисков BitLoc Средство просмотра пароля восстановления BitLocker Средства шифрования диска BitLocker Шифрование диска BitLocker	ker		
	Экспорт параметров конфигурации Указать альтернативный исходный путь			
	< <u>Н</u> азад Д <u>а</u> лее > <u>У</u> станов	ить	Отмена	3

По завершении	установки	компонента	нажмите	Закрыть.
---------------	-----------	------------	---------	----------

📥 Мастер добавления ролей и к	омпонентов	_		×
Ход установки		KOHE4 norti	НЫЙ CEP h.westeros	3EP .loc
Результаты	Просмотр хода установки			
	Установка компонента			
	Установка выполнена на north.westeros.loc.			
	Enhanced Storage Средства удаленного администрирования сервера Средства администрирования компонентов Средства администрирования программы шифрования дисков В Средство просмотра пароля восстановления BitLocker Средства шифрования диска BitLocker Шифрование диска BitLocker	itLocker		
	Этот мастер можно закрыть, не прерывая выполняющиеся задачи. Наб выполнения задачи или откройте эту страницу снова, выбрав на панел "Уведомления", а затем "Сведения о задаче". Экспорт параметров конфигурации	людайте и коман,	а ходо д пункт	м
	< <u>Н</u> азад Д <u>а</u> лее > Закр	ыть	Отмен	a

Редактирование шаблона сертификата пользователя

Чтобы сертификат пользователя **MSCA** мог работать с **BitLocker**, ему необходимо добавить новую политику применения, которой в нём нет по умолчанию.

В рамках настоящего документа будет отредактирован **шаблон JaCarta user**, созданный в рамках документа — **"JaCarta PKI для аутентификации в домене Windows Server 2016".**

Для редактирования шаблона откройте оснастку Центр сертификации (которая была создана в рамках ранее упомянутого документа "JaCarta PKI для аутентификации в домене Windows Server 2016"), далее щёлкните Шаблоны сертификатов и выберите Управление.

 ЦентрСертификации - [Корень консоли\Центр сертификации (Локальн Файл Действие Вид Избранное Окно Справка 	ый)\westeros-NORTH-CA\Шаблоны серти	фикатов] — 🗆 🗙
Корень консоли Ч Центр сертификации (Лок. Ч Шентр сертификации (Лок. С Отозванные сертифи Запросы в ожидани Неудачные запросы Шаблоны сертифи Создать Неудачные сертифи Создать Корень консонторолле Почтовая репликация каталога Поверка подлииности контролле Поверка подлииности кетрегоз Агент восстановления EFS Управление Создать Вид Новое окно отсюда Новый вид панели задач Обновить Экспортировать список Справка	Назначение Агент запроса сертификата Вход со смарт-картой, Проверка под Почтовая репликация службы катало Проверка подлинности клиента, Про Восстановление файлов Шифруюцая файловая система (EFS) Проверка подлинности клиента, Про Проверка подлинности клиента, Про Проверка подлинности клиента, Про Шифруюцая файловая система (EFS) <8с> Подписывание списка доверия (Micr	Действия Шаблоны сертификатов ▲ Дополнительные дей ▶ JaCarta user ▲ Дополнительные дей ▶
Запуск оснастки шаблонов сертификатов		

В открывшемся окне найдите JaCarta user, щёлкните по нему правой кнопкой и откройте его Свойства.

🗷 Консоль шаблонов сертифика	тов				- 🗆 X
Файл Действие Вид Справк	a				
🖛 🔿 🔚 🐹 🖾 🖾 🕞					
🖳 Шаблоны сертификатов (north	Отображаемое имя шаблона	Версия схемы	Bepc	Назначения 🔨	Действия
	🖳 IPSec	1	8.1		Шаблоны сертификатов (🔺
	🕮 IPSec (автономный запрос)	1	7.1		Дополнительные дей 🕨
	JaCarta user Скопировать шаблов	н		т	
	🕮 RAS- и IAS-сеј Подать повторную за	аявку для всех владельнев (сертификат	ов Эд	JaCarta user
	Изменить имена				Дополнительные дей 🕨
	Парана восстан			эн	
	Все задачи			>	
	Д Агент регистр Далить				
	П Администрат				
	🕮 Базовое шиф				
	🗷 Веб-сервер Справка				
	🚇 Вход со смарт-картой	1	6.1		
	🐵 Компьютер	1	5.1		
	🚇 Контроллер домена	1	4.1		
	🚇 Корневой центр сертификации	1	5.1		
	🚇 Маршрутизатор (автономный запрос)	1	4.1		
	🚇 Перекрестный центр сертификации	2	105.0		
	🚇 Подписывание кода	1	3.1	_	
	Подписывание отклика OSPC	3	101.0	Подписание С	
	Подписывание списка доверия сертиф	1	3.1		
	Подчиненный центр сертификации	1	5.I 2.1		
		1	5.1 71		
	Пользователь со смарт-картой	1	11.1		
	Почтовая репликация каталога	2	115.0	Почтовая реп	
	🚇 Проверенный сеанс	1	3.1		
	💷 проверка подлинности Kerberos	2	110.0	Проверка под	
	🖳 Проверка подлинности контроллера д	2	110.0	Проверка под	
	🗷 Проверка подлинности рабочей станц	2	101.0	Проверка под 🗸	
< >>	<			>	

Перейдите во вкладку Расширения, нажмите Изменить.

