



Модуль «Мониторинг и управление сертификатами ЭП» (ЭОС РКИ-сервис)

**Руководство администратора и
пользователя**



ГРУППА КОМПАНИЙ «ЭОС»

Модуль «Мониторинг и управление сертификатами ЭП» (ЭОС РКИ-сервис)

Руководство администратора и пользователя

Москва
2024

В данном документе приведены сведения о порядке установки, настройки и применения модуля «Мониторинг и управление сертификатами ЭП» (ЭОС PKI-сервис).

Книга не является полной документацией к программному обеспечению. Для использования программы необходимо наличие других книг, включаемых в комплект.

Модуль «Мониторинг и управление сертификатами ЭП» (ЭОС PKI-сервис) постоянно совершенствуется и, в связи с этим, возможны некоторые несоответствия, касающиеся описания пользовательского интерфейса.

Документация разработана специалистами ГРУППЫ КОМПАНИЙ «ЭОС».

Модуль «Мониторинг и управление сертификатами ЭП» (ЭОС PKI-сервис) является торговой маркой ГРУППЫ КОМПАНИЙ «ЭОС».

Право на тиражирование программных продуктов и документации принадлежит ГРУППЕ КОМПАНИЙ «ЭОС».

Все упомянутые в данном издании товарные знаки и зарегистрированные товарные знаки принадлежат своим законным владельцам.

© ГРУППА КОМПАНИЙ «ЭОС». Все права защищены

107113, Москва, ул. Шумкина, д. 20 стр. 1.

Тел/факс: (495) 221-24-31

e-mail: support@eos.ru

<http://www.eos.ru>

АННОТАЦИЯ

Настоящие методические рекомендации предназначены для администратора, осуществляющего установку и настройку модуля «Мониторинг и управление сертификатами ЭП» (ЭОС PKI-сервис), а также для пользователей, выполняющих операции по управлению сертификатами с использованием данного модуля.

СОДЕРЖАНИЕ

1.	ОПИСАНИЕ НАЗНАЧЕНИЯ И ПРИМЕНЕНИЯ ЭОС РКІ-СЕРВИС	8
1.1.	Область применения РКІ.....	8
1.2.	Системные требования	8
1.2.1.	Список поддерживаемых ОС	8
1.2.1.1.	Требования к программному обеспечению для Windows	8
1.2.1.2.	Требования к программному обеспечению для Linux	9
1.2.2.	Требования к аппаратному обеспечению	9
1.3.	Состав и назначение компонентов	9
1.3.1.	Служба наблюдения.....	9
1.3.2.	Служба оповещения	9
1.3.3.	Графический интерфейс	9
1.3.4.	Служба обмена информацией по сертификатам с СПО КАРМА	10
2.	УСТАНОВКА РКІ НА LINUX	11
2.1.	Список поддерживаемых ОС	11
2.2.	Подготовка серверов к установке системы	11
2.2.1.	Требования	11
2.2.2.	Запуск терминала	11
2.2.3.	Установка и настройка необходимых компонентов	11
2.2.3.1.	Установка дополнительного ПО	11
2.2.3.1.1.	Установка "КриптоПро"	11
2.2.3.1.2.	Установка "Кармы"	13
2.2.3.1.3.	Активация службы "carma.service"	13
2.3.	Установка системы	14
2.3.1.	Подготовка файлов дистрибутива	14
2.3.1.1.	Распаковка файлов системы в целевом каталоге установки	14
2.3.1.2.	Переход в директорию сборки	14
2.3.2.	Размещение контейнера .rpx на сервере	15
2.3.3.	Установка службы сервера приложений.....	15
2.3.3.1.	Проверка портов сервера приложений.....	15
2.3.3.1.1.	Конфликт портов при работе "Кармы"	15
2.3.3.2.	Описание параметров скрипта configure_pkisrv_linux.sh	18
2.3.3.3.	Пример вызова скрипта configure_pkisrv_linux.sh.	20
2.3.3.4.	Проверка установки службы сервера приложений	20
2.3.4.	Установка фронт-энд web-сервера	21
2.3.4.1.	Проверка порта frontend сервера.....	21
2.3.4.2.	Описание параметров скрипта configure_pkiweb_linux.sh	22

2.3.4.3.	Примеры вызова скрипта <code>configure_pkiweb_linux.sh</code>	24
2.3.4.4.	Добавление имени сайта в <code>hosts</code>	24
2.3.4.5.	Проверка установки системы.....	24
2.3.5.	Перед началом работы.....	24
2.4.	Перенос данных с прежних версий PKI (< v3.0.0).....	25
2.4.1.	Остановка сервиса прежней версии.....	25
2.4.2.	Остановка сервиса текущей версии.....	25
2.4.3.	Перенос хранилищ сертификатов.....	25
2.4.4.	Перенос файла конфигурации.....	26
2.4.5.	Редактирование файла конфигурации для обеспечения совместимости.....	26
2.4.6.	Выдача необходимых прав перенесённым каталогам и файлам.....	29
2.4.7.	Возобновление работы сервиса текущей версии PKI.....	29
2.4.8.	Сохранение настроек для добавления недостающих параметров.....	29
2.5.	Обновление системы.....	29
2.6.	Удаление системы.....	29
2.7.	Очистка неиспользуемых дистрибутивов предыдущих версий.....	30
3.	УСТАНОВКА PKI НА WINDOWS.....	31
3.1.	Список поддерживаемых ОС.....	31
3.2.	Подготовка серверов к установке системы.....	31
3.2.1.	Требования.....	31
3.2.2.	Запуск powershell.....	31
3.2.3.	Настройка IIS.....	31
3.2.3.1.	Десктопная ОС.....	31
3.2.3.2.	Серверная ОС.....	32
3.2.4.	Установка и настройка необходимых компонентов.....	33
3.2.4.1.	Включение реверс прокси.....	34
3.2.4.2.	Установка дополнительного ПО.....	35
3.3.	Установка системы.....	36
3.3.1.	Подготовка файлов дистрибутива.....	36
3.3.1.1.	Распаковка файлов системы в целевом каталоге установки.....	36
3.3.1.2.	Переход в директорию установки.....	36
3.3.2.	Размещение контейнера .rfx на сервере.....	37
3.3.3.	Установка службы сервера приложений.....	37
3.3.3.1.	Проверка портов сервера приложений.....	38
3.3.3.2.	Описание параметров скрипта <code>configure_pkisrv_windows.ps1</code>	38
3.3.3.3.	Пример вызова скрипта <code>configure_pkisrv_windows.ps1</code>	41
3.3.3.4.	Проверка установки службы сервера приложений.....	41

3.3.4. Установка фронт-энд web-сервера	42
3.3.4.1. Конфигурирование привязки сайта и HSTS (HTTP Strict Transport Security)	42
3.3.4.2. Проверка порта frontend сервера.....	43
3.3.4.3. Описание параметров скрипта configure_pkiweb_windows.ps1	43
3.3.4.4. Пример вызова скрипта configure_pkiweb_windows.ps1	46
3.3.4.5. Добавление имени сайта в hosts.....	46
3.3.4.6. Проверка установки системы	46
3.3.5. Перед началом работы	47
3.4. Перенос данных с прежних версий PKI (< v3.0.0).....	47
3.4.1. Остановка пула и сайта прежней версии	47
3.4.1.1. Вручную	47
3.4.1.2. PowerShell.....	48
3.4.2. Остановка пула и сайта текущей версии	48
3.4.2.1. Вручную	48
3.4.2.2. PowerShell.....	49
3.4.3. Перенос хранилищ сертификатов.....	49
3.4.4. Перенос файла конфигурации.....	50
3.4.5. Редактирование файла конфигурации для обеспечения совместимости	50
3.4.6. Возобновление работы пула и сайта текущей версии PKI.....	52
3.4.6.1. Вручную	52
3.4.6.2. PowerShell.....	53
3.4.7. Сохранение настроек для добавления недостающих параметров.....	53
3.5. Обновление системы	54
3.6. Очистка неиспользуемых дистрибутивов предыдущих версий.....	54
4. ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ	56
4.1. Основные понятия	56
4.2. Среды функционирования PKI-сервиса.....	57
4.3. Функции PKI-сервиса	58
4.4. Компоненты PKI-сервиса.....	58
4.4.1. Служба наблюдения.....	58
4.4.2. Служба оповещения.....	58
4.4.3. Графический интерфейс	58
4.4.4. Служба обмена информацией по сертификатам с СПО КАРМА	58
4.5. Требования среды функционирования PKI-сервиса	59
4.5.1. Требования к аппаратному обеспечению	59
4.5.2. Требования к системному и служебному ПО.....	59

4.5.3.	Требования к сетевому окружению, расположению и доступности.....	59
4.5.3.1.	Доступность почтового сервера, способа подключения и наличие учетной записи.....	59
4.5.3.2.	Доступность сервиса для подключения СПО КАРМА с компьютеров организации.....	59
4.5.3.3.	Доступность внутреннего УЦ (НЭП)	60
4.5.3.4.	Доступ в интернет (КЭП)	60
4.6.	Установка, обновление, создание резервной копии и удаление ЭОС РКІ- сервиса	60
4.7.	Интерфейс.....	60
4.7.1.	Запуск	60
4.7.2.	Выход	60
4.7.3.	Замечание по модели безопасности	60
4.7.4.	Доступные из интерфейса операции с сертификатами	61
4.7.5.	Элементы интерфейса.....	61
4.7.5.1.	Основное окно	61
4.7.5.2.	Страница «Настройки»	62
4.7.5.3.	Панель «Общие настройки»	63
4.7.5.4.	Панель «Импорт промежуточных и корневых сертификатов КЭП»	63
4.7.5.5.	Панель «Параметры ргоху»	64
4.7.5.6.	Панель «Параметры отправки e-mail уведомлений»	64
4.7.5.7.	Панель «Обновление статусов сертификатов».....	65
4.7.5.8.	Панель «Параметры проверки целостности хранилищ»	65
4.7.5.9.	Панель «Импорт сертификатов из подписей»	66
4.7.6.	Страница «Статус».....	66
4.7.7.	Страница «Хранилища сертификатов»	67
4.7.8.	Страница просмотра списка сертификатов определенной категории	68
4.8.	Стандартные операции в ЭОС РКІ-сервис.....	71
4.8.1.	Добавление сертификатов для наблюдения ЭОС РКІ-сервисом.....	71
4.8.1.1.	Автоматический импорт сертификатов Аккредитованных УЦ РФ (КЭП)	71
4.8.1.2.	Файловый импорт.....	72
4.8.1.2.1.	Добавление одиночного сертификата	72
4.8.1.2.2.	Операция импорта корневого сертификата (ограничения и ответственность).....	73
4.8.1.2.3.	Файлы, содержащие коллекцию сертификатов (.p7b).....	74
4.8.1.2.4.	Массовый импорт из базы данных СЭД «ДЕЛО»	74
4.8.1.2.5.	Импорт сертификатов с помощью ПО КАРМА.....	74
4.8.1.3.	Исключение сертификатов из наблюдения.....	75
4.8.1.3.1.	Автоматическое по сроку истечения хранения	75
4.8.1.3.2.	Ручное.....	75

4.8.1.3.3.	Ручное массовое	76
4.9.	Приложение 1	77
4.9.1.	Процесс массового экспорта сертификатов из хранилищ Windows (в файл *.p7b).....	77
4.10.	Приложение 2	82
4.10.1.	Настройка СПО КАРМА на компьютерах организации для работы с ЭОС РКИ-сервис	82
4.10.1.1.	Настройка связки «ДЕЛО-КАРМА» для работы с ЭОС РКИ-сервис	82
4.10.1.2.	Настройка СПО КАРМА (расширение «Проводника») для работы с ЭОС РКИ-сервис	83
4.10.1.2.1.	Получение доступа для серверной "Кармы"	83
4.10.1.2.2.	Получение доступа для "Кармы" удалённого ПК	84
4.11.	Приложение 3	86
4.11.1.	Пример E-mail-оповещения от ЭОС РКИ-сервис	86
4.12.	Приложение 4	86
4.12.1.	Описание использования фильтров полей сертификатов при рассылке e-mail уведомлений	86
4.12.1.1.	Подстановочный знак *	87
4.12.1.2.	Примеры строк фильтрации таблицы адресов	87
5.	РУКОВОДСТВО ПО ИМПОРТУ СЕРТИФИКАТОВ ПОЛЬЗОВАТЕЛЕЙ ИЗ БД СЭД «ДЕЛО»	92
5.1.	Назначение.....	92
5.2.	Установленные ограничения	92
5.3.	Описание процесса импорта	92
5.4.	Порядок импорта.....	92
5.4.1.	Шаг 1. Экспорт из базы данных ДЕЛО	92
5.4.2.	Шаг 2. Импорт в ЭОС РКИ-сервис	92

1. ОПИСАНИЕ НАЗНАЧЕНИЯ И ПРИМЕНЕНИЯ ЭОС РКИ-СЕРВИС

В данном разделе приведены сведения об области применения, а также составе и назначении компонентов модуля «Мониторинг и управление сертификатами ЭП» (ЭОС РКИ-сервис).

1.1. Область применения РКИ

Модуль «Мониторинг и управление сертификатами ЭП» (ЭОС РКИ-сервис) – это технологичное решение, которое позволит организовать централизованное управление жизненным циклом сертификатов проверки электронной подписи от выпуска до прекращения действия. Модуль используется для электронного документооборота во внутренних корпоративных системах, а также для обмена юридически значимыми электронными документами с контрагентами.

ЭОС РКИ-сервис обеспечивает:

- Централизованное хранение и ведение реестра сертификатов ЭП организации и корреспондентов;
- Учёт, статистику и управление сертификатами организации;
- Автоматический импорт сертификатов Аккредитованных УЦ РФ (КЭП);
- Импорт актуальных используемых сертификатов из базы СЭД «ДЕЛО»;
- Автоматическую актуализацию статуса сертификатов КЭП и НЭП;
- Оповещение по e-mail и информирование из графической оболочки (окончание срока действия сертификатов и/или закрытых ключей).

1.2. Системные требования

1.2.1. Список поддерживаемых ОС

- Alt Linux (версии Сервер 10);
- Windows (версии Windows 10, Server 2019).

1.2.1.1. Требования к программному обеспечению для Windows

- Добавлена роль «Веб-сервер IIS» (Web Server IIS) / активированы службы IIS (для десктопной версии ОС).
- Установлены компоненты:
 - пакет ASP.NET Core 6.0 Runtime (v6.0.11) - Windows Hosting Bundle;
 - Microsoft Application Request Routing 3.0;
 - URL Rewrite Module 2.1.
- Установлено дополнительное ПО:
 - «Карма» 56.2.436 и выше;
 - «КриптоПро CSP» 5.0 (5.0.11455) и выше;
 - Пакеты Microsoft Visual C++ Redistributable x86 и x64.
- Наличие SSL-сертификата, подтверждающий домен (Domain-validated certificate).

1.2.1.2. Требования к программному обеспечению для Linux

- Имеется доступ к учётной записи root.
- Установлен пакет dotnet-aspnetcore-runtime-6.0.
- Установлен и запущен web-сервер NGINX.
- Установлено дополнительное ПО:
 - «Карма» 56.2.456 и выше;
 - «КриптоПро CSP» 5.0 R2 (5.0.12000) и выше;
- Наличие SSL-сертификата, подтверждающий домен (Domain-validated certificate).

1.2.2. Требования к аппаратному обеспечению

- Выделенный сервер либо виртуальная машина.
- Не менее 2 ядер процессора.
- Не менее 1 Гб оперативной памяти.
- Не менее 500 Мб дискового пространства + 10 Мб на каждую 1000 наблюдаемых сертификатов.

1.3. Состав и назначение компонентов

PKI состоит из следующих компонентов:

- Служба наблюдения.
- Служба оповещения.
- Графический интерфейс.
- Служба обмена информацией по сертификатам с СПО КАРМА.

1.3.1. Служба наблюдения

Основной программный компонент ЭОС PKI-сервиса. Веб-приложение. Обеспечивает централизованный контроль, мониторинг и обработку информации из сертификатов пользователей, систем, сайтов и пр. Предоставляет ее остальным компонентам. Исполняется в фоновом режиме (как служба). Внутри службы периодически запускается процесс актуализации статусов сертификатов. Предоставляет актуальные цепочки и статусы сертификатов для проверки электронных подписей, как в системе квалифицированной электронной подписи (КЭП), так и при использовании внешних или внутриорганизационных Удостоверяющих Центров.

1.3.2. Служба оповещения

С установленной периодичностью отбирает сертификаты, требующие внимания оператора (истечение срока действия сертификата и/или закрытого ключа) и оповещает о них посредством e-mail. Запускается периодически по настройке или принудительно из интерфейса.

1.3.3. Графический интерфейс

Веб-сайт для отображения, фильтрации, сортировки, отбора и экспорта информации по наблюдаемым сертификатам, настройки и интерактивного

взаимодействия сервиса с оператором. Предоставляет доступ к стандартным операциям ЭОС РКІ-сервис таким как:

1. Добавление в сервис наблюдения единичного сертификата (файл *.cer *.crt).
2. Добавление в сервис наблюдения коллекции сертификатов (файл *.p7b).
3. Загрузка набора сертификатов аккредитованных удостоверяющих центров системы квалифицированной электронной подписи Российской Федерации с сайта <http://e-trust.gosuslugi.ru/CA>.
4. Просмотр списков наблюдаемых сертификатов в хранилищах разных категорий сертификатов с основной информацией сертификата и графической индикацией статуса каждого сертификата.
5. Фильтрация вывода сертификатов при просмотре хранилищ:
 - Полно- и частично-текстовый регистронезависимый поиск по полям «Субъект» и «Издатель»;
 - По датам действия сертификатов;
 - По статусам сертификатов (действительный, недействительный, срок действия закрытого ключа истёк).
6. Сортировка по срокам начала, окончания действия сертификата и окончания действия закрытого ключа.
7. Выгрузка (отфильтрованного) списка сертификатов в формате MS Excel (файл *.xlsx) для целей внешней обработки (отчеты, статистика).
8. Выгрузка набора (отфильтрованных) файлов сертификатов в формате архива *.zip для целей внешней обработки.
9. Добавление комментариев для отдельных сертификатов.
10. Просмотр подробной информации о конкретном сертификате в отдельном окне с возможностью выгрузки его как файла, возможностью удаления из наблюдаемых и возможностью его перемещения в хранилище сертификатов, потерявших доверие.
11. Удаление из наблюдения сертификата или группы сертификатов.

1.3.4. Служба обмена информацией по сертификатам с СПО

КАРМА

Сервис, предназначенный для автоматизированного получения информации по статусам сертификатов КЭП и НЭП для СПО КАРМА, установленном на компьютерах организации.

СПО КАРМА может подключаться к данному сервису и получать актуальную информацию по статусам любых сертификатов (например, при запрете выхода в интернет с АРМ организации), а так же передавать информацию о новых сертификатах, используемых для подписания на АРМе с КАРМОЙ, в ЭОС РКІ-сервис, для дальнейшего наблюдения (автоматическое пополнение базы наблюдаемых сертификатов).

2. УСТАНОВКА PKI НА LINUX

2.1. Список поддерживаемых ОС

- Альт Сервер 10

2.2. Подготовка серверов к установке системы

2.2.1. Требования

- Установлена поддерживаемая ОС.
- Имеется доступ к учётной записи root.
- Установлен пакет dotnet-aspnetcore-runtime-6.0.
- Установлен и запущен web-сервер NGINX*.
- Установлено дополнительное ПО.
 - «Карма» 56.2.456 и выше;
 - «КриптоПро CSP» 5.0 R2 (5.0.12000) и выше.
- Наличие SSL-сертификата, подтверждающий домен (Domain-validated certificate).

* - необходимо убедиться, что нет конфликта за порт **80** и **443** с другими WEB-серверами, например Apache.

Ниже описаны процедуры для установки и настройки требуемого дополнительного ПО

2.2.2. Запуск терминала

Все команды следует выполнять в запущенном терминале с root правами, из каталога, в котором находятся запускаемые скрипты.

В случае запуска из другого каталога надо указать полный путь до каждого из скриптов.

2.2.3. Установка и настройка необходимых компонентов

Используя менеджер пакетов текущей ОС необходимо установить:

- Пакет dotnet-aspnetcore-runtime-6.0
- Пакет nginx

nginx после установки следует запустить:

```
systemctl enable --now nginx.service
```

2.2.3.1. Установка дополнительного ПО

Создать каталог **eos** и назначить права:

```
mkdir /home/<user>/eos
chmod 777 /home/<user>/eos
```

2.2.3.1.1. Установка "КриптоПро"

Скачать дистрибутив "КриптоПро" с официального сайта: <https://cryptopro.ru/products/csp/downloads> и поместить полученный архив **linux-amd64.tgz** в ранее созданный каталог **eos**

Перейти в каталог **eos** и распаковать архив **linux-amd64.tgz**:

```
cd /home/<user>/eos
tar -zxvf linux-amd64.tgz
```

Переходим в распакованный каталог **/home/<user>/eos/linux-amd64** в терминале:

```
cd linux-amd64
```

Устанавливаем необходимый для КриптоПро пакет **cryptopro-preinstall**

АЛТ

```
apt-get install cryptopro-preinstall -y
```

Устанавливаем КриптоПро:

```
./install_gui.sh
```

Появляется графическое окно, отмечаем пункты (пробелом) и устанавливаем (см. Рисунок 1):

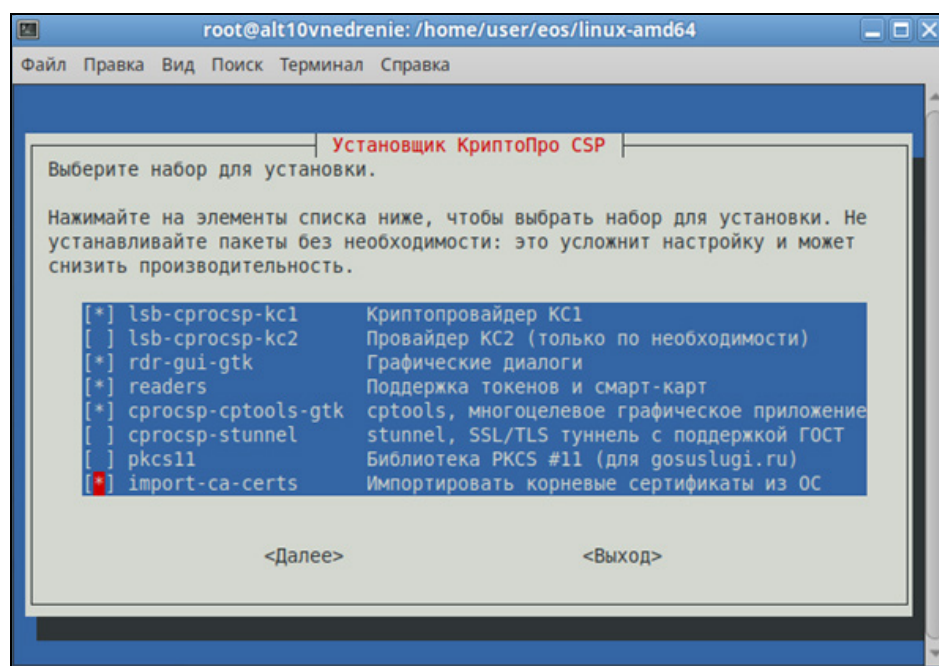


Рисунок 1

Вводим ключ лицензии без пробелов, учитывая регистр:

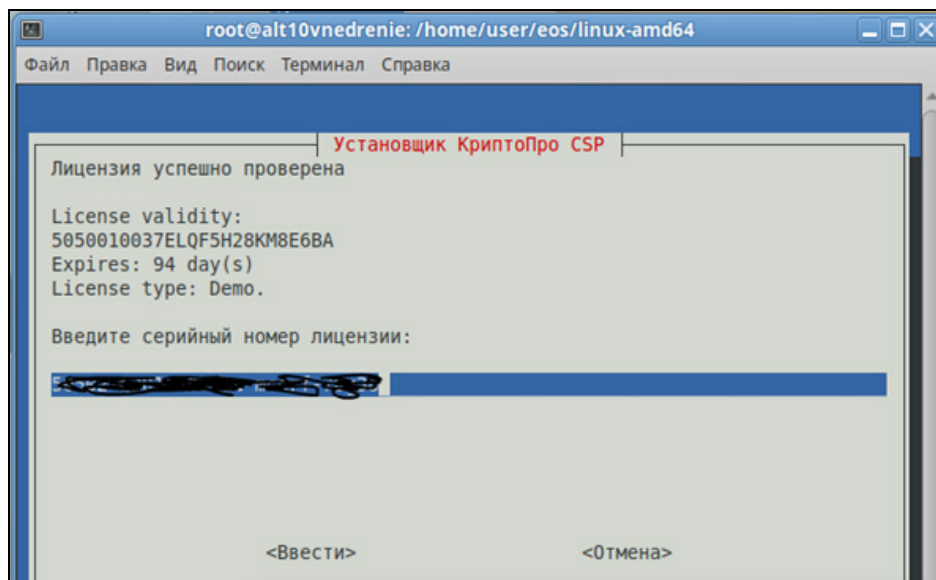


Рисунок 2

2.2.3.1.2. Установка "Кармы"

Файлы Кармы (**carma-common-..**, **carma-capilite-..**) из каталога дистрибутива переносим в каталог **eos**

Для работы "Кармы" потребуется установить пакет **libmicrohttpd**

Установка пакета **libmicrohttpd**:

Альт

```
apt-get install libmicrohttpd -y
```

Переходим в каталог **eos** и устанавливаем пакеты "Кармы"

Альт

```
apt-get install carma-common-<Version>-<OS>.<CPU>.rpm -y
apt-get install carma-capilite-<Version>-<OS>.<CPU>.rpm -y
```

<Version> - версия продукта, например, 56.2.436

<OS> - целевая ОС, например, alt10

<CPU> - разрядность целевого процессора, например, x86_64

2.2.3.1.3. Активация службы "carma.service"

Для автономного запуска и фоновой работы сервиса "Карма" требуется установить службу **carma.service**.

Потребуются файлы:

- **carma.service**;
- **carma.service_install.sh**.

Допустим, они расположены также в каталоге **eos**.

Для установки "Кармы" в режиме сервиса **systemd** необходимо запустить **carma.service_install.sh**, предварительно указав в файле **carma.service** **User** и **Group** в секции **[Service]**.

Переходим в каталог **eos** и запускаем скрипт:

```
./carma.service_install.sh
```

2.3. Установка системы

2.3.1. Подготовка файлов дистрибутива

Скачайте или получите иным путём архив с файлами дистрибутива (**package.zip**).

2.3.1.1. Распаковка файлов системы в целевом каталоге установки

На целевой системе необходимо извлечь файлы из архива дистрибутива по пути **<InstanceDir>**

Каталог **<InstanceDir>** - место расположения как распакованных дистрибутивов версий, откуда запускаются скрипты установки/обновления, так и, после установки, здесь будут расположены служебные папки и папки данных программы (рабочие каталоги).

Планируйте расположение каталога **<InstanceDir>** и свободное место на диске заранее. Далее в инструкции, в параметрах и примерах кода **<InstanceDir>** принимается как **"/opt/pki"**

Директорию необходимо создать заранее.

Перед распаковкой архива, необходимо убедиться, что верно установлена локаль:
locale

Значение параметров должно быть равно ru_RU.utf8. В случае, если напротив параметра LC_ALL пустое значение или параметр LANG не равен ru_RU.utf8, необходимо вписать параметр LC_ALL в файл /root/.i18n.

LC_ALL="ru_RU.utf8"

После внесения изменений необходимо перезапустить сервер.

На целевой системе необходимо извлечь файлы системы из дистрибутива по пути **<InstanceDir>**. Для этого нужно выполнить команду распаковки:

unzip -o -O utf-8 <DistrFileName> -d <InstanceDir>

<DistrFileName> - имя файла дистрибутива, например, package.zip

<InstanceDir> - каталог установки, например, /opt/pki

2.3.1.2. Переход в директорию сборки

Для установки требуемой сборки необходимо перейти в каталог с соответствующей версией:

cd <InstanceDir>/lib/install/<install_ver>/linux

<install_ver> - каталог с актуальной версией

Версионность

Установка архива подразумевает запуск скриптов с директории, содержащей в своём названии версию, например:

./lib/install/install_3.1.0-alpha.3+9a51c3c#20240718.1/

./lib/install/install_3.0.0+be14chd#20240624.3/

Версия имеет такой вид: <мажорная версия>.<минорная версия>.<номер исправления>[-alpha.номер предрелиза]+<хэш последнего коммита>#<дата в формате YYYYMMDD>.<порядковый номер сборки>

Директории, имеющие в своём имени суффикс **alpha** содержат сборки из **dev** веток.

2.3.2. Размещение контейнера .prfx на сервере

Для корректного конфигурирования сервисов понадобится ssl сертификат, заключённый в prfx контейнер - его следует поместить на целевой сервер, например, в каталог `<InstanceDir>`.

2.3.3. Установка службы сервера приложений

На целевой системе необходимо запустить конфигурационный скрипт **configure_pkisrv_linux.sh**, для регистрации службы сервера приложений в systemd.

Скрипт выполняет следующие действия:

- Создаёт все необходимые каталоги
- Создаёт пользователя и группу `<AppName>-pkisrv`
- Настраивает права на каталоги и файлы
- Создаёт и запускает сервис systemd с именем `<AppName>-pkisrv-a.service`

Для конфигурационных файлов будут установлены следующие права (пути указаны относительно каталога `<InstanceDir>`):

1. Каталог `config/<AppName>-pkisrv/a/Settings` будет установлена новая группа, а также установлены полные права владельцу, право на чтение и выполнение на группу для директорий, и только чтение файлов на группу
2. Файлам `config/<AppName>-pkisrv/a/Settings/*.json` будет установлена новая группа, а также установлены полные права владельцу и только чтение на группу
3. Каталог `var` будет установлена новая группа и новый владелец. Будут установлены полные права владельцу, право на чтение и выполнение на группу для директорий, и только чтение файлов на группу

2.3.3.1. Проверка портов сервера приложений

Скрипт перед конфигурированием службы, выполняет проверку на занятость портов, заданных в параметрах **PortA** и **PortB**, однако данная проверка не может считаться абсолютной, т.к. конфликт портов может возникнуть и после завершения процесса конфигурирования. Например, на сервер будет установлено дополнительное ПО, использующее те же самые порты. Поэтому окончательная ответственность за предотвращение конфликтов использования портов лежит на администраторе системы. Для проверки занятых портов скрипт использует утилиту **ss**, если она не установлена - проверка портов будет пропущена.

2.3.3.1.1. Конфликт портов при работе "Кармы"

Возможны ситуации, когда дефолтный порт "Кармы" - 8080 будет занят другим ПО в системе. Проверить это можно путём открытия страницы <http://localhost:8080> в браузере. Если "Карма" работает на данном порту, то на странице будет отображена информация об окружении:

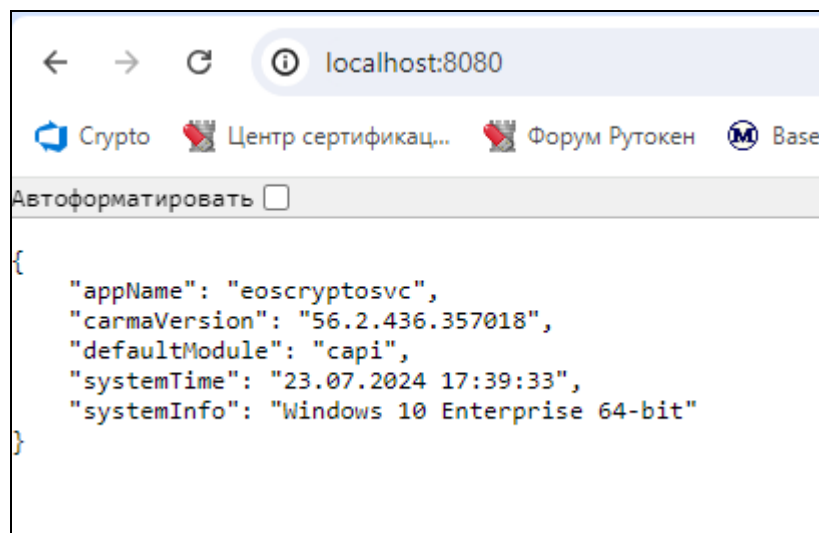


Рисунок 3

Если на страницу нет доступа или вывод отличается от представленного выше - "Карма" не активна, порт занят другим ПО.

В таком случае потребуется изменить порт, отредактировав один из файлов конфигурации "Кармы" вручную:

- "Карма" установлена как служба - редактируем `/etc/CARMA/EosCryptoSvcConfig.ini`
- В ином случае - редактируем `/home/<User>/.config/CARMA/EosCryptoSvcConfig.ini`, где `<User>` - имя текущего пользователя

Нужно сверить и при необходимости установить следующие настройки:

- `EnableHttp=1`
- `EnableDedicatedHttpPort=1`
- `HttpPort=<FreePort>`, где `<FreePort>` - свободный порт, например 3000:



```
###EosCryptoSvc automatically generated config file###

[Service settings]
LogMode=2
LogFile=
ShowTrayIcon=0
IgnoreUnknownRevocationStatus=0
ForceCRLDownload=0
UseOnlyCustomCDPs=0
AllowServicePrivateKeyAccess=1
RemotePrivateKeyAccess=0
EnableHttp=1
EnableDedicatedHttpPort=1
HttpPort=3000
EnableAuth=0
AuthUsername=
AuthPassword=
CheckOCSP=0
OCSPFileName=
ProxyLogin=
ProxyPassword=
ProxyAddress=
ProxyPort=80
ProxyType=0
OCSPTimeout=30000
TSPTIMEout=30000
GeneralTimeout=30000
CRLTimeout=30000
UnloadPFXAfterUsage=1
DefaultModule=capi
Language=Ru

[Custom CDP list]

[Custom error handlers]
```

Рисунок 4

После изменения настроек следует перезапустить (или запустить) "Карму":

- Если установлена как служба - вводим команду **systemctl restart carma.service**
- Если установлена как приложение - перезапускаем приложение.

2.3.3.2. Описание параметров скрипта configure_pkisrv_linux.sh

Таблица 1

Параметр	Название	Примеры допустимых значений	Обязательный	Описание
InstanceDir	Каталог установки	/opt/pki	Да	Каталог установки файлов приложения. Данное имя каталога используется для определения ресурсов, используемых при установке, и для определения пути каталогов хранения конфигурации (config) и рабочих файлов (var) службы сервера приложений.
AppName	Имя приложения	pki	Да	Имя приложения используется для формирования имени пользователя и группы, имени сервиса systemd. Имя должно быть не более двадцати символов, содержать лишь буквы в нижнем регистре, исключать символы, кроме подчёркивания и дефиса, а также не должно начинаться с цифры или пробела.

Параметр	Название	Примеры допустимых значений	Обязательный	Описание
PortA PortB	Порты привязки приложения	10071 10072	Да	<p>Порты протокола TCP/IP, которые будут использованы сервером приложений для получения HTTP (REST) запросов.</p> <p>Нужно указать пару портов. Второй порт пока не используется. Планируется его использование в сценариях обновления системы без остановки обслуживания пользователей по схеме А-В:</p> <ul style="list-style-type: none"> • запуск второго экземпляра сервера приложений • переключение настройки реверс-прокси на фронт-энд сервере на порты этого экземпляра • остановка текущего экземпляра сервера приложений

Параметр	Название	Примеры допустимых значений	Обязательный	Описание
LogsFormat	Формат файлов логов	txt ecs	Нет	<p>Формат, в котором сервер приложений будет писать данные в файлы логов.</p> <p>txt - форматированный текстовый формат, предназначенных для непосредственного чтения человеком.</p> <p>ecs - Elastic Common Schema. Структурированный json формат, предназначенный для последующей загрузки на сервер мониторинга. Этот формат является "родным" для стека сбора, хранения и анализа логов Elastic-Logstash-Kibana. И, возможно, поддерживается и другими вендорами аналогичных систем.</p>

2.3.3.3. Пример вызова скрипта `configure_pkisrv_linux.sh`.

```
bash ./configure_pkisrv_linux.sh --InstanceDir /opt/pki --AppName pki --PortA 10071 --PortB 10072 --LogsFormat txt
```

2.3.3.4. Проверка установки службы сервера приложений

В случае успешного завершения установки, работоспособность службы сервера приложений можно проверить набрав в браузере адрес приложения, находясь на этом же сервере: **http://localhost:<PortA>**. Должен открыться диагностический экран с перечнем модулей сервера приложений.

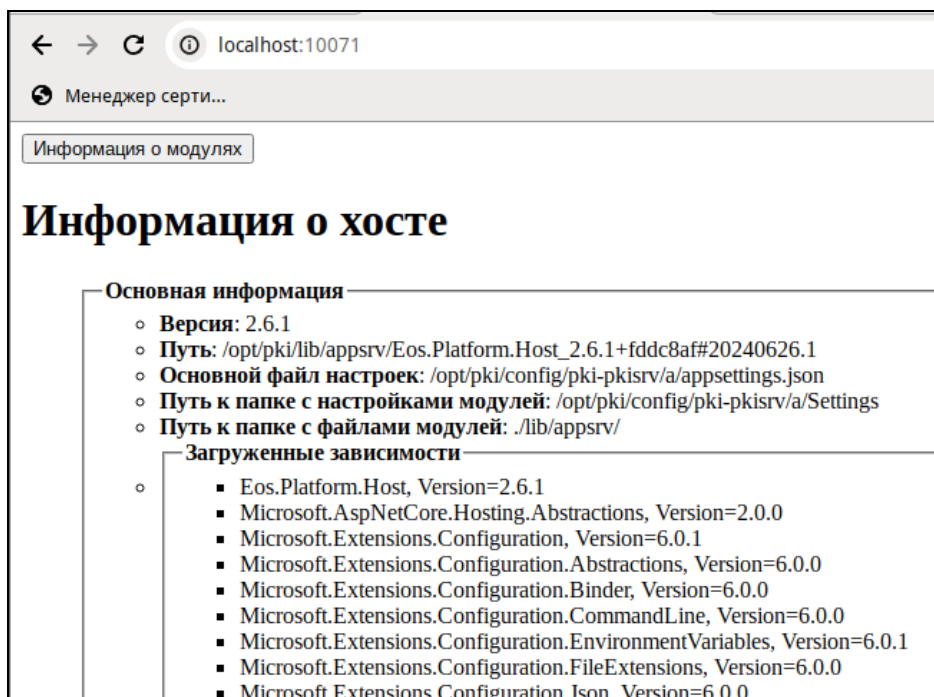


Рисунок 5

2.3.4. Установка фронт-энд web-сервера

Для установки и настройки фронт-энд веб-сайта NGINX используется скрипт **configure_pkiweb_linux.sh**.

Скрипт выполняет следующие действия:

- добавляет и настраивает веб-сайт NGINX
- настраивает привязку сайта к порту TCP/IP в соответствии с параметрами **WebServerName**, **WebServerPort**, привязка конфигурируется на использование протокола HTTPS.
- настраивает правила реверс-прокси для передачи запросов из web-приложения на сервер приложения

2.3.4.1. Проверка порта frontend сервера

Скрипт перед конфигурированием службы, выполняет проверку на занятость порта, заданного в параметре **WebServerPort**, однако данная проверка не может считаться абсолютной, т.к. конфликт портов может возникнуть и после завершения процесса конфигурирования. Например, на сервер будет установлено дополнительное ПО, использующее те же самые порты. Поэтому окончательная ответственность за предотвращение конфликтов использования портов лежит на администраторе системы. Для проверки занятых портов скрипт использует утилиту ss, если она не установлена - проверка портов будет пропущена.

2.3.4.2. Описание параметров скрипта `configure_pkiweb_linux.sh`

Таблица 2

Параметр	Название	Примеры допустимых значений	Обязательный	Описание
InstanceDir	Каталог установки	/opt/pki	Да	Каталог установки файлов приложения. Данное имя каталога используется для определения ресурсов, используемых при установке, и для определения пути каталогов хранения конфигурации (config).
AppName	Имя приложения	pki	Да	Имя приложения - должно быть не более двадцати символов, содержать лишь буквы в нижнем регистре, исключать символы, кроме подчёркивания и дефиса, а также не должно начинаться с цифры или пробела.
WebServerName	Публичное имя сайта	pki.myorg.ru	Нет	Публичное имя сайта (на целевом сервере команда hostname).
WebServerPort	Порт привязки сайта	1443	Нет	Номер порта TCP/IP для привязки сайта к нестандартному порту.

Параметр	Название	Примеры допустимых значений	Обязательный	Описание
AppSrvUrl	Адрес сервера приложений	http://localhost:10071	Да	Адрес сервера приложения. Должен быть указан полный URL включающий протокол, адрес и порт привязки сервера приложений.
PfxPath	Путь к pfx контейнеру	/root/tmp/pkisrv.pfx	Да	Путь к файлу .pfx содержащему публичный и приватный ключи сертификата для TLS протокола. Поскольку файл pfx содержит закрытый ключ, необходимо внимательно следить, чтобы данный файл не попал в общий доступ.
PfxPassphrase	Пароль к контейнеру .pfx	'Passphrase'	Нет (см. описание)	Если пароль не передан, скрипт запросит его в процессе выполнения. Если pfx файл не защищен паролем, нужно ввести пустую строку при выдаче приглашения скрипта.

2.3.4.3. Примеры вызова скрипта `configure_pkiweb_linux.sh`

```
bash ./configure_pkiweb_linux.sh --InstanceDir /opt/pki --AppName pki --
WebServerName pki.myorg.ru --AppSrvUrl "http://localhost:10071" --PfxPath
/root/tmp/pkisrv.pfx --PfxPassphrase 'Passphrase'
```

2.3.4.4. Добавление имени сайта в `hosts`

Для успешного резолва имени требуется внести его в файл `/etc/hosts`. Т.е. необходимо добавить строку в конец файла:

```
127.0.0.1 <WebServerName>
```

Например:

```
127.0.0.1 pki.myorg.ru
```

2.3.4.5. Проверка установки системы

Проверка осуществляется открытием в Интернет браузере (например, Firefox) страницы по адресу `https://<WebServerName>/app/pki`. Должна появиться главная страница PKI:

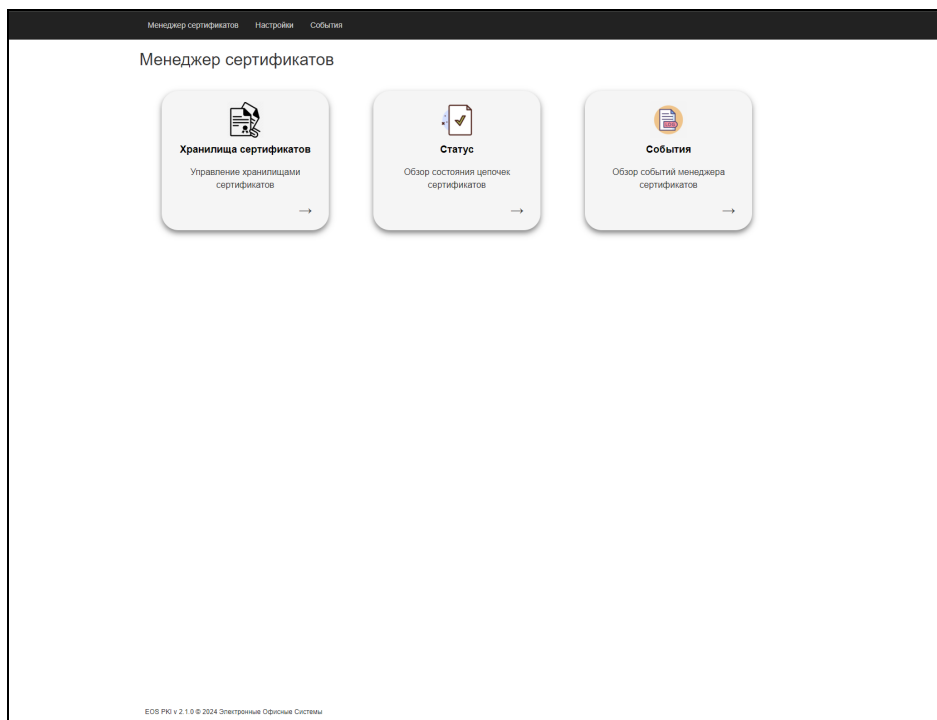


Рисунок 6

2.3.5. Перед началом работы

Для корректной и полноценной работы приложения следует выполнить следующие шаги по настройке:

1. Сверить [порт, на котором работает "Карма"](#) с портом, указанным в настройках PKI и при необходимости актуализировать его

Настройки

"Белый" список интернет-адресов для скачивания списков отзыва

Общие настройки Создать подкаталоги Проверить конфигурацию

Имя PKI сервиса:	EOS PKI
Список разрешенных хостов:	127.0.0.1;192.168.0.0/24::1
Зона импорта:	/opt/pki/var/pki-pkisrv/import
Сервис отправки e-mail уведомлений:	/opt/pki/var/pki-pkisrv/mailler
Каталог хранилищ:	/opt/pki/var/pki-pkisrv/stores
Сервис обновления статуса сертификатов:	/opt/pki/var/pki-pkisrv/stat
КАРМА:	http://127.0.0.1:8080
Загружать СОС из каталога импорта:	☐

Рисунок 7

2. Импортировать промежуточные и корневые сертификаты (раздел "Автоматический импорт сертификатов Аккредитованных УЦ РФ (КЭП)" в руководстве пользователя PKI-сервиса)
3. Обновить статусы сертификатов (раздел "Панель «Обновление статусов сертификатов»" в руководстве пользователя PKI-сервиса)

2.4. Перенос данных с прежних версий PKI (< v3.0.0)

Перенос включает в себя следующие шаги:

1. Остановка сервиса прежней версии PKI (< v3.0.0)
2. Остановка сервиса текущей версии PKI (>= v3.0.0)
3. Перенос хранилищ сертификатов
4. Перенос файла конфигурации
5. Редактирование файла конфигурации для обеспечения совместимости
6. Выдача необходимых прав перенесённым каталогам и файлам
7. Возобновление работы службы текущей версии PKI (>= v3.0.0)
8. Сохранение настроек для добавления недостающих параметров

2.4.1. Остановка сервиса прежней версии

```
systemctl stop Eos.CertMan.service
```

2.4.2. Остановка сервиса текущей версии

```
systemctl stop <AppName>-pkisrv-a.service
```

2.4.3. Перенос хранилищ сертификатов

Требуется перенести каталог хранилищ **stores**, путь до которого указан в настройках прежней версии PKI

Настройки

"Белый" список интернет-адресов для скачивания списков отзыва

Общие настройки Создать подкаталоги Проверить конфигурацию

Имя PKI сервиса:	EOS CertMan
Список разрешенных хостов:	127.0.0.1;192.168.0.0/24::1
Зона импорта:	/var/lib/Eos.CertMan/import_cer
Сервис отправки e-mail уведомлений:	/var/lib/Eos.CertMan/mailler
Каталог хранилищ:	/var/lib/Eos.CertMan/stores
Сервис обновления статуса сертификатов:	/var/lib/Eos.CertMan/stat
КАРМА:	http://127.0.0.1:3000
Загружать СОС из каталога импорта:	☐

Рисунок 8

в каталог `<InstanceDir>/var/pki-pkisrv` с подтверждением замены файлов.