				-			
Шифрование	Аттеста	ция ключей	Имя	субъекта	Треб	ования выд	ач
Общие		Совместимос	ть		Обработка	а запроса	
Устаревшие ша	зблоны	Расширен	ия	Безопас	сность	Серв	ер
"Изменить". Расширения, вкли Спользовани Основные огр Политики выд Политики выд Сведения о ш	оченные в ие ключа раничения цачи менения аблоне сер	этот шаблон: тификата					
<u>О</u> писание Полити Вход со смарт+ка	ки примене	ния:				Изменить	»
<u>О</u> писание Полити Вход со смарт-ка Проверка подлин Защищенная эле	іки примене артой яности клие эктронная п	ния: нта очта				Изменить	····

© "Аладдин Р.Д.", 2018

В открывшемся окне нажмите Добавить.

Изменение расширения политик при	іменен ×				
Политика применения определяет способ использования сертификата.					
Политики применения:					
Вход со смарт-картой Защищенная электронная почта Проверка подлинности клиента					
Добавить <u>И</u> зменить	<u>У</u> далить				
<u>Считать это расширение критически</u>	M				
ОК	Отмена				

Выберите Шифрование диска BitLocker, нажмите ОК.



Далее нажмите ОК.

Изменение расширения политик применен 🗙
Политика применения определяет способ использования сертификата.
Политики применения:
Вход со смарт-картой Защищенная электронная почта Проверка по вликиости клиента
Шифрование диска BitLocker
<u>До</u> бавить <u>У</u> далить
Считать это расширение критическим
ОК Отмена

Шифрование диска BitLocker появится в описании политики применения.

Шифрование	Аттеста	ция ключей	Имя	субъекта	Требов	зания выда	чи
Общие		Совместимос	ть		Обработка	sanpoca	
Устаревшие шаблоны Расширения Безопасность С				Серве	p		
Чтобы изменить расширение, выделите его и нажмите кнопку "Изменить". Расширения, включенные в этот шаблон: Использование ключа Основные ограничения Политики выдачи Политики применения Сведения о шаблоне сертификата							
<u>О</u> писание Полити	ки примене	ния:			[И <u>з</u> менить.	
Вход со смарт-ка	ртой						
Вход со смарт-ка Защищенная эле Проверка подлин Шифрование диск	ртой ктронная п ности клие ка BitLocker	очта нта 1					~

Нажмите Применить, нажмите ОК.

Настройка групповых политик BitLocker для взаимодействия с JaCarta PKI

Далее необходимо настроить политики шифрования BitLocker для взаимодействия со смарт-картами.

Для этого откройте **Диспетчер серверов -> Средства -> Управления групповой политикой.** Далее правой кнопкой щёлкните **Default Domain Policy** и нажмите **Изменить.**

.____



Откроется окно редактора групповой политики.

Выберите Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Шифрование диска BitLocker



Выберите параметр проверки согласованности правил использования смарт-карт.