2.4.4. Перенос файла конфигурации

Требуется перенести прежний файл конфигурации `/var/www/Eos.CertMan/appsettings.json` в каталог `<InstanceDir>/var/pki-pkisrv`

Далее следует переименовать файл: `<InstanceDir>/var/pki-pkisrv/appsettings.json` → `<InstanceDir>/var/pki-pkisrv/pkiConfig.json`, удалив перед этим уже существующий `<InstanceDir>/var/pki-pkisrv/pkiConfig.json` файл.

2.4.5. Редактирование файла конфигурации для обеспечения совместимости

Для успешного использования прежнего конфигурационного файла необходимо вручную изменить несколько параметров:

Возможно, что в вашем файле конфигурации не будет каких-то параметров, рассмотренных ниже - ничего страшного, значит этот параметр пропускаем и идём дальше

1. Имя блока `"ApplicationInfo"` изменить на `"AppInfo"`

Было:

```
"ApplicationInfo": {
  "Name": "Eos.CertMan"
},
```

Стало:

```
"AppInfo": {
  "Name": "Eos.CertMan"
},
```

2. Заменить адреса рабочих каталогов сервиса с предыдущей версии на устанавливаемую, в формате `<InstanceDir>/var/pki-pkisrv/...`

Пример с учётом того, что `<InstanceDir> = "/opt/pki"`:

Было:

```
"import": "/var/lib/Eos.CertMan/import_cer",
"stores": "/var/lib/Eos.CertMan/stores",
"stat": "/var/lib/Eos.CertMan/stat",
"mailer": "/var/lib/Eos.CertMan/mailer",
```

Стало:

```
"import": "/opt/pki/var/pki-pkisrv/import",
"stores": "/opt/pki/var/pki-pkisrv/stores",
"stat": "/opt/pki/var/pki-pkisrv/stat",
"mailer": "/opt/pki/var/pki-pkisrv/mailer",
```

3. В блоке **mailNotification** параметр **port**: необходимо удалить кавычки - значение должно быть числом, а не строкой:
 "port": "587" -> "port": 587

Было:

```
"mailNotification": {
  "enabled": false,
  "smtp": "smtp.mail.ru",
  "port": "587",
```

Стало:

```
"mailNotification": {
  "enabled": false,
  "smtp": "smtp.mail.ru",
  "port": 587,
```

4. В блоке **proxy** параметр **port**: необходимо удалить кавычки - значение должно быть числом, а не строкой:
 "port": "3128" -> "port": 3128

Было:

```
"proxy": {
  "enabled": false,
  "anonymous": false,
  "host": "194.87.111.108",
  "port": "3128",
```

Стало:

```
"proxy": {
  "enabled": false,
  "anonymous": false,
  "host": "194.87.111.108",
  "port": 3128,
```

5. В блоке **signatureImport** параметр **errCountForCancel**: необходимо удалить кавычки - значение должно быть числом, а не строкой:
 "errCountForCancel": "10" -> "errCountForCancel": 10

Было:

```
"signatureImport": {
  "path": "D:\\FiSt\\DeloWebSignatures\\EOS_EXPORT_SIGN",
  "errCountForCancel": "10",
  "needCleaning": false
```

Стало:

```

"signatureImport": {
  "path": "D:\\FiSt\\DeloWebSignatures\\EOS_EXPORT_SIGN",
  "errCountForCancel": 10,
  "..."
}

```

6. В блоке `updateCerts` параметр `autoCleanStartTime`: необходимо удалить кавычки - значение должно быть числом, а не строкой:
`"autoCleanStartTime": "60" -> "autoCleanStartTime": 60`

Было:

```

"updateCerts": {
  "enabled": false,
  "autoClean": true,
  "autoCleanStartTime": "60"
}

```

Стало:

```

"updateCerts": {
  "enabled": false,
  "autoClean": true,
  "autoCleanStartTime": 60
}

```

7. В блоке `importETrust` параметр `nextLaunchDelayInHours`: необходимо удалить кавычки - значение должно быть числом, а не строкой:
`"nextLaunchDelayInHours": "24" -> "nextLaunchDelayInHours": 24`

Было:

```

"importETrust": {
  "enabled": false,
  "nextLaunchDelayInHours": "24"
}

```

Стало:

```

"importETrust": {
  "enabled": false,
  "nextLaunchDelayInHours": 24
}

```

Примечание

После первого запуска приложения настройки времени для службы проверки целостности хранилищ сбросятся. На веб странице настроек необходимо задать время запуска и остановки заново.

Проверка целостности хранилищ		
Проверка целостности:	☒	
Время запуска:	00:00	⌚
Время остановки:	00:00	⌚

Рисунок 9

2.4.6. Выдача необходимых прав перенесённым каталогам и файлам

Для выдачи прав вновь добавленным файлам и каталогам следует выполнить [остановку сервиса](#) и запустить скрипт установки [службы сервера приложений](#) из [каталога текущей версии](#) или выполнить [полноценное обновление](#) при наличии новых версий.

Параметры для скрипта должны быть идентичны параметрам, указанным при установке!

2.4.7. Возобновление работы сервиса текущей версии РКИ

```
systemctl start <AppName>-pkisrv-a.service
```

2.4.8. Сохранение настроек для добавления недостающих параметров

Вполне возможны ситуации, когда в переносимом файле конфигурации не будет хватать каких-то параметров, используемых в приложении. Для исключения ошибок при обращении к ним сервисом требуется сохранить текущую конфигурацию на странице настроек.

Переходим на страницу настроек (раздел "Страница «Настройки»" в руководстве пользователя РКИ-сервиса), пролистываем страницу вниз и нажимаем на кнопку "Сохранить изменения конфигурации". После этого файл конфигурации будет перезаписан и дополнен всеми необходимыми параметрами.

2.5. Обновление системы

Перед обновлением системы необходимо выполнить [остановку сервиса](#).

Далее на целевой системе, при помощи стандартного архиватора, необходимо, с заменой файлов, извлечь файлы системы из обновленного дистрибутива по пути `<InstanceDir>`. Запустить соответствующий скрипт из каталога с требуемой, для установки, версией.

Вызовы скриптов при обновлении идентичны вызовам при установке. Сервис после обновления запустится скриптом самостоятельно.

Параметры для скриптов обновления должны быть идентичны параметрам, указанным при установке!

2.6. Удаление системы

Для удаления требуемой сборки необходимо перейти в каталог с соответствующей версией:

```
cd <InstanceDir>/lib/install/<install_ver>/linux
```

Далее необходимо запустить скрипт `uninstall.sh`:

```
./uninstall.sh --InstanceDir <InstanceDirVal> --AppName <AppNameVal>
```

`<InstanceDirVal>` - обязательный. Каталог установки файлов приложения, например, `/opt/pki`

`<AppNameVal>` - обязательный. Наименование приложения, например, `pki`

Внимание! Перед удалением, скрипт не запрашивает дополнительных разрешений. Рекомендуем запускать этот же скрипт, добавив параметр `--DryRun`, который позволит оценить весь перечень удаляемых компонентов заблаговременно.

Пример вызова скрипта с параметром `--DryRun`, для проверки списка удаляемых компонентов:

```
.\uninstall.sh --InstanceDir <InstanceDirVal> --AppName <AppNameVal> --DryRun
```

2.7. Очистка неиспользуемых дистрибутивов предыдущих версий

Для удаления неиспользуемых дистрибутивов необходимо перейти в каталог, с которого был установлен актуальный экземпляр.

```
cd <InstanceDir>/lib/install/<install_ver>/linux
```

Далее необходимо запустить скрипт `uninstall.sh` с параметром `--CleanUp`:

```
.\uninstall.sh --InstanceDir <InstanceDirVal> --AppName <AppNameVal> --CleanUp
```

`<InstanceDirVal>` - обязательный. Каталог установки файлов приложения, например, `/opt/pki`

`<AppNameVal>` - обязательный. Наименование приложения, например, `pki`

1. Алгоритм работы скрипта, запущенного с параметром `CleanUp`. Выбираются все компоненты существующих сборок, кроме той, с которой запущен данный скрипт. Выборка осуществляется путём чтения файлов, содержащих описание компонентов.
2. Отдельно определяются компоненты активной сборки. Данный список составляется исходя из версий которые, содержат в себе файлы `appsettings.json` и/или `index.html`.
3. Из списка компонентов, не относящихся к комплекту дистрибутива из которого был запущен скрипт, делается исключение компонентов активной сборки.
4. Происходит удаление компонентов по сформированному, после всех исключений, списку.

Результатом работы скрипта запущенного с параметром `--CleanUp` будет вывод всех удалённых компонентов.

Внимание! Перед удалением, скрипт не запрашивает дополнительных разрешений. Рекомендуем запускать этот же скрипт, добавив параметр `--DryRun`, который позволит оценить весь перечень удаляемых компонентов заблаговременно.

Пример вызова скрипта с параметром `--DryRun`, для проверки списка удаляемых компонентов:

```
.\uninstall.sh --InstanceDir <InstanceDirVal> --AppName <AppNameVal> --CleanUp --DryRun
```

3. УСТАНОВКА PKI НА WINDOWS

3.1. Список поддерживаемых ОС

- Рабочие станции
 - Windows 10
- Серверные ОС
 - Windows Server 2019

3.2. Подготовка серверов к установке системы

3.2.1. Требования

- Установлена поддерживаемая ОС с последними обновлениями
- Сервер состоит в домене
- Добавлена роль «Веб-сервер IIS» (Web Server IIS) / активированы службы IIS (для десктопной версии ОС)
- Установлены компоненты
 - пакет ASP.NET Core 6.0 Runtime (v6.0.11) - Windows Hosting Bundle
 - Microsoft Application Request Routing 3.0
 - URL Rewrite Module 2.1
- Установлено дополнительное ПО
 - «Карма» 56.2.436 и выше
 - «КриптоПро CSP» 5.0 (5.0.11455) и выше
 - Пакеты Microsoft Visual C++ Redistributable x86 и x64
- Наличие SSL-сертификата, подтверждающий домен (Domain-validated certificate)

Ниже подробно описан процесс установки и настройки всех необходимых компонентов и дополнительного ПО

3.2.2. Запуск powershell

Все команды следует выполнять в запущенном PowerShell от имени администратора, из каталога, в котором находятся запускаемые скрипты.

В случае запуска из другого каталога надо указать полный путь до каждого из скриптов.

3.2.3. Настройка IIS

3.2.3.1. Десктопная ОС

На целевой системе требуется включить "Службы IIS". Кроме обязательной основной функциональности IIS дополнительно следует установить "Инициализацию приложений" из компонентов разработки приложений:

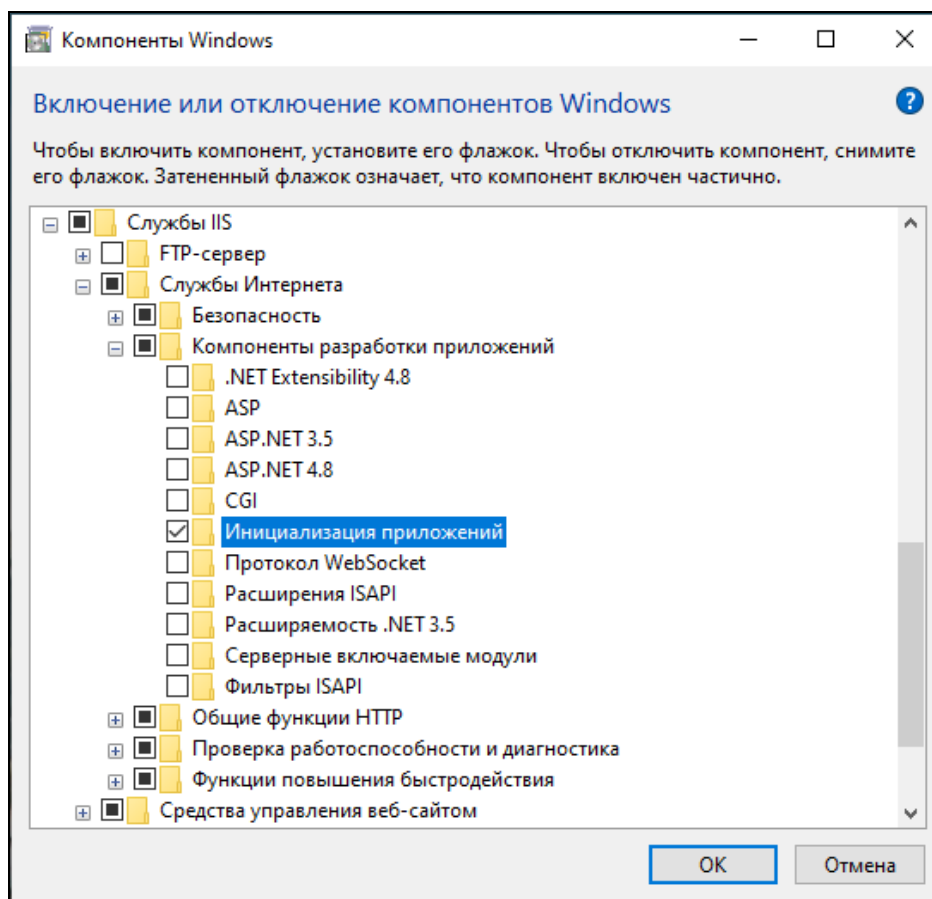


Рисунок 10

3.2.3.2. Серверная ОС

На целевом сервере необходимо установить роль веб-сервера IIS. Кроме обязательной основной функциональности IIS дополнительно следует установить "Инициализацию приложений" из компонентов разработки приложений.

Для этого следует выполнить командлет PowerShell:

Основные компоненты

Install-WindowsFeature Web-Server

Install-WindowsFeature Web-AppInit

Также это можно сделать используя "Мастер добавления ролей и компонентов", попасть в который можно через Диспетчер серверов (Пуск > Диспетчер серверов, затем Управление > Добавить роли и компоненты).

Нажмите здесь для раскрытия...

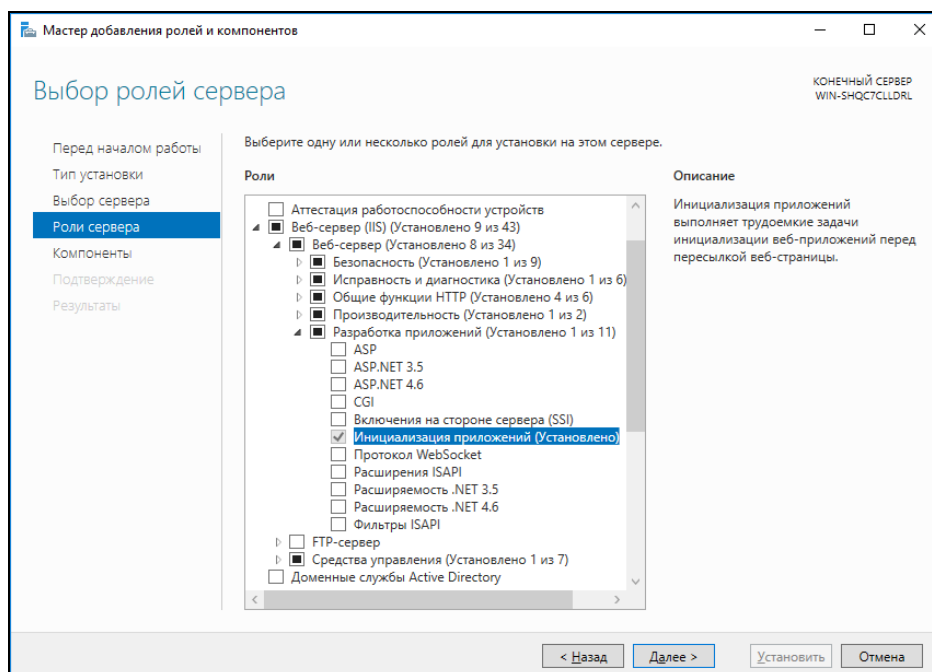


Рисунок 11

3.2.4. Установка и настройка необходимых компонентов

Необходимо установить:

- ASP.NET Core 6.0 Runtime (v6.0.11) - Windows Hosting Bundle
 - <https://dotnet.microsoft.com/ru-ru/download/dotnet/thank-you/runtime-aspnetcore-6.0.11-windows-hosting-bundle-installer>
- Microsoft Application Request Routing 3.0
 - [x86 installer](#) / [x64 installer](#)
- URL Rewrite Module 2.1
 - [x86 installer](#) / [x64 installer](#)

Установку можно производить вручную, запуская соответствующие инсталляторы, либо иницируя установку с терминала PowerShell.

```
# RewriteModule
($msi = Start-Process "msiexec" -ArgumentList "/i
<ComponentsDir>\<RewriteInstallFile> /quiet /norestart" -Wait -
Passthru).ExitCode

# ApplicationRequestRouting
($msi = Start-Process "msiexec" -ArgumentList "/i
<ComponentsDir>\<ARRInstallFile> /quiet /norestart" -Wait -Passthru).ExitCode

# Dotnet Hosting Bundle (AspNetCoreModuleV2 + .NET Runtime)
($msi = Start-Process <ComponentsDir>\dotnet-hosting-6.0.11-win.exe -
ArgumentList "/quiet /norestart" -Wait -PassThru).ExitCode

# Проверка
Reset-IISServerManager -Confirm:$false
Get-IIISConfigSection -SectionPath "system.webServer/modules" | Get-
IIISConfigCollection | Get-IIISConfigCollectionElement | %{
$_.Attributes["name"].Value }
# RewriteModule
# ApplicationRequestRouting
# AspNetCoreModuleV2
```

<ComponentsDir> - путь до каталога с необходимыми компонентами

<RewriteInstallFile> - имя файла установки URL Rewrite Module 2.1, например, **rewrite_amd64_en-US.msi**

<ARRInstallFile> - имя файла установки Microsoft Application Request Routing 3.0, например, **requestRouter_amd64.msi**

После установки указанных компонентов, необходимо настроить работу модуля **Application Request Routing** в режиме реверс прокси сервера.

3.2.4.1. Включение реверс прокси

Включить прокси можно используя PowerShell:

Включение прокси

```
Get-IISConfigSection -SectionPath "system.webServer/proxy" | Set-IISConfigAttributeValue -AttributeName Enabled -AttributeValue True
```

Проверка текущего значения настройки прокси

```
Get-IISConfigSection -SectionPath "system.webServer/proxy" | Get-IISConfigAttributeValue -AttributeName Enabled
```

Или в графическом интерфейсе IIS:

1. Запускаем модуль "Application Request Routing"

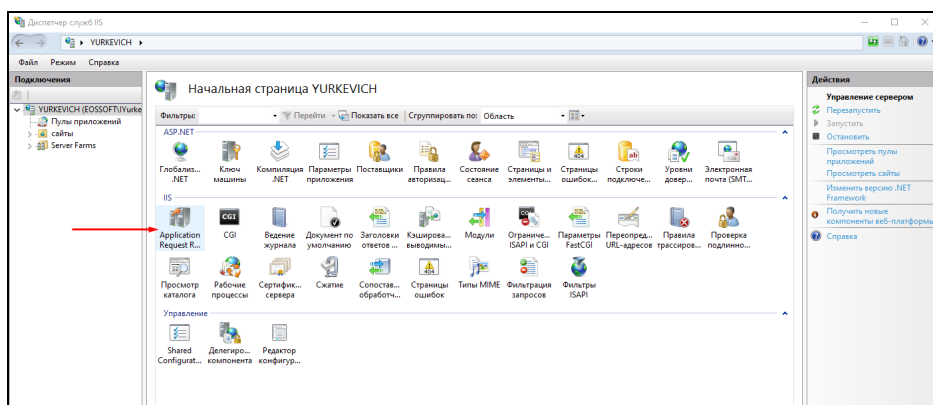


Рисунок 12

2. Переходим в настройки

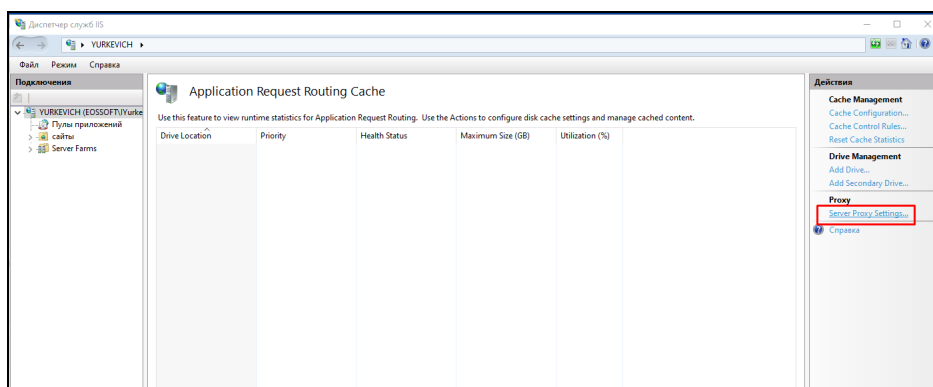


Рисунок 13

3. Ставим галочку в чекбоксе напротив опции "Enable proxy" и применяем настройки

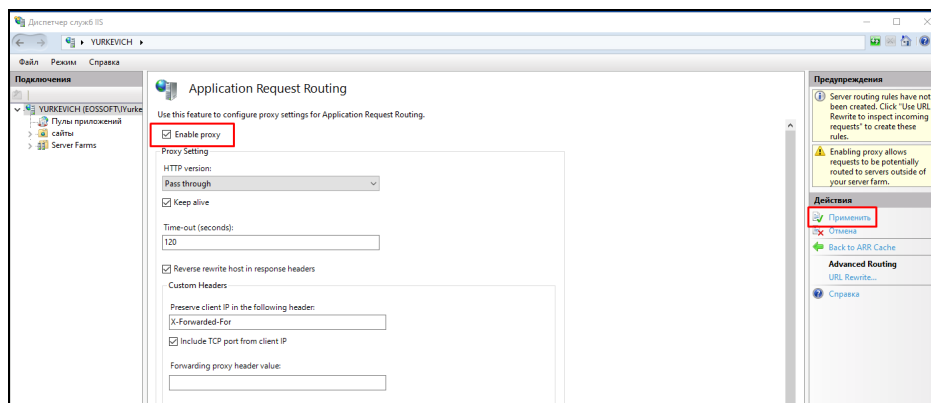


Рисунок 14

3.2.4.2. Установка дополнительного ПО

Также для работы PKI требуется установка дополнительного ПО:

- «Карма» 56.2.436 и выше
- Установочные файлы поставляются с дистрибутивом (каталог Carma). Для установки запускаем **setup.exe**
- «КриптоПро CSP» версии 5.0 (5.0.11455) и выше
- <https://cryptopro.ru/products/csp/downloads>
- Пакеты Microsoft Visual C++ Redistributable x86 и x64:
- https://aka.ms/vs/17/release/vc_redist.x86.exe
- https://aka.ms/vs/17/release/vc_redist.x64.exe

"Карма" устанавливается строго без расширений сервиса, режим запуска - Служба Windows. Остальные настройки можно оставить по дефолту:

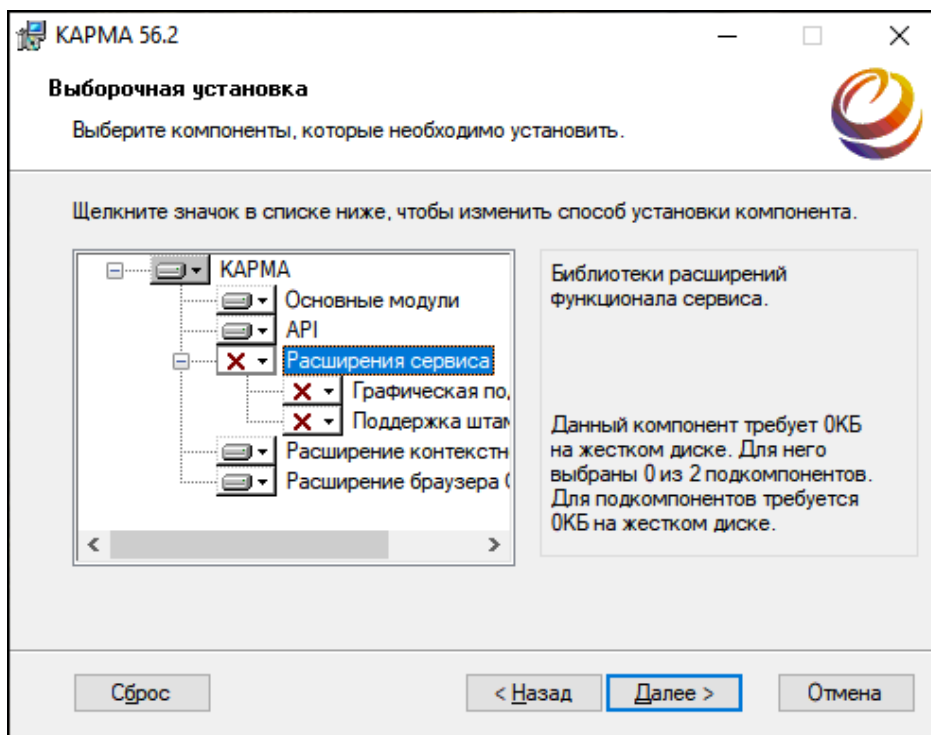


Рисунок 15

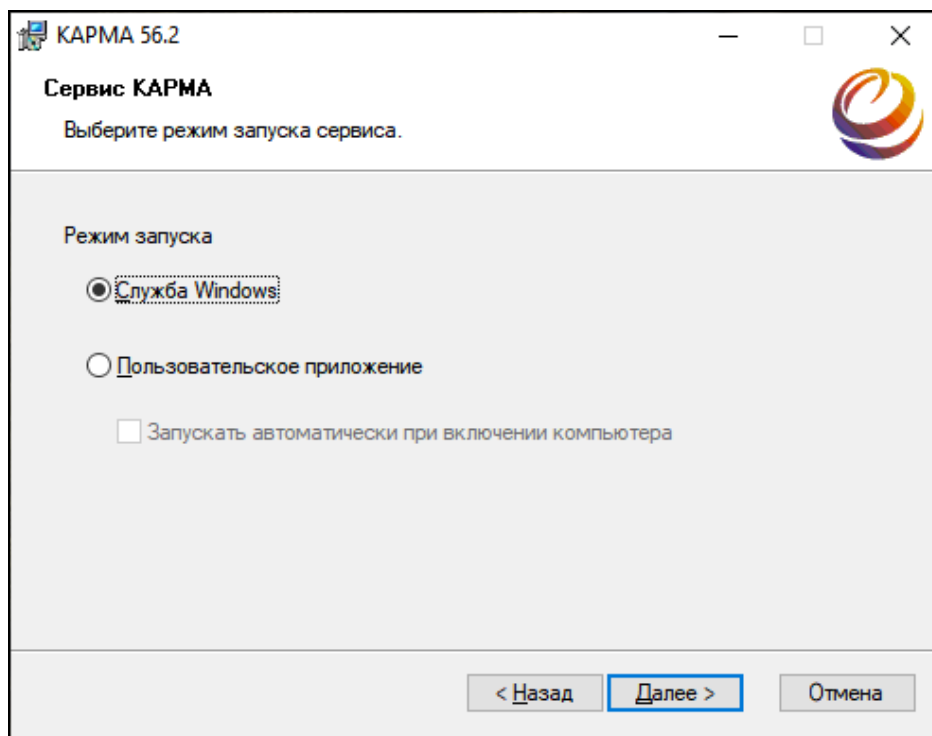


Рисунок 16

3.3. Установка системы

3.3.1. Подготовка файлов дистрибутива

Скачайте или получите иным путём архив с файлами дистрибутива (**package.zip**).

3.3.1.1. Распаковка файлов системы в целевом каталоге установки

На целевой системе, при помощи стандартного архиватора, необходимо извлечь файлы из архива дистрибутива по пути `<InstanceDir>`

Каталог `<InstanceDir>` - место расположения как распакованных дистрибутивов версий, откуда запускаются скрипты установки/обновления, так и, после установки, здесь будут расположены служебные папки и папки данных программы (рабочие каталоги).

Планируйте расположение каталога `<InstanceDir>` и свободное место на диске заранее. Далее в инструкции, в параметрах и примерах кода `<InstanceDir>` принимается как `"C:\Eos\pki"`

Директорию необходимо создать заранее, либо она будет создана автоматически при указании её в интерфейсе архиватора.

3.3.1.2. Переход в директорию установки

Для установки требуемой версии необходимо сначала перейти в каталог с соответствующей версией используя PowerShell:

```
cd <InstanceDir>\lib\install\<install_ver>\windows
```

`<install_ver>` - каталог с актуальной версией

Версионность

Установка архива подразумевает запуск скриптов с директории, содержащей в своём названии версию, например:

```
.lib\install\install_3.1.0-alpha.3+9a51c3c#20240718.1\  
.lib\install\install_3.0.0+be14chd#20240624.3\
```

Версия имеет такой вид: <мажорная версия>.<минорная версия>.<номер исправления>[-alpha.номер предрелиза]+<хэш последнего коммита>#<дата в формате YYYYMMDD>.<порядковый номер сборки>

Директории, имеющие в своём имени суффикс **alpha** содержат сборки из **dev** веток.

3.3.2. Размещение контейнера .pfx на сервере

Для корректного конфигурирования сервисов понадобится ssl сертификат. Это может быть уже установленный сертификат, либо сертификат заключённый в pfx контейнер. Если предполагается использование уже установленного сертификата, то необходимо проверить, что данный сертификат установлен в сертификаты локального компьютера (LocalMachine) по пути "Размещение веб-служб" (WebHosting). Если предполагается использование .pfx контейнера, то его следует поместить на целевой сервер, например, в каталог <InstanceDir>.

3.3.3. Установка службы сервера приложений

Для установки службы сервера приложений используется скрипт **configure_pkisrv_windows.ps1**.

Скрипт выполняет следующие действия:

- выполняет проверку необходимых установленных компонентов и конфигураций:
- Установлена роль **Web-сервер**, включая функцию **Инициализация приложений (Web-AppInit)**
- Установлен модуль **ASP.NET Core (ASP.NET Core Module)** для версии 6.0.2 или выше (входит в **Пакет размещения .NET Core (.NET Core Hosting Bundle)**)
- Установлена среда выполнения **ASP.NET Core (ASP.NET Core Runtime)** версии 6.0.2 или выше (входит в **Пакет размещения .NET Core (.NET Core Hosting Bundle)**)
- Установлен среда выполнения **.NET (.NET Runtime)** версии 6.0.2 или выше (входит в **Пакет размещения .NET Core (.NET Core Hosting Bundle)**)
- создает веб-сайт и пул приложений в сервере IIS и настраивает запуск сервера приложений системы в созданном веб-сайте. Имя сайта и пула совпадают и имеют вид: <AppName>-pkisrv-a.

Пул настраивается на работу под специальной, создаваемой автоматически, локальной учетной записью (пользователь пула). Имя учетной: <AppName>-pkisrv. Пароль для учетной записи формируется автоматически с помощью генератора случайных значений, длина пароля - 128 символов. Данный пароль меняется каждый раз при запуске скрипта **configure_pkisrv_windows.ps1**, и нигде не сохраняется, чтобы избежать возможности входа в интерактивную сессию под данной учетной записью.

- настраивает привязку протокола http или https к заданному порту (пока используется только <PortA>). Настраивается только один из протоколов в зависимости от параметров, задающих TLS сертификат. Если один из этих параметров задан - создается привязка https, иначе - http.
- формирует необходимые конфигурационные файлы сервера приложений в каталоге <InstanceDir>\config\<AppName>-pkisrv*.a.
- настраивает правила сетевого экрана Windows для разрешения входящих подключений по назначенным портам <PortA> и <PortB>. Имя правила сетевого экрана формируется по шаблону: EOS-pkisrv-<AppName>-In-TCP

3.3.3.1. Проверка портов сервера приложений

Скрипт перед конфигурированием службы, выполняет проверку на занятость портов, заданных в параметрах <PortA> и <PortB>, однако данная проверка не может считаться абсолютной, т.к. конфликт портов может возникнуть и после завершения процесса конфигурирования. Например, на сервер будет установлено дополнительное ПО, использующее те же самые порты. Поэтому окончательная ответственность за предотвращение конфликтов использования портов лежит на администраторе системы.

3.3.3.2. Описание параметров

скрипта configure_pkisrv_windows.ps1

Таблица 3

Параметр	Название	Примеры допустимых значений	Обязательный	Описание
InstanceDir	Каталог установки	C:\Eos\pki	Да	Каталог установки файлов приложения. Данное имя каталога используется для определения ресурсов, используемых при установке, и для определения пути каталогов хранения конфигурации (config) и рабочих файлов (var) службы сервера приложений.
AppName	Имя приложения	pki	Да	Имя приложения используется для формирования имени пула приложения и имени пользователя, под которым

Параметр	Название	Примеры допустимых значений	Обязательный	Описание
				<p>выполняется процесс пула.</p> <p>Можно использовать только маленькие латинские буквы, цифры, символ "-".</p> <p>Кроме того, значения этих параметров должны подбираться с учетом требований ОС Windows к создаваемым объектам. Одним из сильно ограничивающих требований является максимальная длина имени локального пользователя Windows - 20 символов,</p>
ServiceAccount	Учетная запись службы	AppPoolAccount LocalAccount	Да	<p>Выбор типа учетной записи под которой будет выполняться пул приложений IIS.</p> <p>Может иметь одно из значений:</p> <p>AppPoolAccount - для запуска пула приложений будет использована специальная учетная запись IIS</p> <p>LocalAccount - для запуска пула будет использована автоматически создаваемая скриптом локальная учетная запись с именем, совпадающим с именем пула приложений, и с автоматически сгенерированным паролем.</p>
PortA PortB	Порты привязки приложения	10071 10072	Да	Порты протокола TCP/IP, которые будут использованы сервером приложений для получения HTTP (REST) запросов.

Параметр	Название	Примеры допустимых значений	Обязательный	Описание
				<p>Нужно указать пару портов. Второй порт пока не используется. Планируется его использование в сценариях обновления системы без остановки обслуживания пользователей по схеме А-В:</p> <p>запуск второго экземпляра сервера приложений</p> <p>переключение настройки реверс-прокси на фронт-энд сервере на порты этого экземпляра</p> <p>остановка текущего экземпляра сервера приложений</p>
LogsFormat	Формат файлов логов	txt ecs clef	Нет	<p>Формат, в котором сервер приложений будет писать данные в файлы логов.</p> <p>txt - форматированный текстовый формат, предназначенных для непосредственного чтения человеком.</p> <p>ecs - Elastic Common Schema. Структурированный json формат, предназначенный для последующей загрузки на сервер мониторинга. Этот формат является "родным" для стека сбора, хранения и анализа логов Elastic-Logstash-Kibana. И, возможно, поддерживается и другими вендорами аналогичных систем.</p> <p>clef - это формат, родной для библиотеки Serilog.</p>

Параметр	Название	Примеры допустимых значений	Обязательный	Описание
				Отличается компактностью записи. Может быть использован для загрузки на сервер мониторинга, но, возможно, потребует ручной настройки парсера для загрузки в систему хранения. Точно "из коробки" данный формат поддерживается системой Seq (платная, проприетарная), а также утилитой просмотра логов Analogy.LogViewer (бесплатная, OSS).

3.3.3.3. Пример вызова скрипта `configure_pkisrv_windows.ps1`.

```
.\configure_pkisrv_windows.ps1 -InstanceDir C:\Eos\pki -AppName pki -PortA 10071 -PortB 10072 -ServiceAccount LocalAccount
```

3.3.3.4. Проверка установки службы сервера приложений

В случае успешного завершения установки, работоспособность службы сервера приложений можно проверить набрав в браузере адрес приложения, находясь на этом же сервере: **http://localhost:<PortA>**. Должен открыться диагностический экран с перечнем модулей сервера приложений.

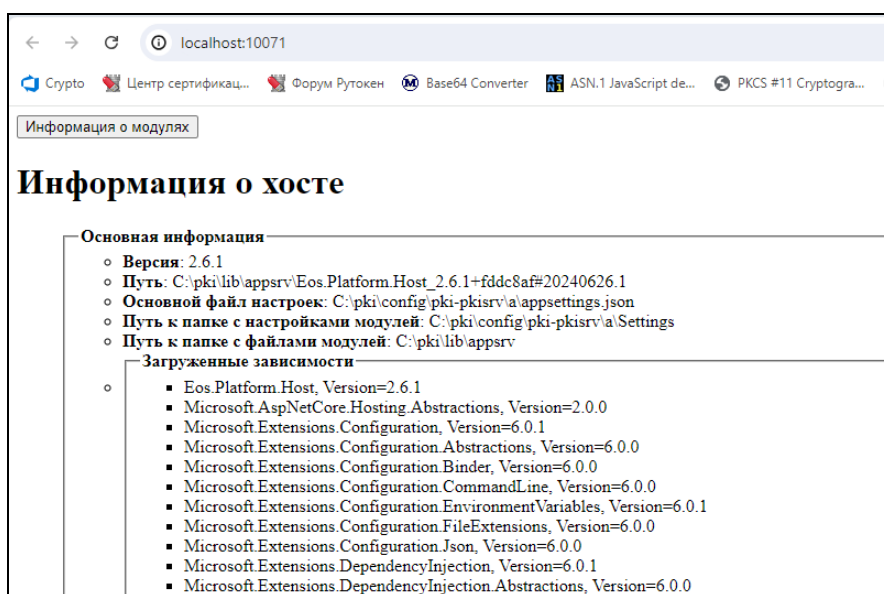


Рисунок 17

3.3.4. Установка фронт-энд web-сервера

Для установки фронт-энд web-сервера используется скрипт **configure_pkiweb_windows.ps1**.

Скрипт выполняет следующие действия:

- выполняет проверку необходимых установленных компонентов и конфигураций:
- Установлена **роль Web-сервер**
- Установлен **модуль IIS Url Rewrite** версии 2.1 и выше
- Установлен **модуль IIS Application Request Routing** версии 3.0 и выше
- Включена настройка **Enable Proxy** в **Application Request Routing**
- создает веб-сайт и пул приложений в сервере IIS. Имя сайта и пула совпадают и имеют вид: **<AppName>-pkiweb**. Пул запускается под учетной записью **ApplicationPoolIdentity**.
- настраивает привязку сайта к порту TCP/IP в соответствии с параметрами **WebServerName**, **WebServerPort**, привязка конфигурируется на использование протокола HTTPS.
- настраивает правила сетевого экрана Windows для разрешения входящих подключений, если используется нестандартный порт **WebServerPort**. Имя правила сетевого экрана формируется по шаблону: **EOS-pkiweb-<AppName>-In-TCP**
- настраивает правила реверс-прокси для передачи запросов из web-приложения на сервер приложения

3.3.4.1. Конфигурирование привязки сайта и HSTS (HTTP Strict Transport Security)

Фронт-энд сервер может быть сконфигурирован с привязками двух видов:

- привязка по стандартным портам
- привязка по нестандартному порту

Вид привязки определяется значениями параметров **WebServerName** и **WebServerPort**.

Привязка по стандартным портам 443 и 80 выполняется, если не передан параметр **WebServerPort**.

Поскольку фронт-энд сервер должен работать только по протоколу HTTPS, при попытке пользователя зайти на сайт на порт 80, сервер выполняет перенаправление запроса на порт 443 и установку заголовка HSTS. Заголовок обрабатывается браузером пользователя, и в дальнейшем браузер будет отправлять запросы только по протоколу HTTPS на порт 443.

В привязке также указывается публичное имя веб-сервера, если оно передано в параметре **WebServerName**, такая конфигурация IIS называется **виртуальный веб-сервер**. Использование виртуального веб-сервера позволяет установить на одном сервере с IIS несколько сайтов, каждый из которых будет привязан к стандартным портам, что упрощает пользователю набор адреса сайта в браузере, так как нет необходимости вводить номер порта.

Использование виртуальных серверов также подразумевает, что на DNS серверах в сети организации будут заведены соответствующие CNAME или ALIAS записи, позволяющие направить запросы браузера на один физический сервер при обращении к любому виртуальному серверу, установленному на нем.

Если все-таки необходимо выполнить установку без использования функционала виртуальных серверов, например, приложение должно быть доступно по IP адресу или в организации нет возможности настроить DNS, параметр **WebServerName** не должен передаваться при выполнении установки и привязка будет выполнена для любых входящих запросов. При использовании стандартных портов 443 и 80 скрипт конфигурирования не сможет настроить веб-сервер, если в IIS уже есть сайт с привязкой к одному из стандартных портов. Как правило, это так и есть - по умолчанию сервер IIS сразу после установки уже содержит сайт Default Web Site, привязанный к порту 80. Чтобы установить в таком случае систему на стандартные порты, нужно отключить или удалить сайт Default Web Site.

Если отключить Default Web Site нет возможности, систему придется настроить на работу по не стандартному порту. Для этого номер порта нужно передать в параметре **WebServerPort**.

3.3.4.2. Проверка порта frontend сервера

Скрипт перед конфигурированием службы, выполняет проверку на занятость порта, заданного в параметре **WebServerPort**, однако данная проверка не может считаться абсолютной, т.к. конфликт портов может возникнуть и после завершения процесса конфигурирования. Например, на сервер будет установлено дополнительное ПО, использующее те же самые порты. Поэтому окончательная ответственность за предотвращение конфликтов использования портов лежит на администраторе системы.

3.3.4.3. Описание параметров

скрипта `configure_pkiweb_windows.ps1`

Таблица 4

Параметр	Название	Примеры допустимых значений	Обязательный	Описание
InstanceDir	Каталог установки	C:\Eos\pki	Да	Каталог установки файлов приложения. Данное имя каталога используется для определения ресурсов, используемых при установке, и для определения пути каталогов хранения конфигурации (config).
AppName	Имя	pki	Да	Имя

Параметр	Название	Примеры допустимых значений	Обязательный	Описание
	приложения			<p>приложения используется для формирования имени пула приложения.</p> <p>Можно использовать только маленькие латинские буквы, цифры, символ "-".</p> <p>Кроме того, значения этих параметров должны подбираться с учетом требований ОС Windows к создаваемым объектам.</p> <p>Одним из сильно ограничивающих требований является максимальная длина имени локального пользователя Windows - 20 символов.</p>
WebServerName	Публичное имя сайта	pki.myorg.ru	Нет	<p>Публичное имя сайта, по которому пользователи должны будут обращаться для работы с приложением.</p> <p>Используется для создания привязки сайта приложения в режиме виртуального сервера IIS.</p> <p>Если имя сайта не задано, привязка будет создана без указания имени узла.</p>
WebServerPort	Порт привязки сайта	1443	Нет	<p>Номер порта TCP/IP для привязки сайта к нестандартному порту.</p> <p>Если порт не задан, привязка будет выполнена к стандартным портам 443 и 80 (см. Конфигурирование привязки сайта и HSTS (HTTP Strict Transport</p>

Параметр	Название	Примеры допустимых значений	Обязательный	Описание
				Security)).
AppSrvUrl	Адрес сервера приложений	http://localhost:10071	Да	Адрес сервера приложения. Должен быть указан полный URL включающий протокол, адрес и порт привязки сервера приложений.
PfxPath	Путь к pfx контейнеру	C:\Users\Administrator\pkisrv.pfx	Да (см. описание)	Путь к файлу .pfx содержащему публичный и приватный ключи сертификата для TLS протокола. Не может использоваться одновременно с параметрами CertSerialNumber или CertThumbprintVal. Поскольку файл pfx содержит закрытый ключ, необходимо внимательно следить, чтобы данный файл не попал в общий доступ.
PfxPassphrase	Пароль к контейнеру .pfx	'Passphrase'	Нет (см. описание)	Если пароль не передан, скрипт запросит его в процессе выполнения. Если pfx файл не защищен паролем, нужно ввести пустую строку при выдаче приглашения скрипта.
CertSerialNumber	Серийный номер сертификата	00D5A3E153869C7944	Да (см. описание)	Серийный номер сертификата является альтернативным способом для установки сертификата, необходимого для работы с использованием TLS. Если этот параметр указан, то сервер будет доступен по протоколу https. Не может использоваться одновременно с параметрами

Параметр	Название	Примеры допустимых значений	Обязательный	Описание
				PfxPath или CertThumbprintVal.
CertThumbprint	Отпечаток сертификата	14DC7A0C5A896 BB6B3E286F63E 258C655EC5DC A8	Да (см. описание)	Отпечаток сертификата является альтернативным способом для установки сертификата, необходимого для работы с использованием TLS. Если этот параметр указан, то сервер будет доступен по протоколу https. Не может использоваться одновременно с параметрами PfxPath или CertSerialNumber.