Файл Действие Вид Сровка Пользовательска Полозовательска Порокравательска Просотравательска Правсерт политики Просотравательска Правсерт политики Просотравательска Правсерт политики Правсерт политики Посске. Состовние Ксс Составства Пот парамет политики позволяет проверить согласова, Не задана	Редактор управления групповыми пол	итиками		_	ð ×
 Политики ветоза Политики ветоза Пользовательска Пользовательска Порограмма поу усласования сертификатов правили ссолзования сертификатов Программа поу усласования сертификатов Просмотр собы Рабочие папки Рабочие папки	<u>айл Д</u> ействие <u>В</u> ид <u>С</u> правка				
 Политики атоза ∧ Шифрование диска BitLocker Пользовательски Пользовательски Пороводник Програмна по у. Просмотр собып Региспложение и Чименить параметр политики Требования: Региспложение и Не ниже Windows Server 2008 R2 им Windows 7 Соржба установ, Служба установ, Служба установ, Служба удалени Соржа и избудалени Соржа удаление обок Карание сертификата смарт-карта Соржба удалени Соржба удалени собра Срадена обохн Маениче инфо колокет пра в расширенном Запретить перзапись пользователя дла диска, зацищенных собра кала и сопъзвовани карон сари срафиката смарт-карта Соржба удалени собра У даленное удале Маениче	• 🔿 🖄 📰 🗟 🛛 🗊 💙				
 Пользовательски рибликити позволяет проверить согласованность правил использования сертификатов Прогоряма по у. Прогоряная по у. Прогоряная по у. Прогоряная по у. Прогоряная по у. Просмотр собы Рабочие палки Рабочие палки Рабочие палки Рабори для сбер Сняронизация уст ими позволяет сворать палку по ум Не задана Выберите способ восстановления BitLocker в доменны Не задана Выберите способ восстановления диска и уровень стойкости Не задана Выберите способ восстановления диска и уровень стойкости Не задана Выберите способ восстановления диска и уровень стойкости Не задана Выберите способ восстановления диска и уровень стойкости Не задана Выберите способ восстановления пользовате выбрать палку по ум Не задана Выберите способ восстановления пользовате политики позволяет свыбрать палку по ум Не задана Выберите способ восстановления диска и уровень стойкости Не задана Спужбы IS Спужбы удялен Совместимость, Совместимость Совместимость Совместимость Совместимость Узаливаетов произник клочении Вitocker. Узалищенных клоча (СКС) Узалищенных клоча (СКС) Узаливаетов расширенном Установщик Шкоча (СКС) Чаранное упрая Установщик Шкоча (СКС) Соврестимость Установщик Шкоча (СКС) Соврестимость Узалищенных клоча (СКС) Узаливаетов в расширенном Установщик Шкоча (СКС) Чаранное упрая Узаливаетов долая центификатор объекта для проверко пользов	🧮 Политики автоза 🔺 🚞 Пользовательскі	📋 Шифрование диска BitLocker	Состовние	Состояние	Коммент
 Проитрыватель смарт-карт Смарт-карт Смарт-карт Смарт-карт Узменить параметр политики Развертывание п Развертывание п Развертывание п Требования: Не ниже Windows Server 2008 R2 или Windows 7 Сборки для сбор Описание: Этот параметр политики Тот параметр политики Тот параметр политики Похожба журнала Служба урален Службы IIS Службы IIS Службы IIS Сружбы IIS Сружбы IIS Сружбы IIS Совместимость / Порменяется при включении BitLocker. Идентификатор объекта из сортификата. ВitLocker. Этот параметр политики Тот параметр политики Тот параметр политики Поводнет в расциренном исстимость / Удаленное упра Удаленное упра Утановцики Win Фактор дополни Центр мобилые Центр мобилые Центр мобилые 	 Пользовательски Проводник Программа по у. 	позволяет проверить согласованность правил использования сертификатов	 Диски операционной системы Несъемные диски с данными 	Cocrossine	Kommerri
 Расположение и Регистрация уст; Регистрация установания диска и уровень стойкости Не задана Регистрация установание политики позволяет связать идентификато объекта из сертификата смарт-карта Регистрация удаленна Ридентификатор объекта Удаленнае упра Ридентификата опозвоать для проверки подлинности Ридентификата опозвоать для проверки подлинното ВіЦоскег, Ридентификата в расширенном использования илюча (ЕКU) сертификата. ВіЦоскея для порадентр политики проверки подлинности Ридентификата пользовать для диско, защищенното ВіЦоске, Ридентификатор объекта Установщи Киби Ридентификата пользовать для диско, защищенното ВіЦоске, Ридентификата рака в дана Ридентификата расположенти катор объекта Ридентификата в расширенном использования илюча (ЕКU) сертификата в пользовать для проверки подлинности Ридентификата пользовать для диско, защищенното ВіЦоске, Ридентификата расположенти сертификата расположенти на расположени на расположенти на расположени на расположени на расположени н	Проигрыватель Просмотр собыл Рабочие папки Развертывание п	смарт-карт Изменить <u>параметр политики</u> Требования:	 Съемные носители с данными Хранить сведения о восстановлении BitLocker в доменны Этот параметр политики позволяет выбрать папку по ум Выберите способ восстановления пользователями диск 	Не задана Не задана Не задана	Нет Нет Нет
 > Служба журнала: Позволяет связать щентификата объекта из Службы IIS Службы IIS Службы удаленна Солужбы удаленна Совместимость, Совместимость, Совместимость, Совместимость, Содержимое обл Содержимое обл Содержимое обл Содержимое обл Содержимое обл Содержимое обл Содержимое обл Содержимое обл Содержимое обл Содержимое обл Сукаванная оболяет. Удаленная оболяет. Удаленное упра Уудаленное упра Уудаленное упра Уустановщики Win Фактор дополни Центо вобильне Центо вобильне Сопоставля и делитификатор объекта успановщиката пользователя для диска, защищенного BitLocker, Сопоставля и делитификата сризователя для диска, защищенного BitLocker, Сопоставля и делитификата сопоставля и делитификаторо Сопоставля и делитификата сризователя для диска, защищенного BitLocker, Сопоставля и делитификата сопоставля и делитификатор Сопоставля и делитификатор объекта из Содержима сопользователя для диска, защищенного BitLocker, Сопоставля и делитификатор Сопоставля и делитификатор Сопос	> Расположение и Регистрация уст; Сборки для сбор Синхронизация г	Не ниже Windows Server 2008 R2 или Windows 7 Описание: Этот парамето политики	 Выберите метод шифрования диска и уровень стойкости Выберите метод шифрования диска и уровень стойкости Этот параметр политики позволяет выбрать метод шифр Этот параметр политики позволяет унказать уникальные 	Не задана Не задана Не задана Не задана	Нет Нет Нет Нет
Смарт-карта помощью BitLocker. Этот параметр политики применяется при включении Совместимость / вitLocker. Сореда выполнен Идентификатор объекта Удаленная оболк Идентификатор объекта Удаленное упра Идентификата в расширенном Улавление циф определик, какие сертификата Установщик Win поконо использовать для Фактор дополни проверки подлинного BitLocker, сопоставля идентификатор Центр мобильне сертификата пользовать для Центр мобильне сопоставля идентификатор	Служба журнала Служба установа Службы IIS Службы IIS Службы удаленного службы службы службы службы удаленного службы удаленного службы удаленного службы удаленного служб	позволяет связать идентификатор объекта из сертификата смарт-карты с диском, защищенным с	В Запретить перезапись памяти при перезагрузке Этот параметр политики позволяет проверить согласова	Не задана Не задана	Her Her
 Среда выполнен Идентификатор объекта указывается в расширенном использовании ключа (ЕКИ) Удаленная оболк Использовании ключа (ЕКИ) Уравление циф определтись, какие сертификата Фактор дополни проверки подлинности сертификата пользователя для дист докульта. Центр мобильнс сипоставля идентификатор 	Смарт-карта Совместимость, Совместимость і Совместимость і Совместимость і Содержимое обл	помощью BitLocker. Этот параметр политики применяется при включении BitLocker.			
Фактор дополнит проверки подлинности цетовая систем центр мобильнс сертификата пользователя для диска, защищенного BitLocker, споставля идентификатор	 Среда выполнен Удаленная обол: Удаленное упрає Управление циф Угравление циф 	Идентификатор объекта указывается в расширенном использовании ключа (EKU) сертификата. BitLocker может определить, какие сертификаты иожно использовать для			
🛄 Центр обеспечен 🔰 объекта из сертификата с	 Фактор дополни Цветовая систем Центр мобильнс Центр обеспечен 	проверки подлинности сертификата пользователя для диска, защищенного BitLocker, сопоставляя идентификатор объекта и сертификатор			
 Сиветр обновлен Центр обновлен Цифровой ящих Заданным этим параметром Пифрование дик политики. 	> 🤷 Центр обновлен 🎬 Цифровой ящик > 🛄 Шифрование дис	иденти фикатором объекта, заданным этим параметром политики.	· .		
Metho «I lýck» и пані Y	— Меню «Пуск» и пані ♥ Ц	Bacumpannu (Cranganru X	•		

9 параметров

В отобразившемся окне отметьте Включено, нажмите Применить и ОК.

Проверьте значение идентификатора, должно быть так, как показано ниже 1.3.6.1.4.1.311.67.1.1

_	
Этот параметр политики позволяет пр	роверить согласованность правил использования сер — 🛛 🗙
Этот параметр политики позволяет п Предыдущий параметр Следующий	роверить согласованность правил использования сертификатов смарт-карт і параметр
○ <u>Н</u> е задано Комментарий:	^
Включено	
О <u>О</u> тключено	×
Требования к версии:	Не ниже Windows Server 2008 R2 или Windows 7 ^
Параметры:	Справка:
Идентификатор объекта.	Этот параметр политики позволяет связать идентификатор
1.3.6.1.4.1.311.67.1.1	с помощью BitLocker. Этот параметр политики применяется при включении BitLocker.
	Идентификатор объекта указывается в расширенном использовании ключа (EKU) сертификата. BitLocker может определить, какие сертификаты можно использовать для проверки подлинности сертификата пользователя для диска, защищенного BitLocker, сопоставляя идентификатор объекта из сертификата с идентификатором объекта, заданным этим параметром политики.
	Идентификатор объекта по умолчанию равен 1.3.6.1.4.1.311.67.1.1
	Примечание. BitLocker не требует наличия у сертификата атрибута EKU, однако если такой атрибут настроен, ему
	ОК Отмена Применить

Перейдите в раздел **Несъёмные диски с данными** и откройте параметр **настройки использования смарт-карт на несъемных дисках с данными.**



В отобразившемся окне отметьте Включено, нажмите Применить и ОК.