3.3.4.4. Пример вызова скрипта configure_pkiweb_windows.ps1

```
.\configure_pkiweb_windows.ps1 -InstanceDir C:\Eos\pki -AppName pki -
WebServerName pki.myorg.ru -AppSrvUrl http://localhost:10071 -PfxPath
C:\Users\Administrator\pkisrv.pfx -PfxPassphrase 'Passphrase'
```

3.3.4.5. Добавление имени сайта в hosts

Для успешного резолва имени требуется внести его в файл C:\Windows\System32\drivers\etc\hosts. Т.е. необходимо добавить строку в конец файла:

127.0.0.1

<WebServerName>

Например:

127.0.0.1 pki.myorg.ru

3.3.4.6. Проверка установки системы

Проверка осуществляется открытием в Интернет браузере (например, Firefox) страницы по адресу **https://<WebServerName>/app/pki**. Должна появиться главная страница PKI:

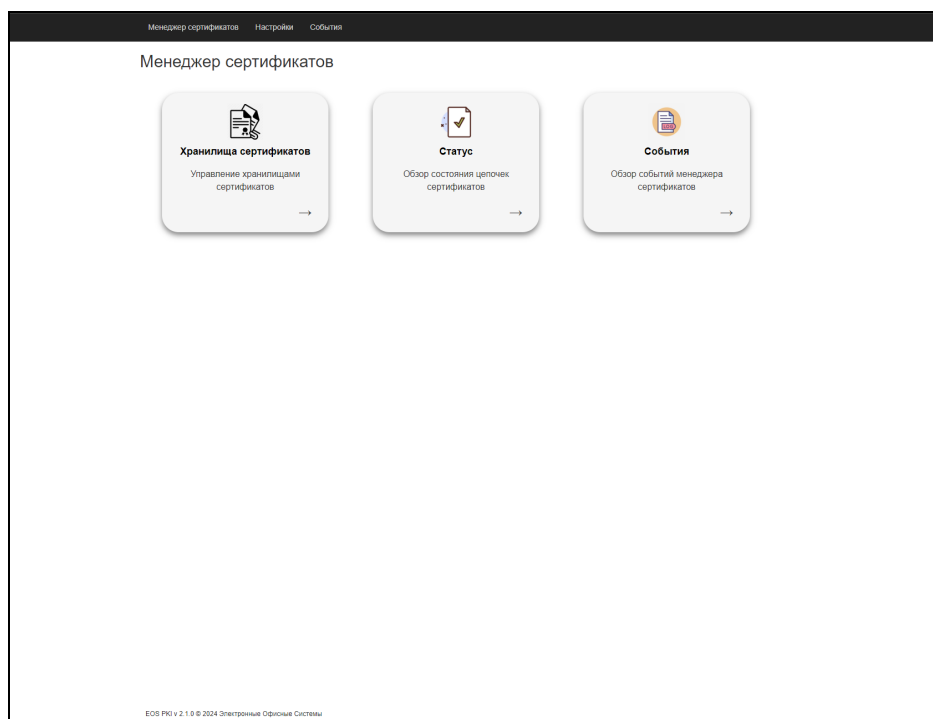


Рисунок 18

3.3.5. Перед началом работы

Для корректной и полноценной работы приложения следует выполнить следующие шаги по настройке:

- Импортировать промежуточные и корневые сертификаты (раздел "Автоматический импорт сертификатов Аккредитованных УЦ РФ (КЭП)" в руководстве пользователя РКІ-сервиса)
- Обновить статусы сертификатов (раздел "Панель «Обновление статусов сертификатов»" в руководстве пользователя РКІ-сервиса)

3.4. Перенос данных с прежних версий РКІ (< v3.0.0)

Перенос включает в себя следующие шаги:

- Остановка пула и сайта прежней версии РКІ (< v3.0.0)
- Остановка пула и сайта текущей версии РКІ (>= v3.0.0)
- Перенос хранилищ сертификатов
- Перенос файла конфигурации
- Редактирование файла конфигурации для обеспечения совместимости
- Возобновление работы пула и сайта текущей версии РКІ (>= v3.0.0)
- Сохранение настроек для добавления недостающих параметров

3.4.1. Остановка пула и сайта прежней версии

3.4.1.1. Вручную

Останавливаем Default Web Site:

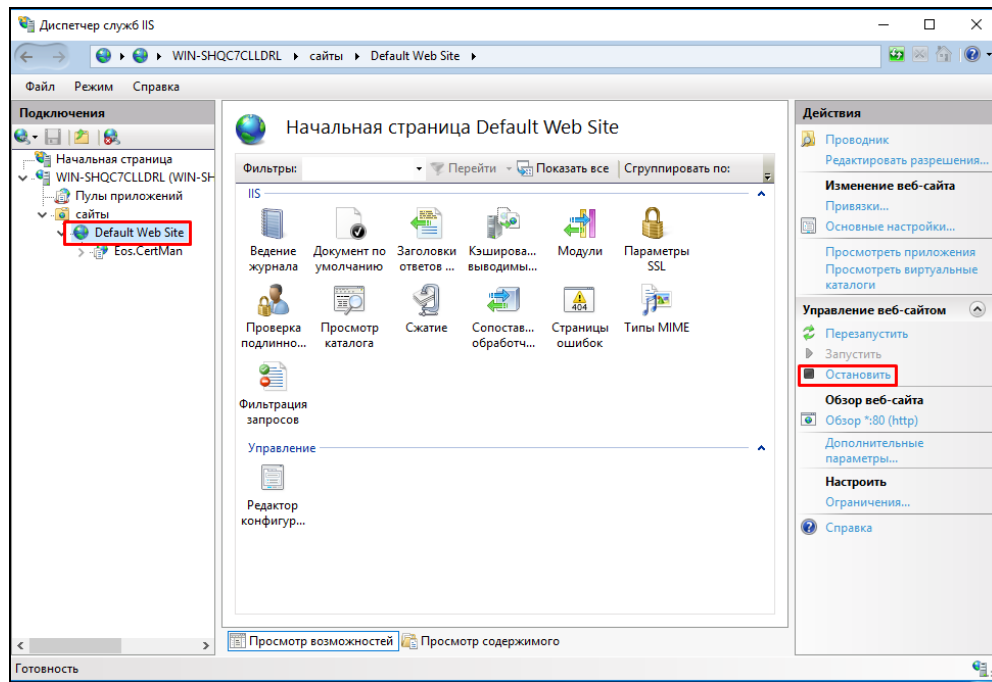


Рисунок 19

Останавливаем DefaultAppPool:

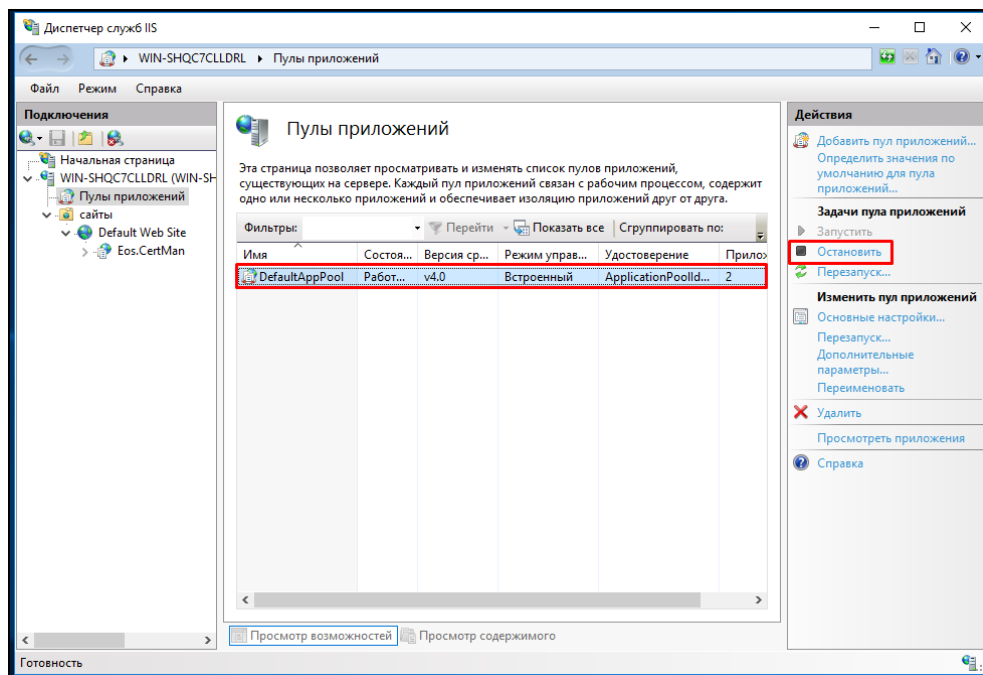


Рисунок 20

3.4.1.2. PowerShell

```
Stop-Website -Name "Default Web Site"
Stop-WebAppPool -Name DefaultAppPool
```

3.4.2. Остановка пула и сайта текущей версии

3.4.2.1. Вручную

Останавливаем <AppName>-pkisrv-a сайт:

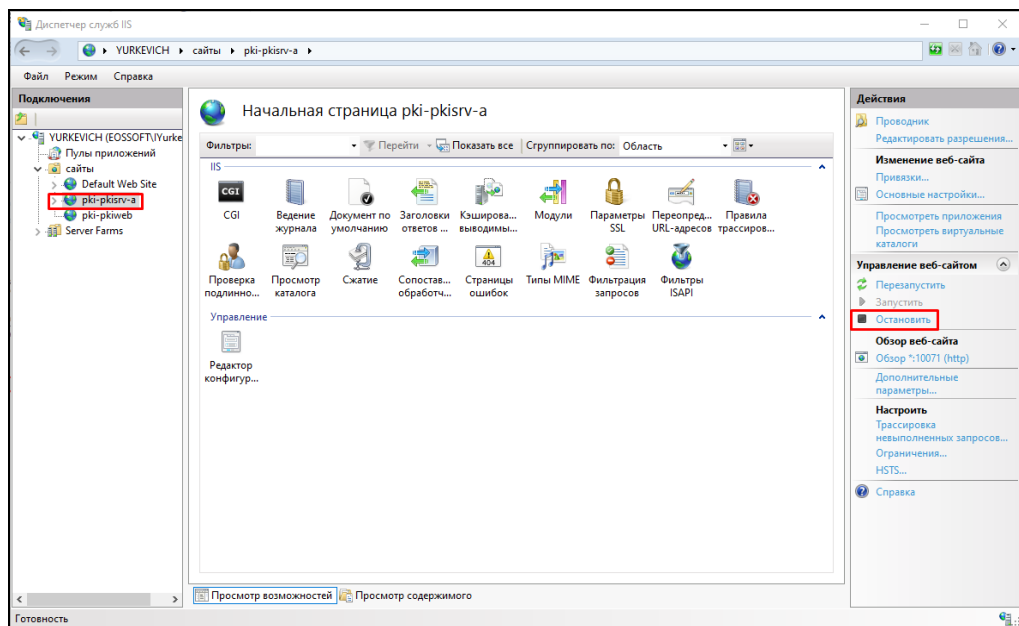


Рисунок 21

Останавливаем <AppName>-pkisrv-a пул:

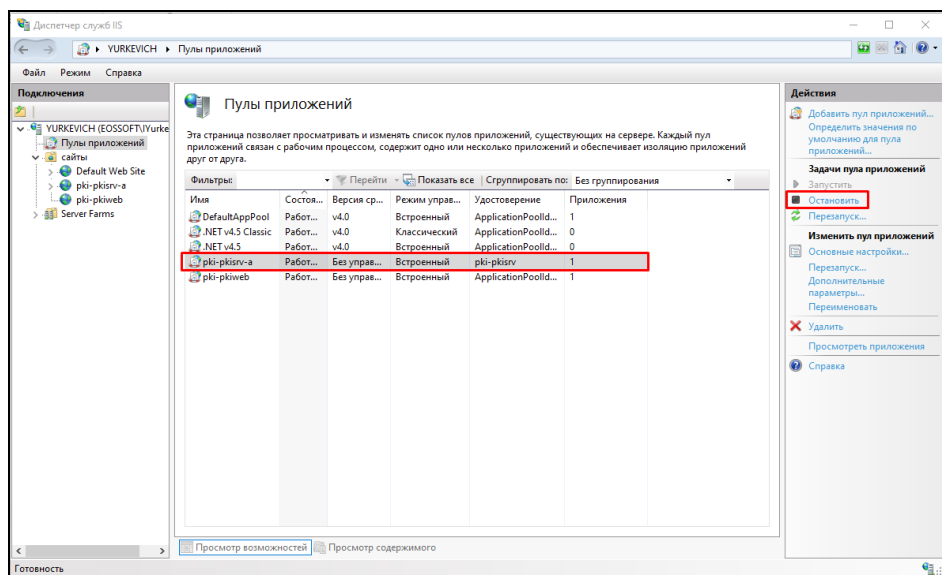


Рисунок 22

3.4.2.2. PowerShell

```
Stop-Website -Name <AppName>-pkisrv-a
Stop-WebAppPool -Name <AppName>-pkisrv-a
```

3.4.3. Перенос хранилищ сертификатов

Требуется перенести каталог хранилищ **stores**, путь до которого указан в настройках прежней версии PKI

Настройки

"Белый" список интернет-адресов для скачивания списков отзыва

Общие настройки Создать подкаталоги Проверить конфигурацию

Имя PKI сервиса:	EOS PKI
Список разрешенных хостов:	127.0.0.1;192.168.0.0/24;::1
Зона импорта:	D:\Fistimport_cer
Сервис отправки e-mail уведомлений:	D:\Fistmailer
Каталог хранилищ:	D:\Fiststores
Сервис обновления статуса сертификатов:	D:\Fiststat
КАРМА:	http://127.0.0.1:8080
Загружать СОС из каталога импорта:	☐

Рисунок 23

в каталог `<InstanceDir>\var\pki-pkisrv` с подтверждением замены файлов.

3.4.4. Перенос файла конфигурации

Требуется перенести прежний файл конфигурации `C:\inetpub\wwwroot\Eos.CertMan\appsettings.json` в каталог `<InstanceDir>\var\pki-pkisrv`

Далее следует переименовать файл: `<InstanceDir>\var\pki-pkisrv\appsettings.json` → `<InstanceDir>\var\pki-pkisrv\pkiConfig.json`, удалив перед этим уже существующий `<InstanceDir>\var\pki-pkisrv\pkiConfig.json` файл.

3.4.5. Редактирование файла конфигурации для обеспечения совместимости

Для успешного использования прежнего конфигурационного файла необходимо вручную изменить несколько параметров:

Возможно, что в вашем файле конфигурации не будет каких-то параметров, рассмотренных ниже - ничего страшного, значит этот параметр пропускаем и идём дальше

1. Имя блока `"ApplicationInfo"` изменить на `"AppInfo"`

Было:

```
"ApplicationInfo": {
  "Name": "Eos.CertMan"
},
```

Стало:

```
"AppInfo": {
  "Name": "Eos.CertMan"
},
```

2. Заменить адреса рабочих каталогов сервиса с предыдущей версии на устанавливаемую, в формате `<InstanceDir>\var\pki-pkisrv\...`

Пример с учётом того, что `<InstanceDir> = "C:\Eos\pki"`:

Было:

```
"import": "C:\\Eos.CertMan\\import_cer",
"stores": "C:\\Eos.CertMan\\stores",
"stat": "C:\\Eos.CertMan\\stat",
"mailer": "C:\\Eos.CertMan\\mailer",
```

Стало:

```
"import": "C:\\Eos\\pki\\var\\pki-pkisrv\\import",
"stores": "C:\\Eos\\pki\\var\\pki-pkisrv\\stores",
"stat": "C:\\Eos\\pki\\var\\pki-pkisrv\\stat",
"mailer": "C:\\Eos\\pki\\var\\pki-pkisrv\\mailer",
```

3. В блоке **mailNotification** параметр **port**: необходимо удалить кавычки - значение должно быть числом, а не строкой:
 "port": "587" -> "port": 587

Было:

```
"mailNotification": {
  "enabled": false,
  "smtp": "smtp.mail.ru",
  "port": "587",
```

Стало:

```
"mailNotification": {
  "enabled": false,
  "smtp": "smtp.mail.ru",
  "port": 587,
```

4. В блоке **proxy** параметр **port**: необходимо удалить кавычки - значение должно быть числом, а не строкой:
 "port": "3128" -> "port": 3128

Было:

```
"proxy": {
  "enabled": false,
  "anonymous": false,
  "host": "194.87.111.108",
  "port": "3128",
```

Стало:

```
"proxy": {
  "enabled": false,
  "anonymous": false,
  "host": "194.87.111.108",
  "port": 3128,
```

5. В блоке **signatureImport** параметр **errCountForCancel**: необходимо удалить кавычки - значение должно быть числом, а не строкой:
 "errCountForCancel": "10" -> "errCountForCancel": 10

Было:

```
"signatureImport": {
  "path": "D:\\FiSt\\DeloWebSignatures\\EOS_EXPORT_SIGN",
  "errCountForCancel": "10",
  "needCleaning": false
```

Стало:

```

"signatureImport": {
  "path": "D:\\FiSt\\DeloWebSignatures\\EOS_EXPORT_SIGN",
  "errCountForCancel": 10,

```

6. В блоке `updateCerts` параметр `autoCleanStartTime`: необходимо удалить кавычки - значение должно быть числом, а не строкой:
`"autoCleanStartTime": "60" -> "autoCleanStartTime": 60`

Было:

```

"updateCerts": {
  "enabled": false,
  "autoClean": true,
  "autoCleanStartTime": "60"

```

Стало:

```

"updateCerts": {
  "enabled": false,
  "autoClean": true,
  "autoCleanStartTime": 60

```

7. В блоке `importETrust` параметр `nextLaunchDelayInHours`: необходимо удалить кавычки - значение должно быть числом, а не строкой:
`"nextLaunchDelayInHours": "24" -> "nextLaunchDelayInHours": 24`

Было:

```

"importETrust": {
  "enabled": false,
  "nextLaunchDelayInHours": "24"
}

```

Стало:

```

"importETrust": {
  "enabled": false,
  "nextLaunchDelayInHours": 24
}

```

Примечание

После первого запуска приложения настройки времени для службы проверки целостности хранилищ сбросятся. На веб странице настроек необходимо задать время запуска и остановки заново.

Проверка целостности хранилищ		
Проверка целостности:	☒	
Время запуска:	00:00	⌚
Время остановки:	00:00	⌚

Рисунок 24

3.4.6. Возобновление работы пула и сайта текущей версии PKI

3.4.6.1. Вручную

Запускаем `<AppName>-pkisrv`-а пул:

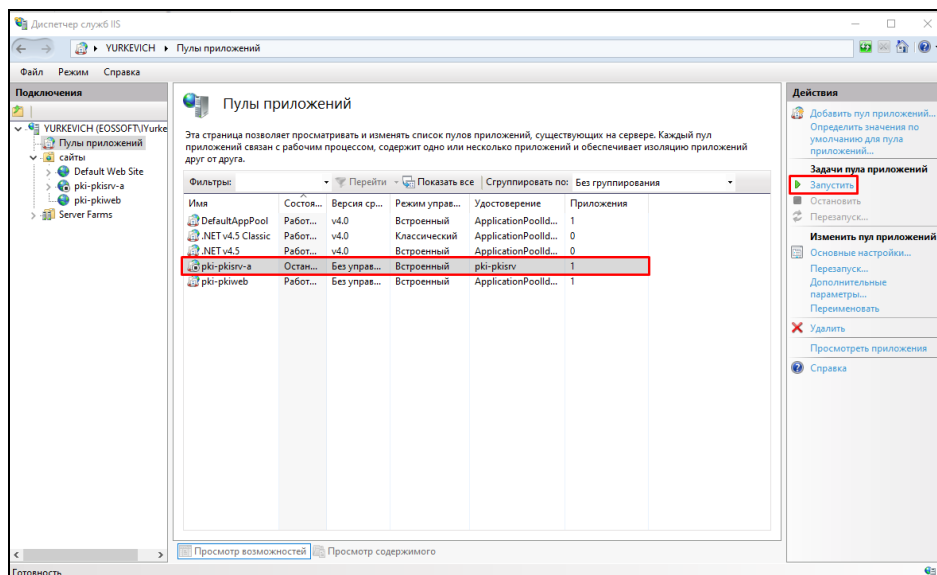


Рисунок 25

Запускаем <AppName>-pkissrv-a сайт:

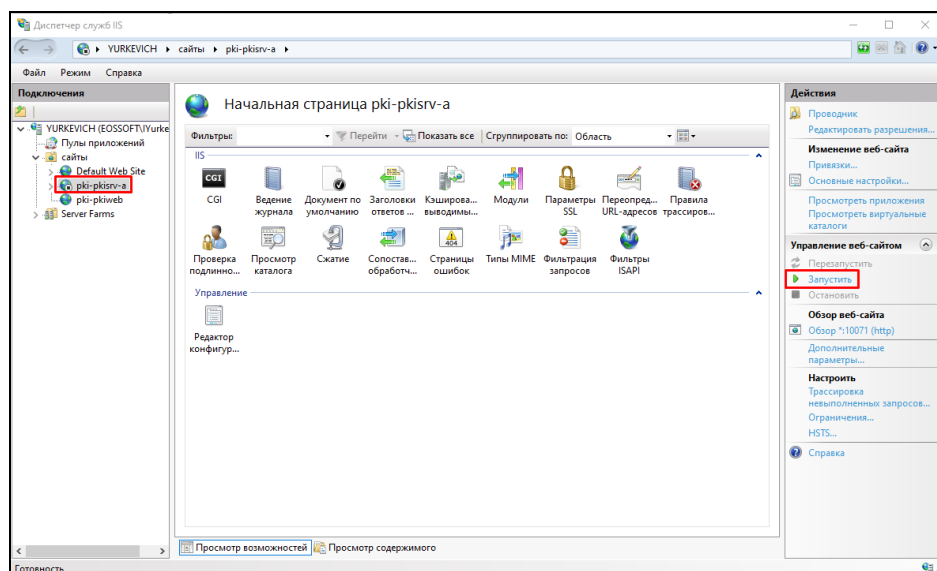


Рисунок 26

3.4.6.2. PowerShell

```
Start-WebAppPool -Name <AppName>-pkissrv-a
Start-Website -Name <AppName>-pkissrv-a
```

3.4.7. Сохранение настроек для добавления недостающих параметров

Вполне возможны ситуации, когда в переносимом файле конфигурации не будет хватать каких-то параметров, используемых в приложении. Для исключения ошибок при обращении к ним сервисом требуется сохранить текущую конфигурацию на странице настроек.

Переходим на страницу настроек (раздел "Страница «Настройки»" в руководстве пользователя РКІ-сервиса), пролистываем страницу вниз и нажимаем на кнопку "Сохранить изменения конфигурации". После этого файл конфигурации будет перезаписан и дополнен всеми необходимыми параметрами.

3.5. Обновление системы

Перед обновлением системы необходимо выполнить [остановку пула и сайта](#).

Далее на целевой системе, при помощи стандартного архиватора, необходимо, с заменой файлов, извлечь файлы системы из обновленного дистрибутива по пути `<InstanceDir>`. Запустить соответствующий скрипт из каталога с требуемой, для установки, версией.

Вызовы скриптов при обновлении идентичны вызовам при установке. Пул и сайт после обновления запускаются скриптом самостоятельно.

Параметры для скриптов обновления должны быть идентичны параметрам, указанным при установке!

Удаление системы

Для удаления требуемой сборки необходимо перейти в каталог с соответствующей версией:

```
cd <InstanceDir>/lib/install/<install_ver>/windows
```

Далее необходимо запустить скрипт `uninstall.ps1`:

```
.\uninstall.ps1 -InstanceDir <InstanceDirVal> -AppName <AppNameVal>
```

`<InstanceDirVal>` - обязательный. Каталог установки файлов приложения, например, `C:\Eos\pki`

`<AppNameVal>` - обязательный. Наименование приложения, например, `pki`

Внимание! Перед удалением, скрипт не запрашивает дополнительных разрешений. Рекомендуем запускать этот же скрипт, добавив параметр `-DryRun`, который позволит оценить весь перечень удаляемых компонентов заблаговременно.

Пример вызова скрипта с параметром `-DryRun`, для проверки списка удаляемых компонентов:

```
.\uninstall.ps1 -InstanceDir <InstanceDirVal> -AppName <AppNameVal> -DryRun
```

3.6. Очистка неиспользуемых дистрибутивов предыдущих версий

Для удаления неиспользуемых дистрибутивов необходимо перейти в каталог, с которого был установлен актуальный экземпляр.

```
cd <InstanceDir>/lib/install/<install_ver>/windows
```

Далее необходимо запустить скрипт `uninstall.ps1` с параметром `-CleanUp`:

```
.\uninstall.ps1 -InstanceDir <InstanceDirVal> -AppName <AppNameVal> -CleanUp
```

`<InstanceDirVal>` - обязательный. Каталог установки файлов приложения, например, `C:\Eos\pki`

`<AppNameVal>` - обязательный. Наименование приложения, например, `pki`

Алгоритм работы скрипта, запущенного с параметром `CleanUp`.

1. Выбираются все компоненты существующих сборок, кроме той, с которой запущен данный скрипт. Выборка осуществляется путём чтения файлов, содержащих описание компонентов.
2. Отдельно определяются компоненты активной сборки. Данный список составляется исходя из версий которые, содержат в себе файлы appsettings.json и/или index.html.
3. Из списка компонентов, не относящихся к комплекту дистрибутива из которого был запущен скрипт, делается исключение компонентов активной сборки.
4. Происходит удаление компонентов по сформированному, после всех исключений, списку.

Результатом работы скрипта запущенного с параметром `-CleanUp` будет вывод всех удалённых компонентов.