💭 Этот параметр политики позволяет на	строить исг	аользование смарт-карт на несъемных ди — 🛛 🗙
Этот параметр политики позволяет на Предвідущий параметр <u>Следующий</u>	астроить исі і параметр	пользование смарт-карт на несъемных дисках с данными
○ <u>Н</u> е задано Комментарий:		^
Включено		
О <u>О</u> тключено Требования к версии:	Не ниже V	Vindows Server 2008 R2 или Windows 7
Параметры:		Справка:
☐ Требовать использование смарт-карт н несъемных дисках с данными	la	 Этот параметр политики позволяет определять возможность использования смарт-карт для проверки подлинности доступа пользователей к несъемным дискам с данными, защищенными с помощью BitLocker на компьютере. Если вы включите этот параметр, то сможете использовать смарт-карты для проверки подлинности доступа пользователя к диску. Вы можете сделать проверку подлинности с использования смарт-карт барательной, установив флажок «Требовать использования смарт-карт для несъемных дисков с данными». Примечание: Эти параметры применяются при включении BitLocker, а не при разблокировке диска. BitLocker разрешает разблокировку диска с любыми предохранителями, доступными на диске. Если вы отключите этот параметр политики, пользователи не
		ОК Отмена <u>П</u> рименить

Перейдите в раздел Съёмные носители с данными и откройте параметр настройки использования смарт-карт на съёмных носителях с данными.

Редактор управления групповыми политиками			-	o ×
Файл Действие Вид Справка				
> Расположение и датчики	Съемные носители с данны	ми		
Регистрация устройства				
Сборки для сбора данных и предварит	Этот параметр политики		Состояние	Состояние
Синхронизация параметров	позволяет настроить		🖹 Управление использованием BitLocker для съемных диск	Не задана
> Служба журнала событий	съемных носителях с данными		🔛 Этот параметр политики позволяет настроить использов	Не задана
Служба установки ActiveX			🗄 Запретить запись на съемные диски, не защищенные Bit	Не задана
🧰 Службы IIS	Изменить параметр политики	^	🗄 Этот параметр политики позволяет настроить использов	Не задана
> 📋 Службы удаленных рабочих столов			Применить тип шифрования диска к съемным носителя	Не задана
🖺 Смарт-карта	Гребования:		Разрешить доступ к съемным дискам с данными, защищ	Не задана
Совместимость драйверов и устройст	не ниже windows Server 2008 К2 иди Windows 7		Этот параметр политики позволяет настроить использов	Не задана
Совместимость приложений			Выбор методов восстановления съемных дисков, защищ	Не задана
📔 Содержимое облака	Описание:			
Среда выполнения приложения	Этот параметр политики			
📔 Удаленная оболочка Windows	позволяет указать, можно ли			
> 🧮 Удаленное управление Windows	проверки подлинности доступа			
🚞 Управление цифровыми правами Win	пользователей к съемным			
📔 Установщик Windows	носителям с данными,			
🦳 Фактор дополнительной проверки под	защищенными с помощью			
📋 Цветовая система Windows Color Syste	BitLocker на компьютере.			
📋 Центр мобильности Windows	Если вы включите этот			
📔 Центр обеспечения безопасности	параметр, то сможете			
> 📋 Центр обновления Windows	использовать смарт-карты для			
📔 Цифровой ящик	проверки подлинности доступа			
🗸 🧰 Шифрование диска BitLocker	пользователя к диску. Вы			
🦳 Диски операционной системы	полинности с использованием			
📔 Несъемные диски с данными	смарт-карт обязательной,			
📔 Съемные носители с данными	установив флажок «Требовать			
🦳 Меню «Пуск» и панель задач	использования смарт-карт для			
> 📔 Панель управления	съемных носителей с данными».			
🦳 Принтеры	Примечание, Эти параметры			
🦰 Сервер	применяются при включении			
» 🦳 Сеть	BitLocker, а не при	h.4		
> 📔 Система	разблокировке диска. BitLocker	~	<	>
A 10 10 10 10 10 10 10 10 10 10 10 10 10	разрешает разодокировку лиска Расширенный (Стандартный /			
0	Стандартный			
о параметров				

В отобразившемся окне отметьте Включено, нажмите Применить и ОК.



Включение защиты (шифрования) носителя со стороны клиента

Теперь пользователь может активировать BitLocker для своего физического диска или съёмного носителя с данными. Для этого выполните следующее.

Перейдите на пользовательскую рабочую станцию.



Откройте Проводник. Выберите диск, который необходимо зашифровать. В настоящем примере это диск E:\.



Откройте его содержимое, чтобы убедиться, что он не пуст.

👝 🛃 📙 🖛		Средства работы с дисками	Новый том (Е	:)		- 0	×
Файл Главная По	оделиться Вид	Управление					~ 🕐
Закрепить на панели Копи быстрого доступа Буфер обм	іровать Вставить 👔	Переместить в т ХУ, Ш Копировать в т □ П Упорядочить	далить ▼ ереименовать	Создать Создать	Свойства	Ц т 2 Выделить 5	
$\leftarrow \rightarrow \times \land = 2$	тот компьютер > Н	овый том (E)			Поиск: Н	овый том (E·)	0
🖈 Панель быстрого д	с Имя	^	Дата изменени	ія Тип		Размер	-
📃 Рабочий стол 🖈	3.0.0.2323 (de	mo)	20.10.2017 16:19	9 Папка с	фаилами		
🕂 Загрузки 📌	интернет вец	цей	20.10.2017 16:19	9 Папка с	файлами файлами		
📋 Документы 📌	1		20.10.2017 16:18	8 Текстова	т ый докум	0 КБ	
📰 Изображения 🖈	📄 menu.lst		18.10.2017 18:5	6 Файл "LS	ST"	2 КБ	
📑 Видео	📄 plpbt.bin		25.02.2012 7:25	Файл "ВІ	IN"	43 KE	
🁌 Музыка	💿 shifthd		22.08.2013 13:24	4 Пакетны	ій файл	5 KE	
🐔 OneDrive	usbdrive.tag	Тип: Пакетный Размер: 4.26 КБ	файл Windows	Файл "Т/	AG"	0 КБ	
💻 Этот компьютер		Дата изменения	a: 22.08.2013 13:2	4			
∰ Сеть	-						
Элементов: 8							

Нажмите назад 🤄 . В открывшемся окне щёлкните правой кнопкой диск Е:\, в отобразившемся меню выберите Включить BitLocker.

💻 🛃 📗 🖵		Средства	работы с дисками	Этот компьютер				-		×
Файл Компьютер	Вид	Уг	правление						^	?
Свойства Открыть Переин	иеновать	Дост мультин	уп к Подключи иедиа - сетевой дис	Границии сетевое ктака расположение	Сткрыть параметры	o y V S V	цалит войст правл	ь или изменить программу ва системы іение	I	
Расположение			Сеть				-			
 Панель быстрого д Рабочий стол Загрузки Загрузки Документы Изображения Изображения Видео Музыка ОпеDrive Этот компьютер Сеть 	с ~ Па	пьютер > апки (б) Вид Загр Муз тройств Лок 49,3 Нов 2,83	Открыть Открыть в но Закрепить на Включить Віт Поделиться Восстановить Добавить в б Закрепить на Форматировать Создать ярль Переименова Свойства	ивом окне и панели быстрого дост Locker ь прежнюю версию иблиотеку и начальном экране ать ик ать	yna	> >	(D:)	Поиск: Этот компьютер	عر 	2

Элементов: 9 🕴 Выбран 1 элемент

:== 📰

Отметьте Использовать смарт-карту для снятия блокировки диска, нажмите Далее.

÷	🎭 Шифрование диска BitLocker (E:)	×
	Выберите способы разблокировки диска	
	<u>И</u> спользовать пароль для снятия блокировки диска	
	Пароли должны содержать прописные и строчные буквы, цифры, пробелы и символы.	
	Введите с <u>в</u> ой пароль	
	Введите пароль еще раз	
	Использовать смарт-карту для снятия блокировки диска	
	Необходимо будет вставить смарт-карту. ПИН-код смарт-карты потребуется при снятии блокировки с диска.	
	Далее Отме	ена

В отобразившемся окне выберите способ сохранить ключ восстановления, в файл или отправить на печать. В настоящем примере используется сохранение ключа в файл, выберите **Сохранить в файл.** Сохранённый файл будет содержать ключ в виде открытого текста, его можно распечатать позже. Этот ключ можно будет использовать для разблокировки диска в случае утери смарт-карты.

Не следует хранить ключ разблокировки на рабочей станции, которая содержит объекты,защищённые этим ключом.

		×
←	🏘 Шифрование диска BitLocker (E:)	
	Как вы хотите архивировать свой ключ восстановления?	
	 Некоторыми параметрами управляет системный администратор. 	
	Если вы забыли свой пароль или потеряли смарт-карту, вы можете использовать ключ восстановления для доступа к диску.	
	→ Сохранить в файл	
	→ Напечатать ключ восстановления	
	<u>Что такое ключ восстановления?</u>	
	<u>Д</u> алее Отмен	а

Далее укажите директорию, в которую будет сохранён файл и его имя.

🔫 Сохранение ключа восстановления BitLocker как	×
슈 · · · 个 🛄 > Этот ком > Рабочий стол 🗸 ゔ	Поиск: Рабочий стол 🔎
Упорядочить 🔻 Создать папку	E= ▼ (?)
 Я Панель быстрогс 	Дата изменения Тип
Рабочий сто. 🖈 Нет элементов, удовлетвор	яющих условиям поиска.
🖊 Загрузки 🖈	
🚰 Документы 🖈	
📰 Изображени 🖈	
📕 Видео	
👌 Музыка	
> 🐔 OneDrive	
🔉 💻 Этот компьютер	
× <	>
Имя файла: Ключ восстановления BitLocker F4B36FAF-6EFE	-4089-B897-0FCE786033A0 ~
<u>т</u> ип файла: Текстовые файлы (*.txt)	~
🔿 Скрыть папки	Со <u>х</u> ранить Отмена

В следующем окне нажмите Да.

В настоящем документе ключ сохраняется на этот же ПК только в качестве примера. Не следует хранить ключ разблокировки на рабочей станции, которая содержит объекты, защищённые этим ключом. Полученный файл вы можете скопировать на несколько носителей или распечатать ключ.