Внимание! Перед удалением, скрипт не запрашивает дополнительных разрешений. Рекомендуем запускать этот же скрипт, добавив параметр `-DryRun`, который позволит оценить весь перечень удаляемых компонентов заблаговременно.

Пример вызова скрипта с параметром `-DryRun`, для проверки списка удаляемых компонентов:

```
.\uninstall.ps1 -InstanceDir <InstanceDirVal> -AppName <AppNameVal> -CleanUp  
-DryRun
```

4. ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ

4.1. Основные понятия

- **Сертификат**

Сертификат открытого ключа (так же «сертификат ЭП», «сертификат ключа подписи», «сертификат ключа проверки электронной подписи») – электронный документ установленного формата (x.509), содержащий информацию, однозначно указывающую на принадлежность владельцу сертификата («субъекту») определенного **открытого криптографического ключа**. [1]

Структура сертификата содержит множество стандартизованных информационных полей (поля сертификата), определяющих правила, возможности и ограничения использования данного сертификата. Например, даты начала и окончания срока действия сертификата.

Сертификат выпускается (издается) Удостоверяющим Центром (УЦ), который подписывает сертификат своей электронной подписью. Электронная подпись гарантирует неизменность информации сертификата.

В «физическом плане» сертификат представляет собой файл с расширением «cer» или «crt», например **mycert.cer**

В Проводнике Windows обозначается значком



Файлы, содержащие сразу несколько сертификатов, могут иметь расширения “p7b”, “pfx”, “sst”.

- **Наблюдаемый сертификат**

Сертификат, добавленный в качестве наблюдаемого в «ЭОС РКИ-сервис». Такой сертификат учитывается и обрабатывается в ЭОС РКИ-сервисе до тех пор, пока не будет удален из сервиса.

- **Категории сертификатов**

Для целей ПО «ЭОС РКИ-сервис» и настоящего руководства выделены следующие категории сертификатов, в зависимости от владельца, издателя и статуса сертификата:

- **Сертификат конечного пользователя/системы** – сертификат, выданный Удостоверяющим Центром. Владелец сертификата, указанным в поле «субъект», является физическое или юридическое лицо, должностное лицо, информационная система, веб-сайт\сервер и пр. Такой сертификат может быть использован для выполнения пользовательских операций (ЭП, шифрование данных, аутентификация и т.д.), но не может использоваться для подписи (издания) других сертификатов. Наиболее массовая категория сертификатов.
- **Сертификат промежуточного Удостоверяющего Центра** – сертификат, выданный Удостоверяющим Центром (корневым или другим промежуточным). Владелец, указанным в поле «субъект», является Удостоверяющий Центр. Данный сертификат **может** быть применен для выдачи (издания) других

сертификатов. В системе квалифицированных сертификатов (по 63-ФЗ) такие сертификаты имеют Аккредитованные Удостоверяющие Центры.

- **Сертификат корневого Удостоверяющего Центра** – сертификат, издателем и владельцем которого является один и тот же субъект, «самоподписанный сертификат».

Является «корнем доверия». Решение о доверии такому сертификату должно приниматься осознанно, человеком, поскольку доверие такому сертификату (корневому УЦ) означает доверие всем нижележащим промежуточным УЦ, сертификаты которых изданы (подписаны) данным корневым УЦ, и, далее, пользовательским сертификатам.

В системе квалифицированных сертификатов РФ (по 63-ФЗ) таких корневых сертификатов несколько, со сроками действия каждого 18 лет, время от времени выпускаются новые. Более ранние были выпущены с «владельцем» Головной Удостоверяющий Центр, позже – «Минкомсвязь России», современный – «Минцифры России».

- **Сертификаты, утратившие доверие** – Для оперативного\аварийного «блокирования» доверия к конкретным сертификатам в среде предприятия.
- **Список отзыва сертификатов (СОС)**

Удостоверяющие Центры не только выпускают сертификаты, но и могут их отозвать, по различным причинам.

Отзыв сертификата представляет собой добавление серийного номера такого сертификата в Список Отзыва Сертификатов (СОС) выпустившего его УЦ.

СОС так же, как и сертификат, представляет собой электронный документ, подписанный электронной подписью Удостоверяющего Центра.

Удостоверяющий Центр с установленной периодичностью публикует СОС. Номер отозванного сертификата фигурирует в СОС до тех пор, пока не закончится срок действия сертификата, изначально в нем обозначенный.

Наличие актуального СОС необходимо для определения статуса сертификата – если сертификат выдан, и на текущий момент не отозван (не находится в СОС) – сертификат можно использовать.

Аккредитованные Удостоверяющие Центры (по 63-ФЗ) выпускают СОС каждый день.

В «физическом плане» СОС представляет собой файл с расширением «crl», например, **CA_number_1_date.crl**

В Проводнике Windows обозначается значком



[1] Принадлежность субъекту открытого ключа так же подразумевает монопольное владение субъектом закрытым ключом, парным к данному открытому, и используемого для создания электронной подписи.

4.2. Среда функционирования PKI-сервиса

- Alt Linux (версии Сервер 10)

- Windows (версии Windows 10, Server 2019)

4.3. Функции РКИ-сервиса

- Централизованное размещение сертификатов организации и, при необходимости, корреспондентов
- Учёт, статистика и управление сертификатами организации
- Автоматическая актуализация статуса сертификатов КЭП и НЭП
- Функции предоставления статуса сертификатов для СПО КАРМА в организации
- Оповещение по e-mail и информирование из графической оболочки (окончание срока действия сертификата и/или закрытого ключа)
- Импорт актуальных используемых сертификатов из базы СЭД «ДЕЛО»

4.4. Компоненты РКИ-сервиса

4.4.1. Служба наблюдения

Основной программный компонент ЭОС РКИ-сервиса. Веб-приложение. Хранит сертификаты, обрабатывает их информацию и предоставляет ее остальным компонентам. Исполняется в фоновом режиме (как служба). Внутри службы периодически запускается пересчёт статусов. сертификатов

4.4.2. Служба оповещения

С установленной периодичностью отбирает сертификаты, требующие внимания оператора (истечение срока действия сертификата и/или закрытого ключа) и оповещает о них посредством e-mail. Запускается периодически по настройке или принудительно из интерфейса.

4.4.3. Графический интерфейс

Веб-сайт для отображения, фильтрации, отбора и экспорта информации по наблюдаемым сертификатам, настройки и интерактивного взаимодействия сервиса с оператором. URL для входа (пример) – <https://pki.myhost.loc/app/pki>

4.4.4. Служба обмена информацией по сертификатам с СПО КАРМА

Сервис, предназначенный для автоматизированного получения информации по статусам сертификатов КЭП и НЭП для СПО КАРМА, установленном на компьютерах организации.

СПО КАРМА может подключаться к данному сервису и получать актуальную информацию по статусам любых сертификатов (например, при запрете выхода в интернет с АРМ организации), а так же передавать информацию о новых сертификатах, используемых для подписания на АРМе с КАРМОЙ, в ЭОС РКИ-сервис, для дальнейшего наблюдения (автоматическое пополнение базы наблюдаемых сертификатов).

Настройка СПО КАРМА для работы с ЭОС РКИ-сервисом описана в Приложении 2.

4.5. Требования среды функционирования РКИ-сервиса

4.5.1. Требования к аппаратному обеспечению

- Выделенный сервер либо виртуальная машина
- Не менее 2 ядер процессора
- Не менее 1 Гб оперативной памяти
- Не менее 500 Мб дискового пространства + 10 Мб на каждую 1000 наблюдаемых сертификатов

4.5.2. Требования к системному и служебному ПО

- Операционная система из списка поддерживаемых ЭОС РКИ-сервисом
- Сертифицированный ФСБ России криптопровайдер, реализующий российские криптографические алгоритмы. Например, «КриптоПро CSP» 5.0 R2 (5.0.12000) и выше для соответствующей платформы
- СПО КАРМА
- для Windows минимальная версия: **56.2.436**
- для Linux минимальная версия: **56.2.456**
- Браузер, запускаемый на хосте развертывания ЭОС РКИ-сервиса

4.5.3. Требования к сетевому окружению, расположению и доступности

4.5.3.1. Доступность почтового сервера, способа подключения и наличие учетной записи

Для работы функций оповещения по электронной почте необходимо наличие предварительно настроенной почтовой учетной записи, от имени которой будут рассылаться оповещения, например eos.pkiservice@mydomaine.ru.

Возможно подключение по SMTP протоколу.

Соответствующие протоколы и сетевые порты не должны блокироваться средствами межсетевого экранирования и антивирусными приложениями.

Возможно анонимное подключение к SMTP, с или без использования SSL.

4.5.3.2. Доступность сервиса для подключения СПО КАРМА с компьютеров организации

СПО КАРМА (версии **56.2.436** и выше), расположенное на компьютерах сотрудников организации, имеет возможность использовать ЭОС РКИ-сервис для non-OS-based получения статуса сертификатов. Функция особенно актуальна для закрытых сетей без доступа в интернет.

Для функционирования данной возможности должна быть обеспечена сетевая доступность ЭОС РКИ-сервиса по протоколу для компьютеров организации. Соответствующий протокол и порт не должен блокироваться средствами межсетевого экранирования и антивирусными приложениями.

4.5.3.3. Доступность внутреннего УЦ (НЭП)

При использовании сертификатов внутреннего удостоверяющего центра(ов) организации (внутридоменного; стороннего доверенного) должна быть организована связь по протоколу http между ЭОС РКИ-сервисом и таким УЦ.

4.5.3.4. Доступ в интернет (КЭП)

Настоятельно рекомендуется устанавливать ЭОС РКИ-сервис на компьютере\сервере, имеющем доступ к сети Интернет (http), иначе многие **автоматизации**, относящиеся к сфере квалифицированных сертификатов (Аккредитованные Удостоверяющие Центры по 63-ФЗ «Об электронной подписи»), будут недоступны.[3]

[2] Если связь с УЦ невозможно установить, будут необходимы регулярные «ручные» регламентные работы по доставке СОС таких УЦ в ЭОС РКИ-сервис

[3] Если доступ в Интернет невозможен, будут необходимы **ежедневные** «ручные» регламентные работы

4.6. Установка, обновление, создание резервной копии и удаление ЭОС РКИ-сервиса

Установка и первичная настройка, обновление с версий 1.* и 2.*, способы создания резервных копий и восстановление из них, а так же удаление ЭОС РКИ-сервиса описаны в отдельных руководствах для соответствующих поддерживаемых платформ (операционных систем).

4.7. Интерфейс

4.7.1. Запуск

ЭОС РКИ-сервис является веб-приложением, для интерактивного взаимодействия необходимо использовать браузер.

Запустите браузер, и в адресной строке наберите адрес, присвоенный сервису на этапе установки, например – <https://pki.myhost.loc/app/pki>

4.7.2. Выход

Закройте страницу сайта ЭОС РКИ-сервис, либо закройте браузер.

4.7.3. Замечание по модели безопасности

ЭОС РКИ-сервис текущей версии НЕ реализует ролевых или иных разграничительных моделей доступа с разным функционалом для разных категорий (администраторы, пользователи).

Настройка и интерактивное взаимодействие с сервисом предполагается с полными, «административными» правами, поэтому по умолчанию сайт сервиса целиком доступен только при подключении к нему из браузера, запущенного на этом же компьютере\сервере. Для работы администратора с удаленных хостов внесите их в список разрешенных подключений в соответствующем разделе в «Настройках»

4.7.4. Доступные из интерфейса операции с сертификатами

- Добавление в сервис наблюдения единичного сертификата (файл *.cer *.crt)
- Добавление в сервис наблюдения коллекции сертификатов (файл *.p7b)
- Загрузка набора сертификатов аккредитованных удостоверяющих центров системы квалифицированной электронной подписи Российской Федерации с сайта <http://e-trust.gosuslugi.ru/CA>
- Просмотр списков наблюдаемых сертификатов в хранилищах разных категорий сертификатов с основной информацией сертификата и графической индикацией статуса каждого сертификата
- Фильтрация вывода сертификатов при просмотре хранилищ
- Полно- и частично-текстовый регистронезависимый поиск по полям «Субъект» и «Издатель»
- По датам действия сертификатов
- По статусам сертификатов (действительный, недействительный, срок действия закрытого ключа истёк)
- Сортировка по срокам начала, окончания действия сертификата и окончания действия закрытого ключа
- Выгрузка (отфильтрованного) списка сертификатов в формате MS Excel (файл *.xlsx) для целей внешней обработки (отчеты, статистика)
- Выгрузка набора (отфильтрованных) файлов сертификатов в формате архива *.zip для целей внешней обработки
- Оставление комментариев для отдельных сертификатов
- Просмотр подробной информации о конкретном сертификате в отдельном окне с возможностью выгрузки его как файла, возможностью удаления из наблюдаемых и возможностью его перемещения в хранилище сертификатов, потерявших доверие
- Удаление из наблюдения сертификата или группы сертификатов, отмеченных чекбоксом

4.7.5. Элементы интерфейса

4.7.5.1. Основное окно

Интерфейс ЭОС PKI-сервиса структурирован как большинство современных веб-приложений и сайтов – основные «служебные» (настроечные или возвратные) ссылки расположены на верхней горизонтальной полосе (баре), и доступны в любой момент времени работы, а «функциональные» представлены «плиточным» интерфейсом, и меняются в зависимости о выполняемой задачи.

Верхний бар

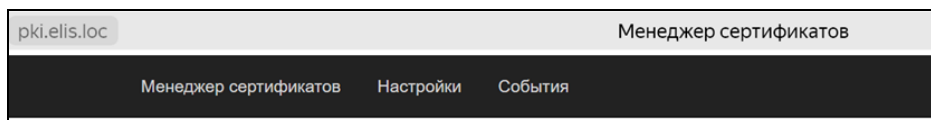


Рисунок 27

- «Менеджер сертификатов» – возврат на главную страницу сервиса
- «Настройки» - переход на страницу настроек
- «События» - переход на страницу доступа к журналам (логам) сервиса (события и ошибки)

Основной экран («главная» страница) ЭОС PKI-сервиса содержит следующие «плиточные» элементы управления (ссылки):

- «Хранилища сертификатов» – переход на страницу, где представлены хранилища сертификатов разных категорий
- «Статус» - переход на страницу **краткой совокупной информации** о статусе работы сервиса и наблюдаемых сертификатов относительно их срока действия
- «События» - переход на страницу доступа к журналам (логам) сервиса (события и ошибки), аналогично ссылке в верхнем баре

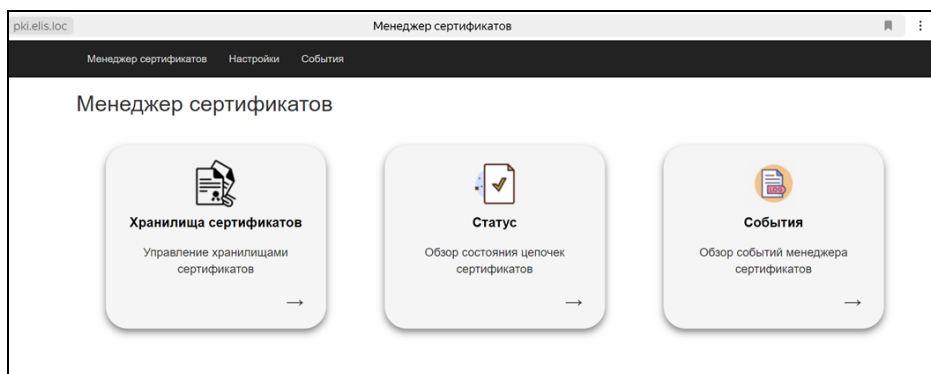


Рисунок 28

4.7.5.2. Страница «Настройки»

Показывает настройки, применяемые в данный момент ЭОС PKI-сервисом, а также содержит элементы, позволяющие такие настройки изменять.

Страница настройки содержит несколько панелей, относящихся к определённым группам настроек (**Общие настройки, Импорт корневых и промежуточных сертификатов, Proxu, Отправка e-mail уведомлений, Обновление статусов сертификатов, Проверка целостности хранилищ, Импорт сертификатов из подписей**).

Редактирование настроек заключается в перемещении ползунков чекбоксов, либо редактирования текстовых полей с последующим нажатием кнопки «Сохранить изменения конфигурации» внизу страницы настроек. При редактировании текстовых полей шрифт меняется на **жирный** и **возможно сохранить изменения** нажатием клавиши Enter.

Вверху страницы имеется ссылка на скачивание txt-файла с «белым» списком адресов в сети интернет для возможной настройки межсетевых экранов (точки распространения списков отзыва).

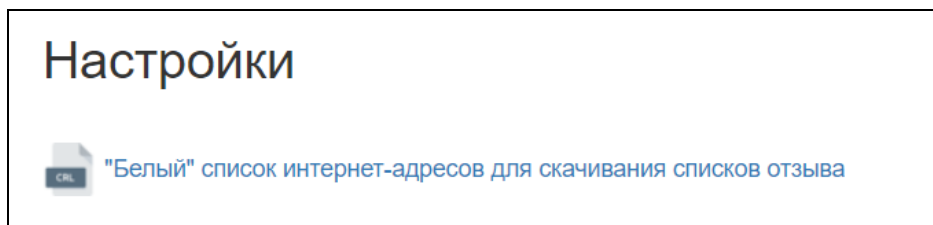


Рисунок 29

4.7.5.3. Панель «Общие настройки»

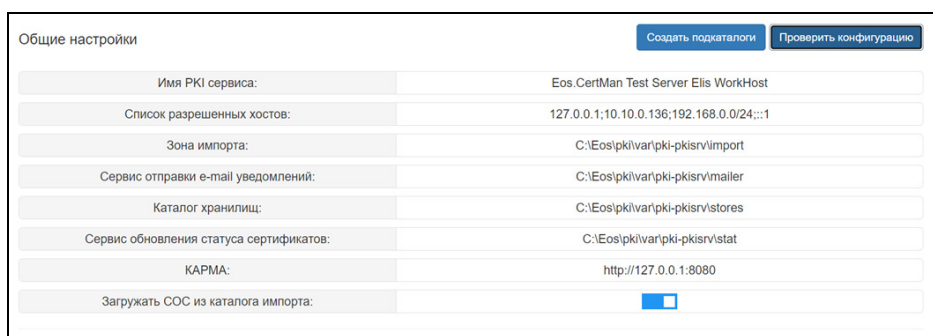


Рисунок 30

Содержит кнопки

- «Создать подкаталоги» - проверка и создание недостающих каталогов и подкаталогов. Все каталоги создаются во время установки. Кнопку необходимо использовать после изменения пути каталогов
- «Проверить конфигурацию» - контроль целостности структуры папок, используемых сервисом

Содержит соответствующие редактируемые поля (см. рисунок).

Стоит уделить внимание полю "Список разрешённых хостов". Поле может содержать IP адреса (например, "127.0.0.1;192.168.0.15") и/или маски подсетей (например, "192.168.0.0/24"), разделённые через ";". С помощью данной настройки определяется пул IP адресов, которым разрешён доступ к веб сайту PKI.

Запросы от внешних пользовательских "Карм" внесены в публичный лист запросов, т.е. беспрепятственно обрабатываются сервисом без настройки списка разрешённых хостов - с любого внешнего IP.

Содержит чекбокс «Загружать СОС из каталога импорта» (применяется при невозможности подключения к Интернет и ручном предоставлении списков отзыва сертификатов (*.crl) в папку (зону) импорта).

4.7.5.4. Панель «Импорт промежуточных и корневых сертификатов КЭП»

Содержит нормально **выключенный** чекбокс «Автономная работа» (применяется при невозможности подключения к Интернет и ручной загрузке сертификатов аккредитованных УЦ системы квалифицированной электронной подписи Российской Федерации).

Содержит настройку периодичности скачивания (в часах) сертификатов аккредитованных УЦ системы квалифицированной электронной подписи Российской Федерации

Импорт корневых и промежуточных сертификатов	
Автономная работа:	☒
До следующего импорта (ч):	24

Рисунок 31

4.7.5.5. Панель «Параметры проху»

Содержит соответствующие настройки для доступа сервиса к сети Интернет с использованием Proxu-сервера.

Параметры проху	
Проху:	☒
Хост:	194.87.111.108
Порт:	3128
Логин:	1231
Пароль:	****
Анонимная авторизация:	☐

Рисунок 32

4.7.5.6. Панель «Параметры отправки e-mail уведомлений»

Содержит настройки используемые для рассылок ЭОС PKI-сервисом e-mail уведомлений – учетной записи «автора» рассылок на SMTP-сервере и общих настраиваемых опций рассылок (см. рисунок), а так же настройки адресатов рассылок, включая фильтры по полям сертификатов, попадающих в рассылку для конкретного адреса. Подробнее о фильтрах рассылки в Приложении 4.

При отсутствии установленных правил **фильтра** рассылки для конкретного адреса, на этот адрес будут посылаться **все** уведомления от сервиса (например, администратору).

Также в дополнение к массовой рассылке, описанной выше, существует возможность доставки уведомлений об истечении срока действия сертификата и/или закрытого ключа владельцам сертификатов хранилища "Основные пользовательские" - опция "Отправлять уведомления владельцу истекающего сертификата".

Рассылка происходит раз в сутки, после 9-00 по времени сервера, с учетом настройки выходных\будних дней (опция "Отправлять уведомления только в будние дни"). Пример письма-оповещения и вложения к нему приведен в Приложении 3.

Письма-оповещения отправляются автоматически, по мере достижения сертификатами контрольных точек (по умолчанию 30 и 7 дней до истечения сертификата, либо по заданным в **днях** интервалах).

В тексте письма отображается минимальный срок окончания действия сертификатов или закрытого ключа, установленный в настройках.

С оповещением может приходить файл в формате MS Excel (файл *.xlsx).

В течение суток служба обновления статуса сертификатов добавляет те сертификаты, по которым нужна рассылка, в список соответствующего дня рассылки.

Панель так же содержит кнопку «**Отправить уведомления**», принудительно запускающую рассылку уведомлений (применяется только к сертификатам, попавшим в список после последней штатной ежедневной рассылки). Принудительно повторить **полную рассылку** за текущие сутки возможно по нажатию кнопки «Отправить e-mail уведомления» страницы «Статус»

Отправка e-mail уведомлений

Отправить уведомления

Отправка уведомлений:	☐
SMTP сервер:	10.10.1.112
Порт:	25
Использовать StartTLS:	☐
Логин:	pkitest@test.loc
Пароль:	*****
Анонимная авторизация:	☐
Рассылка уведомлений до конца действия сертификата (д):	7, 30, 600, 700
Рассылка уведомлений до конца действия закрытого ключа (д):	400
Отправлять уведомления только в будние дни:	☐
Отправлять уведомления владельцу истекающего сертификата:	☐

Почтовые адреса для отправки e-mail уведомлений:

Контактное лицо	Адрес	Фильтр атрибутов сертификата
Все оповещения	e.iodkovsky@eos.ru	Issuer.E="svyaz.ru, Subject.C=RU // Subject.O="Mo" ✖
Василий Иванов	Ivanov@mail.ru	Issuer.E="svyaz.ru, Subject.C=RU // Subject.O="Mo" ✖

Добавить Email

Рисунок 33

4.7.5.7. Панель «Обновление статусов сертификатов»

Содержит нормально **выключённый** чекбокс работы службы обновления статусов сертификатов (пересчёт и подтверждение цепочек доверия). Служба запускается один раз в час. Панель имеет кнопку «**Обновить статусы сертификатов**» для экстренного запуска службы (добавление сертификатов, перемещение в «недоверенные»). Если момент экстренного запуска попал на штатно выполняющийся процесс пересчёта, будет выведено сообщение об ошибке.

Позволяет сервису оперировать меньшим количеством только актуальных сертификатов.