Следующим шагом укажите, какую часть диска требуется зашифровать. Шифровать только занятое место на диске или весь диск. В настоящем примере шифруется весь диск, выберите **Шифровать весь диск** и нажмите **Далее**.

		\times
←	🎭 Шифрование диска BitLocker (E:)	
	Укажите, какую часть диска требуется зашифровать	
	Если вы настраиваете BitLocker на новом диске или ПК, вам достаточно зашифровать только ту часть диска, которая сейчас используется. BitLocker зашифровывает новые данные автоматически по мере их добавления.	
	Если вы включаете BitLocker на уже используемом ПК или диске, рекомендуется зашифровать весь диск. Это гарантирует защиту всех данных — даже удаленных, но еще содержащих извлекаемые сведения.	,
	Шифровать только занятое место на диске (выполняется быстрее, оптимально для новых ПК и дисков)	
	Шифровать весь диск (выполняется медленнее, подходит для уже используемых ПК и дисков)	
	<u>Д</u> алее Отмена	1

Нажмите Начать шифрование.

		\times
÷	🎭 Шифрование диска BitLocker (E:)	
	Зашифровать этот диск?	
	Этот диск можно будет разблокировать только на компьютерах с операционной системой Windows 7 и более поздних версий. Если вы хотите разблокировать этот диск на компьютера: другими версиями Windows, нажмите кнопку "Назад" и создайте пароль.	(c
	Вы сможете разблокировать этот диск с помощью смарт-карты.	
	Процесс шифрования может быть долгим, его длительность зависит от размера диска.	
	До завершения шифрования защита файлов не обеспечивается.	
	Начать шифрование Отме	на

Строка состояния отобразит процесс завершения в процентах. Длительность процесса зависит от размера диска и может занимать продолжительное время.



По завершении процесса нажмите Закрыть.

Шифрование диска BitLocker	×
Шифрование Е: завершено.	
	<u>З</u> акрыть
<u>Управление BitLocker</u>	

Выполните перезагрузку рабочей станции.

На этом настройка BitLocker завершена.

Проверка работоспособности

После перезагрузки подключите JaCarta PKI и откройте проводник. Если ранее всё было верно настроено, около зашифрованного диска появится значок замка. Щёлкните локальный диск (E:) и выберите вариант разблокировки смарт-карта.



Введите PIN-код, нажмите ОК.

Смарт-карта		
Смарт-карта Введите имя пользователя, пароль и ПИН-код. ПИН-код		
ћин-код		
Щелкните здесь для получения дополнительных сведений		
	ОК	Отмена

🚔 🖸 📙 🖛 I		Средства работы с дис	_{ками} Новый том (I	E:)	_	
Файл Главная Под	делиться Вид	Управление				~ 🕐
*	È 🗋 👗	🖕 Переместить в 🔻	🗙 Удалить 👻			
Закрепить на панели Копир быстрого доступа	овать Вставить 🔝	[Копировать в 🔻	📑 Переименовать	Создать папку	Свойства 🧹	Выделить
Буфер обме	ена	Упоряд	очить	Создать	Открыть	
← → √ ♠ 🚔 → Эт	гот компьютер > Н	Іовый том (E:) »	~	О Поиск:	Новый том (Е	.) , 0
📌 Панель быстрого дс	Имя	^	Дата изменен	ия Тип		Размер
📃 Рабочий стол 🖈	3.0.0.2323 (de	mo)	20.10.2017 16:1	9 Папка с	файлами	
🖊 Загрузки 🛛 🖈	new		20.10.2017 16:1	8 Папка с	файлами	
🛱 Документы 📌	интернет ве	цей	20.10.2017 16:1	9 Папка с	файлами	
📰 Изображения 🖈	1		20.10.2017 16:1	8 Текстов	ый докум	0 KE
Паларана и предоктория и предо	i menu.lst		18.10.2017 18:5	6 Файл "L	ST"	2 KE
видео	plpbt.bin		25.02.2012 7:25	о Файл "В	IN"	43 KE
ПУЗыка	less shifthd		22.08.2013 13:2	4 Пакетнь	ый файл	5 KE
\land OneDrive	usbdrive.tag		12.12.2009 21:5	64 Файл "T	AG"	0 КБ
💻 Этот компьютер						
💣 Сеть						
Элементов: 8						

После ввода PIN-кода содержимое диска откроется автоматически.

В проводнике изображение диска сменится с закрытого замка на открытый.



Разблокировка ключом восстановления

В случае утери смарт-карты доступ можно восстановить с помощью сохранённого или

распечатанного ранее ключа. Для этого откройте файл с ключом или достаньте его распечатку.



Далее щёлкните зашифрованный диск и выберите вариант разблокировки **Введите ключ** восстановления.