Обновление статусов сертификатов

Обновить статусы сертификатов

Автообновление:	☒
Удалять истеющие сертификаты пользователей:	☐
Удалять истеющие сертификаты пользователей через ... (д):	60

4.7.5.8. Панель «Параметры проверки целостности хранилищ»

Служебный сервис, поддерживающий консистентность хранилища "Доверенные корневые центры сертификации". Обработывает 1 раз в сутки.

Содержит нормально **выключённый** чекбокс запуска\остановки сервиса проверки целостности и соответствующие настройки периода времени запуска.

Проверка целостности хранилищ		
Проверка целостности:	☒	
Время запуска:	03:00	⊙
Время остановки:	09:00	⊙

Рисунок 34

4.7.5.9. Панель «Импорт сертификатов из подписей»

Содержит кнопку запуска сервиса массового импорта сертификатов подготовленной информации, экспортированной в локальную папку из базы данных СЭД «ДЕЛО». Используется для первичного и/или инкрементного заполнения РКИ-сервиса.

Процедура экспорта из базы «ДЕЛО» и импорта в ЭОС РКИ-сервис описана в отдельной инструкции «ЭОС РКИ-сервис. Импорт сертификатов пользователей из базы данных СЭД «ДЕЛО»»

Содержит путь папки импорта.

Для корректной работы службы импорта в некоторых случаях потребуется выдать полные права на каталог с подписями для пользователя с именем <AppName>-pkisrv, где <AppName> - имя приложения, заданное в параметре при запуске скриптов инсталляции приложения

Импорт сертификатов из подписей		Запустить импорт
Удалять успешно обработанные подписи:	☒	
Путь до папки с подписями:	C:\PKIEXP	
Допустимое количество последовательных ошибок:	100	

Рисунок 35

4.7.6. Страница «Статус»

Краткая информации о всех наблюдаемых сертификатах относительно их срока истечения и сводная информация о количественных параметрах работы сервиса .

Содержит кнопку «**Отправить email уведомления**» - применяется для принудительной отправки e-mail обо ВСЕХ истекающих в заданные интервалы времени сертификатах.

Пример письма-оповещения и вложения к нему приведен в Приложении 3.

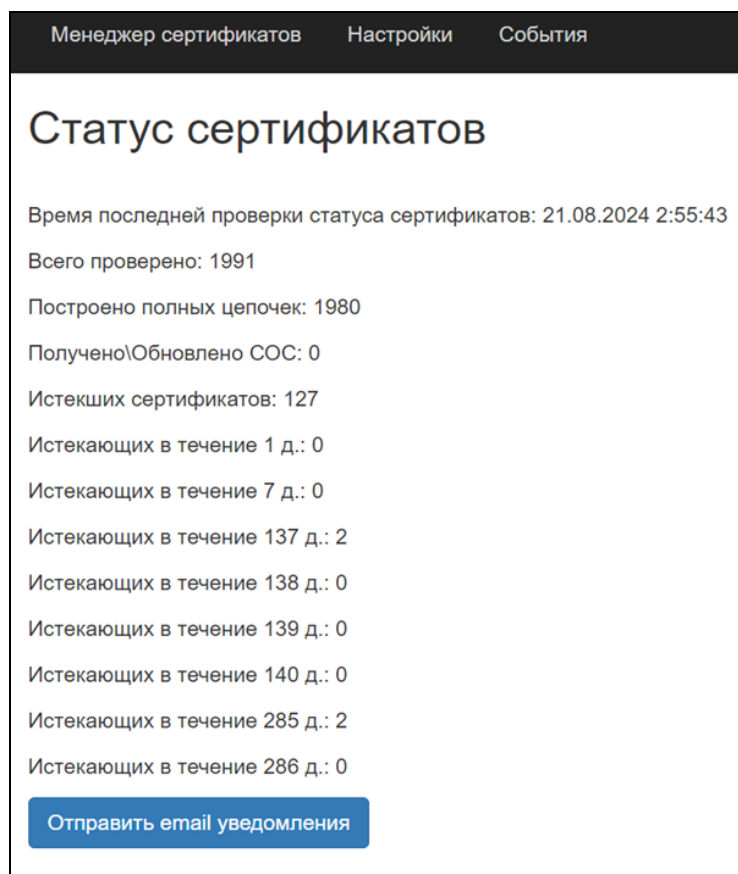


Рисунок 36

4.7.7. Страница «Хранилища сертификатов»

Представлены четыре категории наблюдаемых сертификатов (хранилища).

На «плитках» соответствующих хранилищ показано количество сертификатов, содержащихся в данном хранилище.

При наведении курсора мыши на «плитку» она становится активной, и, при нажатии, совершается переход в выбранное хранилище.

Для каждого хранилища доступны по соответствующим ссылкам в нижней части «плитки» операции добавления в данную категорию новых сертификатов.

Последовательность действий для **корректного** добавления сертификатов в наблюдаемые описана в пункте «Импорт сертификатов».

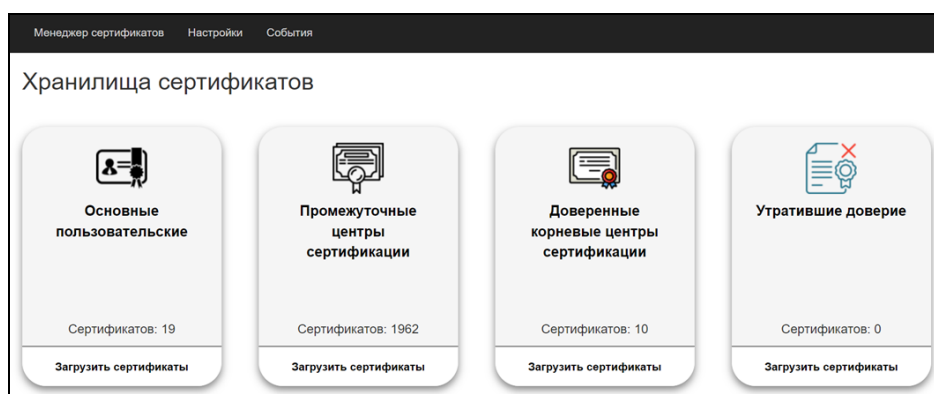


Рисунок 37

4.7.8. Страница просмотра списка сертификатов определенной категории

На странице представлены все сертификаты, помещенные для наблюдения в данную категорию, в виде списка. Список формируется по мере добавления сертификатов в сервис, наиболее позднегодобавленные – внизу списка.

Над списком размещена ссылка «Экспорт в Excel», позволяющая выгрузить в файл список сертификатов данной категории (возможно, предварительно отфильтрованный), и далее работать с ним, как с электронной таблицей.

Над списком размещена ссылка «Экспорт в Zip», позволяющая выгрузить в файл набор файлов сертификатов данной категории (возможно, предварительно отфильтрованный), и далее работать с ним, как с набором файлов сертификатов.

Непосредственно над списком, в правой части, расположены кнопка «Удалить», по-умолчанию не активная, и чекбокс, позволяющий отметить все сертификаты, в данный момент выводимые в списке (с учётом применённых фильтров). Все такие отмеченные сертификаты можно удалить нажатием кнопки «Удалить».

Для каждого сертификата выводятся:

- номер в выводимом списке
- значок инфографики, соответствующий статусу сертификата
- полная информация, содержащаяся в полях «Субъект» и «Издатель»
- Поле для работы с комментариями
- даты действия сертификата и закрытого ключа (при наличии)
- ссылка «Просмотр» для вывода информации о конкретном сертификате в отдельном (всплывающем) окне.
- чекбокс, позволяющий отметить сертификат для удаления

Промежуточные центры сертификации

Экспорт текущего списка в Excel

Экспорт текущего списка в Zip

Фильтрация сертификатов

Фильтр по субъекту

С:

dd.mm.yyyy

По:

dd.mm.yyyy

Фильтр по издателю

Фильтр по статусу: Все

Применить фильтр

Сбросить фильтр

№	i	Субъект	Издатель	Комментарий	С	По	Ключ до	Удалить	
1		sa@domint.ru, 1047796861703, 007225524960, RU, 77 г. Москва, г. Москва, 1-ый Нагатинский проезд д. 10 стр. 1, Удостоверяющий центр АО "Промышленные инновации", УЦАО "Промышленные инновации"	007710474375, 1047702026701, dn@mnvnuas.ru, 125375 г. Москва ул. Тверская д. 7, Минкомсвязь России, Москва, 77 г. Москва, RU, YU 1 ИС ГЦУ	Тестовый коммент	29.09.2016	29.09.2026		Просмотр	☐
2		uc@domint.ru, 1073867027774, 003664083641, RU, 36 Воронежская область, Воронеж, пл.им.Ленина д. 1, Удостоверяющий центр, Департамент связи и массовых коммуникаций Воронежской области, УЦ правительства Воронежской области	007710474375, 1047702026701, dn@mnvnuas.ru, 125375 г. Москва ул. Тверская д. 7, Минкомсвязь России, Москва, 77 г. Москва, RU, YU 1 ИС ГЦУ		12.01.2017	07.12.2026	12.01.2027	Просмотр	☐
3		1067746185195, 007841016636, sa@48.center-infom.ru, RU, 48 Ленинградская область, г. Петлики, ФГУП ЦентриИнформ, ПдФ ФГУП ЦентриИнформ, Center-Infom LLC, Удская ул., д. 15	007710474375, 1047702026701, dn@mnvnuas.ru, 125375 г. Москва ул. Тверская д. 7, Минкомсвязь России, Москва, 77 г. Москва, RU, YU 1 ИС ГЦУ		24.11.2016	24.11.2026		Просмотр	☐
4		1067746185195, 007841016636, Галактика проспект д.28, sa@52.center-infom.ru, RU, 52 Нижегородская область, с. Нижний Новгород, ФГУП ЦентриИнформ, ИФ ФГУП ЦентриИнформ, Center-Infom NI	007710474375, 1047702026701, dn@mnvnuas.ru, 125375 г. Москва ул. Тверская д. 7, Минкомсвязь России, Москва, 77 г. Москва, RU, YU 1 ИС ГЦУ		13.07.2016	13.07.2026		Просмотр	☐
5		1067746185195, 007841016636, Красная набережная ул. д.37, sa@30.center-infom.ru, RU, 30 Астраханская область, г. Астрахань, ФГУП ЦентриИнформ, АстраФ ФГУП ЦентриИнформ, Center-Infom AstF	007710474375, 1047702026701, dn@mnvnuas.ru, 125375 г. Москва ул. Тверская д. 7, Минкомсвязь России, Москва, 77 г. Москва, RU, YU 1 ИС ГЦУ		24.11.2016	24.11.2026		Просмотр	☐
6		1067746185195, 007841016636, Пенная ул., д. 85, sa@43.center-infom.ru, RU, 43 Карачаево-Черкесская область, г. Карачаевск, ФГУП ЦентриИнформ, КраФ ФГУП ЦентриИнформ, Center-Infom KrfF	007710474375, 1047702026701, dn@mnvnuas.ru, 125375 г. Москва ул. Тверская д. 7, Минкомсвязь России, Москва, 77 г. Москва, RU, YU 1 ИС ГЦУ		24.11.2016	24.11.2026		Просмотр	☐
7		1067746185195, 007841016636, Серебрянниковская ул., д. 14, sa@54.center-infom.ru, RU, 54 Новосибирская область, г. Новосибирск, ФГУП ЦентриИнформ, НосФ ФГУП ЦентриИнформ, Center-Infom NsfF	007710474375, 1047702026701, dn@mnvnuas.ru, 125375 г. Москва ул. Тверская д. 7, Минкомсвязь России, Москва, 77 г. Москва, RU, YU 1 ИС ГЦУ		13.07.2016	13.07.2026		Просмотр	☐
8		1067746185195, 007841016636, Садовая ул., д.24а, sa@62.center-	007710474375, 1047702026701, dn@mnvnuas.ru, 125375 г. Москва ул.						☐

Рисунок 38

Во всплывающем окне индивидуального просмотра информации сертификата имеются кнопки:

- «Удалить» - для ручного удаления сертификата из наблюдения ЭОС РКІ-сервисом

- «Переместить в «Утратившие доверие»» - для оперативного\аварийного «блокирования» доверия к конкретному сертификату
- «Скачать» - для скачивания файла сертификата
- «Сохранить» - выход из окна просмотра конкретного сертификата

А также поле для написания комментария

Рисунок 39

Также сверху страницы расположена область «Фильтрация сертификатов», позволяющая из всего списка сертификатов данной категории выбрать определенные сертификаты, отвечающие запрашиваемым критериям.

Рисунок 40

Возможности фильтрации вывода сертификатов при просмотре хранилищ:

- Полно- и частично-текстовый регистронезависимый поиск по полям «Субъект» и «Издатель»
- По датам действия сертификатов
- По статусам сертификатов (действителен, недействителен, срок действия ключа истёк)

При наведении курсора на поля текстового поиска показываются всплывающие подсказки с примерами. Может быть применено несколько текстовых строк, через запятую (,).

Фильтры применяются одновременно, и в выборку попадают сертификаты, только удовлетворяющие **всем критериям** фильтрации при этом показывается, сколько сертификатов подпадает под критерии из всего количества :

Промежуточные центры сертификации

Экспорт текущего списка в Excel

Экспорт текущего списка в Zip

Москва, Варшавское шоссе

С:

дд.мм.гггг

По:

дд.мм.гггг

Фильтр по издателю

Фильтр по статусу:

Все

Применить фильтр

Сбросить фильтр

Показано сертификатов: 9 из 1800

№	i	Субъект	Издатель	Комментарий	С	По	Ключ до	Удалить	
1	<div></div>	1097746195195, 007841019536, Варшавское шоссе д.37А,стр.8, саф@77-center-inform.ru, RU, 77 г. Москва, Г. Москва, ФГУП ЦентрИнформ, МосФ-ФГУП ЦентрИнформ, Center-Infom Mail	007710474375, 1047702026701, dn@minvuz.ru, 125375 г. Москва ул. Тверская д.7, Минюсвзя России, Москва, 77 г. Москва, RU, УЦ 1 ИС ГУЦ		13.07.2018	13.07.2026		Просмотр	<div></div>
2	<div></div>	1097746195195, 007841019536, Варшавское шоссе д.37А,стр.8, саф@77-center-inform.ru, RU, 77 г. Москва, Г. Москва, ФГУП ЦентрИнформ, МосФ-ФГУП ЦентрИнформ, Center-Infom Mail	007710474375, 1047702026701, dn@minvuz.ru, 125375 г. Москва ул. Тверская д.7, Минюсвзя России, Москва, 77 г. Москва, RU, УЦ 1 ИС ГУЦ		24.11.2016	24.11.2026		Просмотр	<div></div>
3	<div></div>	1157746658431, Варшавское шоссе, дом 1, строение 1-2, комната 3К, 007726346925, RU, Москва, 77 г. Москва, uc@netus.ru, Общество с ограниченной ответственностью «Генеральный Удостоверяющий Центр»	007710474375, 1047702026701, dn@minvuz.ru, 125375 г. Москва ул. Тверская д.7, Минюсвзя России, Москва, 77 г. Москва, RU, УЦ 1 ИС ГУЦ		02.12.2018	02.12.2026		Просмотр	<div></div>
4	<div></div>	1157746658431, Варшавское шоссе, дом 1, строение 1-2, комната 3К, 007726346925, RU, Москва, 77 г. Москва, uc@netus.ru, ООО «ГУЦ», Удостоверяющий центр, ООО «ГУЦ»	dn@minvuz.ru, RU, 77 Москва, г. Москва, улица Тверская, дом 7, Минюсвзя России, 1047702026701, 007710474375, Минюсвзя России		31.07.2018	31.07.2033		Просмотр	<div></div>
5	<div></div>	ООО «ГУЦ», ООО «ГУЦ», Удостоверяющий центр, RU, 77 г. Москва, Москва, uc@netus.ru, Варшавское шоссе, дом 1, строение 1-2, подвал комната 3К, 007726346925, 1157746658431	dn@minvuz.ru, RU, 77 Москва, г. Москва, улица Тверская, дом 7, Минюсвзя России, 1047702026701, 007710474375, Минюсвзя России		08.10.2019	08.10.2034		Просмотр	<div></div>
6	<div></div>	1157746658431, Варшавское шоссе, дом 1, строение 1-2, комната 3К, 007726346925, RU, Москва, 77 г. Москва, uc@netus.ru, Общество с ограниченной ответственностью «Генеральный Удостоверяющий Центр», Удостоверяющий центр, Общество с ограниченной ответственностью «Генеральный Удостоверяющий Центр»	dn@minvuz.ru, RU, 77 г. Москва, Москва, 125375 г. Москва, ул. Тверская, д. 7, Минюсвзя России, 1047702026701, 007710474375, Головной удостоверяющий центр		12.01.2018	12.01.2027		Просмотр	<div></div>
1157746658431, Варшавское шоссе, дом 1, строение 1-2, комната 3К, 007726346925, RU, Москва, 77 г. Москва, uc@netus.ru, Общество с ограниченной ответственностью «Генеральный Удостоверяющий Центр», Удостоверяющий центр, Общество с ограниченной ответственностью «Генеральный Удостоверяющий Центр»									
dn@minvuz.ru, RU, 77 г. Москва, Москва, 125375 г. Москва, ул. Тверская, д. 7, Минюсвзя России, 1047702026701, 007710474375, Головной удостоверяющий центр									

Рисунок 41

Промежуточные центры сертификации

Экспорт текущего списка в Excel

Экспорт текущего списка в Zip

Москва, Варшавское шоссе

С:

дд.мм.гггг

По:

дд.мм.гггг

Фильтр по издателю

Фильтр по статусу:

Действительные

Применить фильтр

Сбросить фильтр

Показано сертификатов: 3 из 1800

№	i	Субъект	Издатель	Комментарий	С	По	Ключ до	Удалить	
1	<div></div>	1157746658431, Варшавское шоссе, дом 1, строение 1-2, комната 3К, 007726346925, RU, Москва, 77 г. Москва, uc@netus.ru, ООО «ГУЦ», Удостоверяющий центр, ООО «ГУЦ»	dn@minvuz.ru, RU, 77 Москва, г. Москва, улица Тверская, дом 7, Минюсвзя России, 1047702026701, 007710474375, Минюсвзя России		31.07.2018	31.07.2033		Просмотр	<div></div>
2	<div></div>	ООО «ГУЦ», ООО «ГУЦ», Удостоверяющий центр, RU, 77 г. Москва, Москва, uc@netus.ru, Варшавское шоссе, дом 1, строение 1-2, подвал комната 3К, 007726346925, 1157746658431	dn@minvuz.ru, RU, 77 Москва, г. Москва, улица Тверская, дом 7, Минюсвзя России, 1047702026701, 007710474375, Минюсвзя России		08.10.2019	08.10.2034		Просмотр	<div></div>
3	<div></div>	RU, 77 г.Москва, Москва, Варшавское шоссе, дом 37, ФГУП «Почта России», Удостоверяющий центр, ФГУП «Почта России», 1037724007276, 007724261610	dn@minvuz.ru, RU, 77 Москва, г. Москва, улица Тверская, дом 7, Минюсвзя России, 1047702026701, 007710474375, Минюсвзя России		17.01.2019	17.01.2034	11.04.2020	Просмотр	<div></div>

Рисунок 42

Промежуточные центры сертификации

Экспорт текущего списка в Excel

Экспорт текущего списка в Zip

Москва

С:

дд.мм.гггг

По:

31.07.2033

Фильтр по издателю

Фильтр по статусу:

Действительные

Применить фильтр

Сбросить фильтр

Показано сертификатов: 30 из 1800

№	i	Субъект	Издатель	Комментарий	С	По	Ключ до	Удалить	
1	<div></div>	1157746658431, Варшавское шоссе, дом 1, строение 1-2, комната 3К, 007726346925, RU, Москва, 77 г. Москва, uc@netus.ru, ООО «ГУЦ», Удостоверяющий центр, ООО «ГУЦ»	dn@minvuz.ru, RU, 77 Москва, г. Москва, улица Тверская, дом 7, Минюсвзя России, 1047702026701, 007710474375, Минюсвзя России		31.07.2018	31.07.2033		Просмотр	<div></div>
2	<div></div>	5087746025373, 007702062879, RU, 77 Москва, г. Москва, Рождественский бульвар, дом 12/8 корпус 1, Удостоверяющий центр, ФГБУ ЦСМС, ФГБУ ЦСМС	dn@minvuz.ru, RU, 77 Москва, г. Москва, улица Тверская, дом 7, Минюсвзя России, 1047702026701, 007710474375, Минюсвзя России		27.07.2018	27.07.2033		Просмотр	<div></div>
3	<div></div>	1027739393175, 007704035764, RU, 77 Москва, Москва, ул. Итальяная, д.1, ОПИТ, ФГУП "РОСТЭК", ФГУП "РОСТЭК"	dn@minvuz.ru, RU, 77 Москва, г. Москва, улица Тверская, дом 7, Минюсвзя России, 1047702026701, 007710474375, Минюсвзя России		24.07.2018	24.07.2033		Просмотр	<div></div>
4	<div></div>	1097746293886, 007729633131, RU, 77 г.Москва, Москва, Ленинские горы, д.1, стр.77, Удостоверяющий центр, Общество с ограниченной ответственностью "Энергетический экспресс", ООО "Энергетический экспресс"	dn@minvuz.ru, RU, 77 Москва, г. Москва, улица Тверская, дом 7, Минюсвзя России, 1047702026701, 007710474375, Минюсвзя России		20.07.2018	20.07.2033		Просмотр	<div></div>
5	<div></div>	qsa@surto.ru, 103770008544, 007711107991, RU, 77 Москва, г. Москва, ул. Сущевский вал, д. 18, ООО "КРИПТО-ПРО", ООО "КРИПТО-ПРО"	dn@minvuz.ru, RU, 77 Москва, г. Москва, улица Тверская, дом 7, Минюсвзя России, 1047702026701, 007710474375, Минюсвзя России		27.07.2018	27.07.2033		Просмотр	<div></div>
6	<div></div>	ул. Шаболова 4, 102770022924, 007705016118, RU, Москва, 77 г.Москва, uc@f100.ru, Государственное учреждение - Пенсионный фонд Российской Федерации, ПФР	dn@minvuz.ru, RU, 77 Москва, г. Москва, улица Тверская, дом 7, Минюсвзя России, 1047702026701, 007710474375, Минюсвзя России		27.07.2018	27.07.2033		Просмотр	<div></div>
7	<div></div>	brsa@phlo.ru, 1027739154343, 007730036073, RU, 77 Москва, Москва, Бережковская набережная д. 30 к.1, Федеральный институт промышленной собственности, Федеральный институт промышленной собственности	dn@minvuz.ru, RU, 77 Москва, г. Москва, улица Тверская, дом 7, Минюсвзя России, 1047702026701, 007710474375, Минюсвзя России		27.07.2018	27.07.2033		Просмотр	<div></div>

Рисунок 43

В шапке таблицы расположены кнопки для сортировки таких столбцов как: "С", "По", "Ключ до"

Промежуточные центры сертификации

Экспорт текущего списка в Excel
 Экспорт текущего списка в Zip

Фильтрация сертификатов

Фильтр по субъекту: С: По:
 Фильтр по издателю: Фильтр по статусу:

№	I	Субъект	Издатель	Комментарий	С	По	Ключ до	Удалить	
1		sa@promtp.ru, 1047796861793, 007725524960, RU, 77 г. Москва, т. Москва, 1-ый Нагатинский проезд д. 10 стр. 1, Удостоверяющий центр АО "Промышленные инновации", УЦ АО "Промышленные инновации"	007710474375, 1047702026701, dn@promtp.ru, 125375 г. Москва ул. Тверская д. 7, Минкомсвязь России, Москва, 77 г. Москва, RU, УЦ 1 ИС ГУЦ	Тестовый коммент	29.09.2016	29.09.2026		<input type="button" value="Просмотр"/>	☐
2		uc@promtp.ru, 1073987027774, 003694083641, RU, 36 Воронежская область, Воронеж, пл. им. Ленина д. 1, Удостоверяющий центр, Департамент связи и массовых коммуникаций Воронежской области, УЦ правительства Воронежской области	007710474375, 1047702026701, dn@promtp.ru, 125375 г. Москва ул. Тверская д. 7, Минкомсвязь России, Москва, 77 г. Москва, RU, УЦ 1 ИС ГУЦ		12.01.2017	07.12.2026	12.01.2027	<input type="button" value="Просмотр"/>	☐

Рисунок 44

- Первое нажатие активирует сортировку по возрастанию
- Второе активирует сортировку по убыванию
- Третье деактивирует сортировку

При активации сортировки столбца "Ключ до" сначала отображаются все сертификаты с наличием информации о действии закрытого ключа

Одновременно действует только **одна** сортировка, после активации сортировки другого столбца - старая сортировка деактивируется

4.8. Стандартные операции в ЭОС PKI-сервис

4.8.1. Добавление сертификатов для наблюдения ЭОС PKI-сервисом

4.8.1.1. Автоматический импорт сертификатов Аккредитованных УЦ РФ (КЭП)

Откройте категорию «Промежуточные Центры Сертификации» (нажмите ссылку «Загрузить сертификаты»)

В верхней части имеется ссылка «Загрузить список "e-trust.gosuslugi.ru/CA"», при нажатии на которую будут загружены все актуальные сертификаты всех Аккредитованных Удостоверяющих Центров Российской Федерации.