				BitLocker (E:)
💻 📝 🛄 🖛		Средства работы с дисками	Этот компьютер	Смарт-карта
Файл Компьютер	Вид	Управление		
🗸 Свойства			Уда.	Введите ключ восстановления
Сткрыть Переименовать Переименовать		Подключить Добавить с сетевой диск трасполож Сеть	етевое Открыть ение параметры 🔂 Упр	ПК Автоматически разблокировать на этом
← → ~ ↑ 💻 ›	Этот ком	пьютер		
📌 Панель быстрого	дс			^
📃 Рабочий стол	*	Загрузки	Изоб	ражения
🕂 Загрузки	* 1			
🖆 Документы	*	Музыка	Рабо	чий стол
Изображения	* -		.	
видео	∨Ус	тройства и диски (3) —		
🧊 Музыка 🐔 OneDrive		Локальный диск (С:) 49,3 ГБ свободно из 59,	9 F6 OVD	RW дисковод (D:)
💻 Этот компьютер				
💣 Сеть		Локальный диск (Е:)		,
Элементов: 9 👘 Выбра	ан 1 элеме	нт		

царана средс Файл Компьютер Вид	тва работы с дисками Этот компьютер Управление	BitLocker (E:)
Свойства Открыть Переименовать Д Расположение	Фоступ к Подключить Добавить сетевое ьтимедиа • сетевой диск • расположение Сеть	Введите 48-значный ключ восстановления, чтобы разблокировать этот диск. (ИД ключа: F4B36FAF)
🔶 🔶 👻 🛧 📃 > Этот компьютер	p	
📌 Панель быстрого дс 🖂 Папки (6)	_
 Рабочии стол у Загрузки Загрузки 	Видео	До
III Документы 💉 💽 Изображения 🖈 💽 Изображения 🖈 📑 Видео	Загрузки	Из
Музыка ОпеDrive	Музыка	Pat
Устройс	ства и диски (3)	
Сеть	Локальный диск (С:) 49,2 ГБ свободно из 59,9 ГБ	DV
ر 😂 ا	Локальный диск (Е:)	
		Разблокировать
Элементов: 9 Выбран 1 элемент		
📲 🔎 🗇 🧲 📒		へ 🌄 (小) ヺ PYC 11:19 24.10.2017

В отобразившемся окне введите 48-значный ключ восстановления и нажмите Разблокировать.

🚔 🛃 📙 🛨		Средства работы с дис	ками:	Новый том (Е:)	-	
Файл Главная По	делиться Вид	Управление					~ 🕐
Закрепить на панели Копи быстрого доступа Буфер обм	ровать Вставить	🙀 Переместить в 🔻 🛄 Копировать в 🛪 Упоря/	🗙 Удал 🗐 Пер	пить - еименовать	Создать Создать	Свойства	Выделить
← → ~ ↑	тот компьютер > Н	овый том (E:) »		~	 Поиск: Новый том (// 		E:) , p
 Панель быстрого до Рабочий стол Загрузки Загрузки Документы Документы Изображения Видео Музыка ОпеDrive Этот компьютер 	Имя 	^ то) цей	2 2 2 2 1 1 2 2 1	Цата изменени 20.10.2017 16:19 20.10.2017 16:18 20.10.2017 16:19 20.10.2017 16:18 8.10.2017 16:18 8.10.2017 18:56 25.02.2012 7:25 22.08.2013 13:24 2.12.2009 21:54	я Тип Папка с Папка с Папка с Текстови Файл "Ц Файл "В Пакетнь Файл "Т,	файлами файлами файлами ый докум 5T" IN" IN" IA файл AG"	Размер 0 КБ 2 КБ 43 КБ 5 КБ 0 КБ
💣 Сеть Элементов: 8							

После ввода ключа откроется содержимое диска.

Отключение BitLocker

Для отключения BitLocker щёлкните правой кнопкой по зашифрованному диску и выберите Управление BitLocker.



В отобразившемся окне выберите **отключить BitLocker** напротив того диска, для которого нужно выполнить отключение.



В отобразившемся окне предупреждения нажмите Отключить BitLocker.

Расшифрование как и зашифрование может занимать продолжительное время, зависит от объёма диска.

Шифрование диска BitLocker	Х
Отключить BitLocker	
Ваш диск будет расшифрован. Это может занять значительное время, но вы можете продолжать пользоваться компьютером.	
Отключить BitLocker Отмен	ia

По завершении нажмите Закрыть.

Шифрование диска BitLocker	×
Расшифровка Е: завершена.	
	<u>З</u> акрыть
<u>Управление BitLocker</u>	

Теперь BitLocker отключён.

Контакты, техническая поддержка

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания "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-rd.ru (общий)

Web: www.aladdin-rd.ru

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

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через Web-сайт:

www.aladdin-rd.ru/support/index.php

Для оперативного решения вашей проблемы укажите используемый вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

Регистрация изменений

Версия	Изменения
1.0	Исходная версия документа

© "Аладдин Р.Д.", 2018

Стр. 178



Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, №3442 от 10.11.17 Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17 Лицензия Министерства обороны РФ № 1384 от 22.08.16 Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011 Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15 Аpple Developer

© ЗАО "Аладдин Р.Д.", 1995–2018. Все права защищены.

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