Внимание! Операция может занимать продолжительное время (до пяти минут)

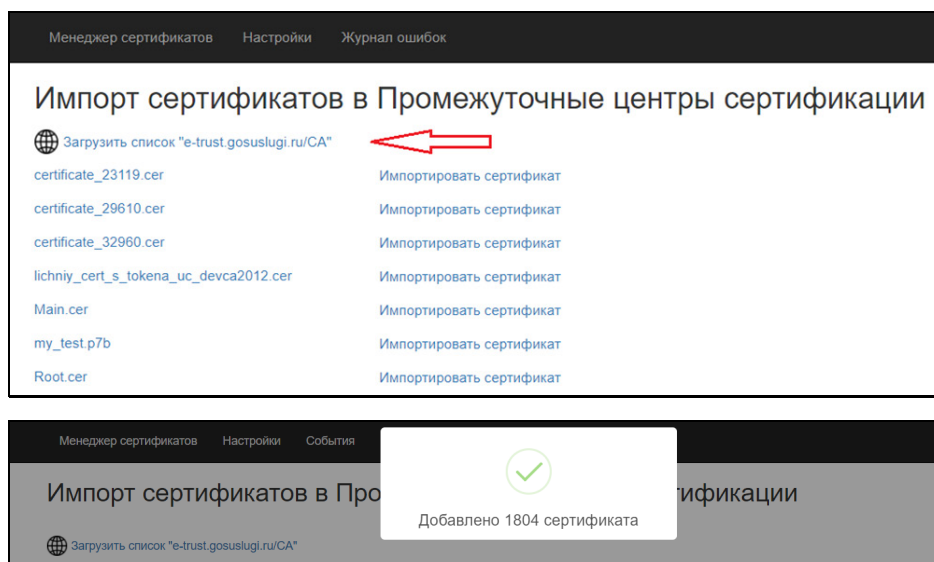


Рисунок 45

4.8.1.2. Файловый импорт

4.8.1.2.1. Добавление одиночного сертификата

Замечание об уникальности: ЭОС PKI-сервис не хранит идентичных сертификатов (копий). При попытке добавления уже существующего сертификата будет отказано.

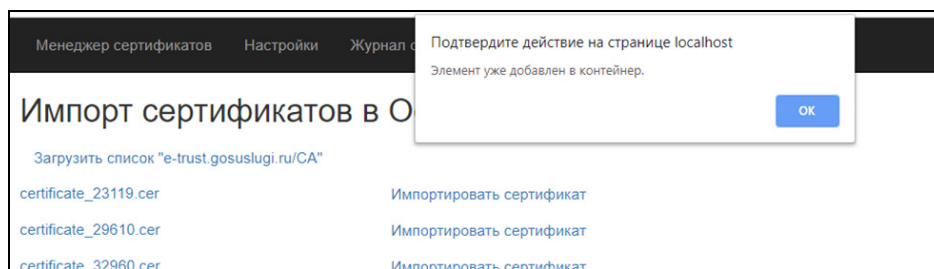


Рисунок 46

Сертификаты для наблюдения в ЭОС PKI-сервис добавляются в два этапа:

- Файлы одиночных сертификатов (*.cer;*.crt) должны быть предварительно записаны в папку импорта сервиса, созданную при установке сервиса и отображаемую как «Зона импорта» в общих настройках - **C:\Eos\pki\var\pki-pkisrv\import** (пример)
- В интерфейсе сервиса, на странице списка категорий (хранилищ) сертификатов, нужно нажать ссылку **«Загрузить сертификаты»** в нижней части «плитки» **соответствующего** хранилища.

Откроется страница импорта, где будут представлены файлы сертификатов, ранее помещенные в папку импорта:

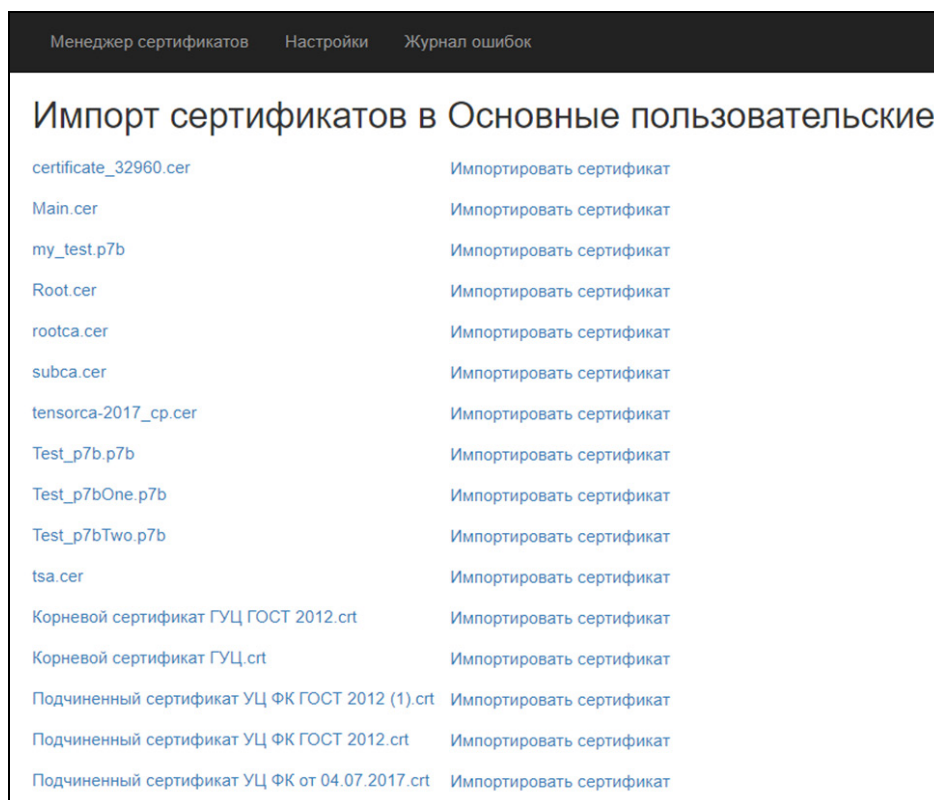


Рисунок 47

При нажатии на ссылку «Импортировать сертификат» напротив соответствующего файла сертификата произойдет добавление сертификата в наблюдаемые ЭОС PKI-сервисом. При этом имя файла импортированного сертификата пропадет из списка на данной странице, а сам файл будет перемещен из папки импорта

C:\Eos\pki\var\pki-pkisrv\import в папку импортированных файлов сертификатов **C:\EOS\pki\var\pki-pkisrv\import_imported**

4.8.1.2.2. Операция импорта корневого сертификата (ограничения и ответственность)

Добавление сертификата **корневого удостоверяющего центра** – особая ситуация, соответствие сертификата данной категории будет проверено, и, при несоответствии, будет отказано в добавлении в наблюдаемые с выводом соответствующего диалогового окна:

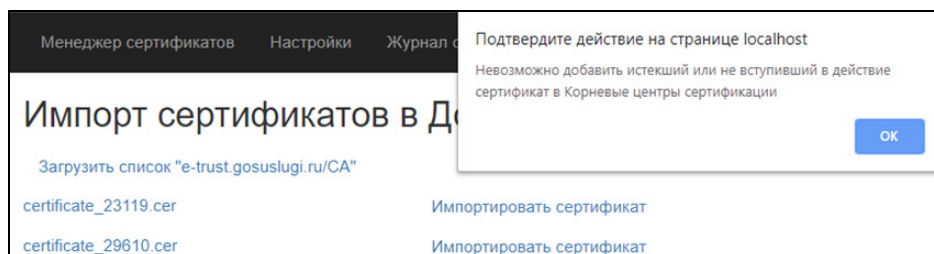


Рисунок 48

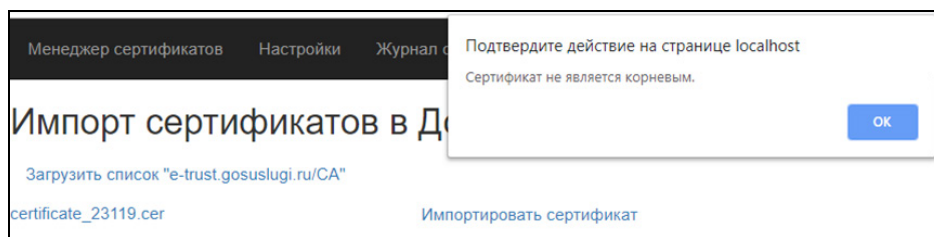


Рисунок 49

4.8.1.2.3. Файлы, содержащие коллекцию сертификатов (.p7b)

Замечание об уникальности.

ЭОС PKI-сервис не хранит идентичных сертификатов (копий). При добавлении сертификатов в наблюдаемые ЭОС PKI-сервисом посредством импорта из файла формата *.p7b, будут добавлены только те сертификаты, которые на данный момент не находятся на наблюдении. Так же не будут импортированы сертификаты корневых удостоверяющих центров, присутствующие в таком файле.

Импорт коллекции сертификатов происходит аналогично импорту одиночного сертификата. Сначала поместите файл *.p7b в папку импорта - **C:\Eos\pki\var\pki-pkisrv\import**, затем из интерфейса выберите соответствующую категорию сертификатов, и далее, на странице импорта, выберите соответствующий файл *.p7b.

В Приложении 1 приведена инструкция по **созданию** файлов *.p7b для массового экспорта-импорта сертификатов.

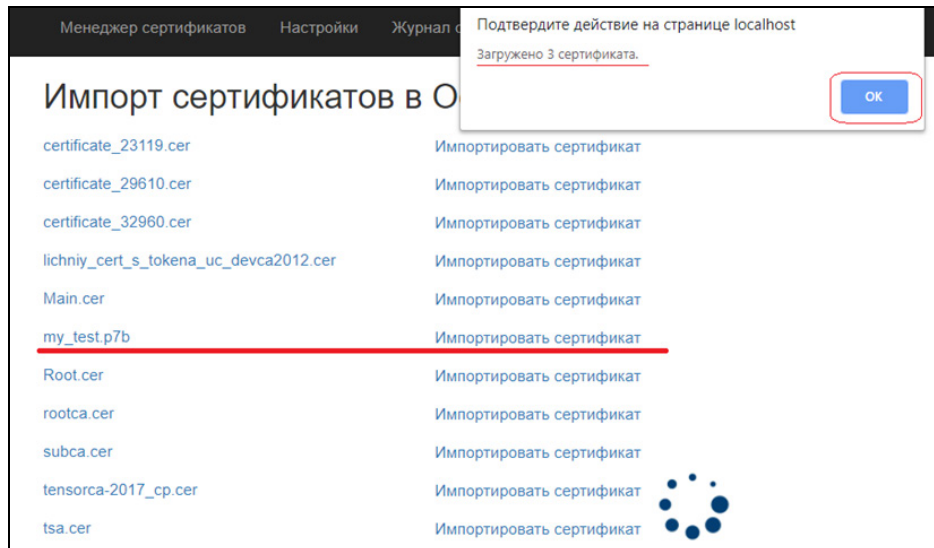


Рисунок 50

4.8.1.2.4. Массовый импорт из базы данных СЭД «ДЕЛО»

Процедура импорта описана в отдельной инструкции «ЭОС PKI-сервис. Импорт сертификатов пользователей из базы данных СЭД «ДЕЛО»»

4.8.1.2.5. Импорт сертификатов с помощью ПО КАРМА

СПО KARMA версии 56.2.436 и выше, установленное на компьютеры организации, при настройке СПО KARMA на использование PKI-сервиса, само отправляет сертификат в PKI-сервис, при **первом использовании данного сертификата для подписания документа**.

Критерием принятия такого сертификата в наблюдаемые PKI-сервисом является успешность «сборки» цепочки доверия для данного сертификата (имеются корневые и промежуточные сертификаты и списки отзыва к ним).

Принятые таким образом в наблюдение сертификаты помещаются в хранилище «Основные пользовательские».

Настройка ПО KARMA для использования совместно с PKI-сервисом описана в Приложении 2.

4.8.1.3. Исключение сертификатов из наблюдения

4.8.1.3.1. Автоматическое по сроку истечения хранения

При включении соответствующего чекбокса на странице «Настройки» и задании интервала хранения после истечения срока действия сертификата.

Относится только к хранилищу «Основные пользовательские»

4.8.1.3.2. Ручное

Для ручного исключения конкретного сертификата из списка наблюдаемых откройте окно подробного просмотра информации о сертификате и нажмите кнопку «Удалить».

Информация о сертификате

Серийный номер:	00ACC7306400000000009C
Субъект:	OGRN=1147606005447, INN=007606095476, C=RU, ST=76 Ярославская область, L=Ярославль, STREET="ул. Победы, д. 16 Б", O="ГБУ ЯО ""Электронный регион""", CN="ГБУ ЯО ""Электронный регион"""
Издатель:	E=dit@minsvyaz.ru, C=RU, ST=77 Москва, L=г. Москва, STREET="улица Тверская, дом 7", O=Минкомсвязь России, OGRN=1047702026701, INN=007710474375, CN=Минкомсвязь России
Комментарий:	<input type="text"/>
Действителен с:	03.08.2018 10:20:36
Действителен по:	03.08.2033 10:20:36
Статус:	Действителен

↓

Удалить Переместить в "Утратившие доверие" Скачать Сохранить

Рисунок 51

4.8.1.3.3. Ручное массовое

Для удаления нескольких сертификатов из списка хранилища отметьте чекбоксы, соответствующих сертификатов и нажмите кнопку «Удалить» в шапке страницы.

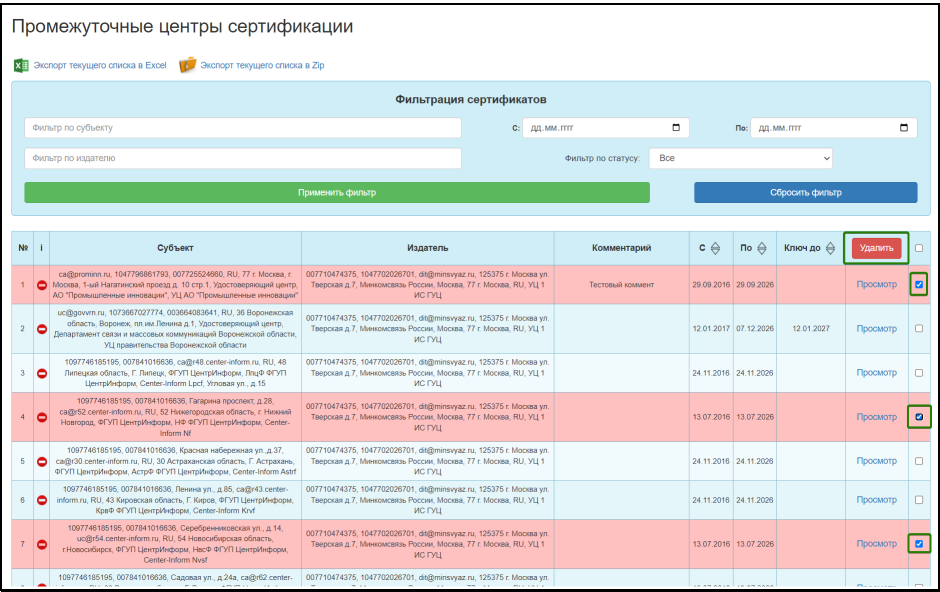


Рисунок 52

Так же возможна массовая установка чекбоксов для удаления, нажатием «общего» чекбокса. Данную опцию рекомендуется использовать, предварительно отфильтровав список сертификатов по какому-либо критерию (например, истёкшие на определенную дату).

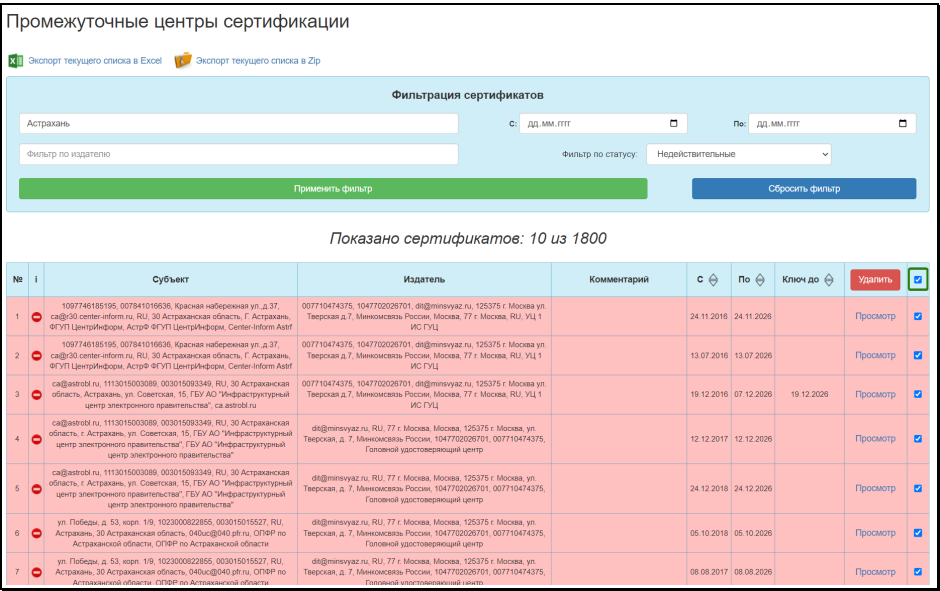


Рисунок 53

4.9. Приложение 1

4.9.1. Процесс массового экспорта сертификатов из хранилищ Windows (в файл *.p7b)

Данную операцию экспорта возможно провести на каждом АРМ организации, где используется функциональность ЭП. Однако, если имеются компьютеры\серверы, где, по устоявшейся практике, держат коллекцию сертификатов организации и\или контрагентов, то следует проводить экспорт именно на таких компьютерах. Такими «точками сосредоточения сертификатов» могут быть:

- АРМ человека, ответственного в организации за работу с сертификатами
- АРМ Технолога системы ДЕЛО
- Сервер Удаленной Проверки системы ДЕЛО
- Веб-сервер системы ДЕЛО
- Сервер приложений системы ДЕЛО
- Выделенный сервер хранения сертификатов

В примере показан экспорт из хранилища «Личное» **текущего пользователя**. Если подлежащее экспорту хранилище относится к Локальному компьютеру, или другому сетевому компьютеру, используйте оснастку «Сертификаты», ассоциированное с таким хранилищем.

Запустите оснастку управления компьютера, набрав «mmc.exe» в командной строке или строке поиска.

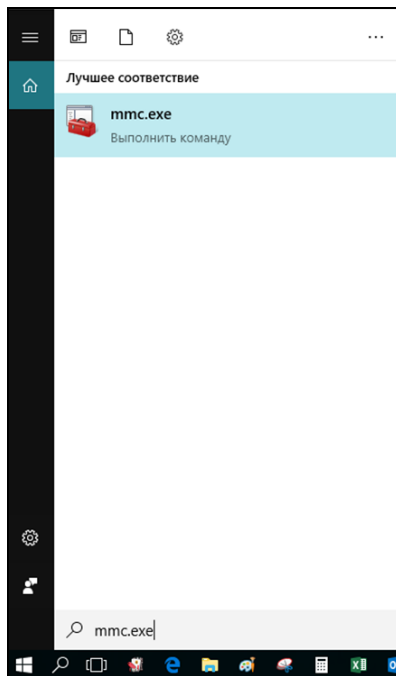


Рисунок 54

Добавьте оснастку «управление сертификатами»: «Файл» → Добавить или удалить оснастку → «Сертификаты» → «моей учетной записью пользователя» → Готово → ОК.

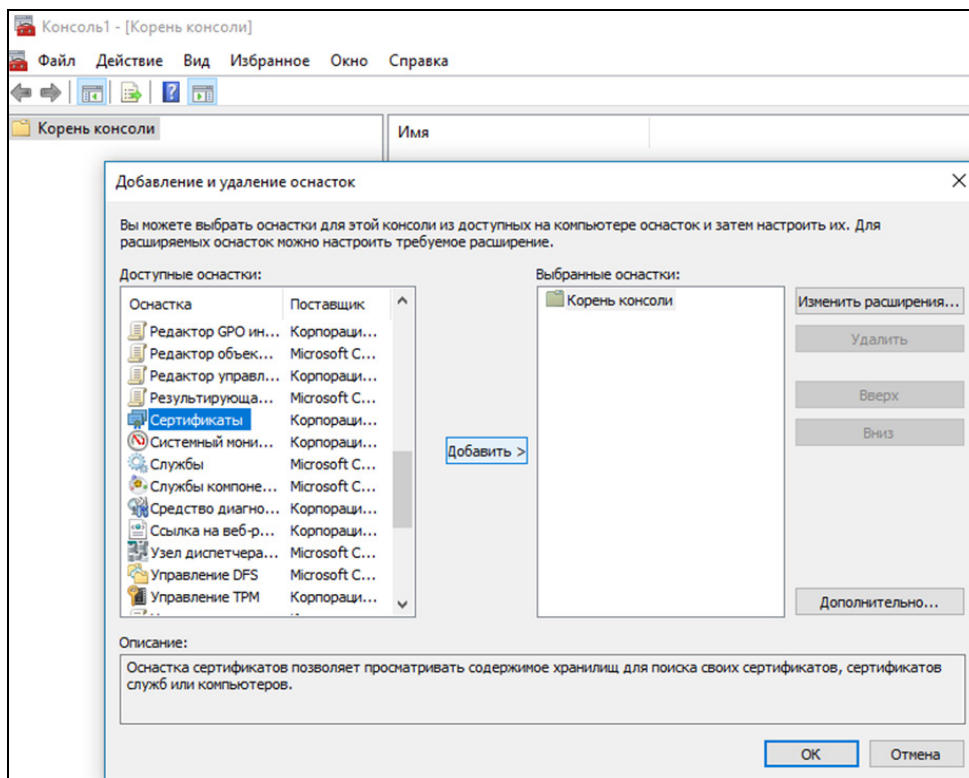


Рисунок 55

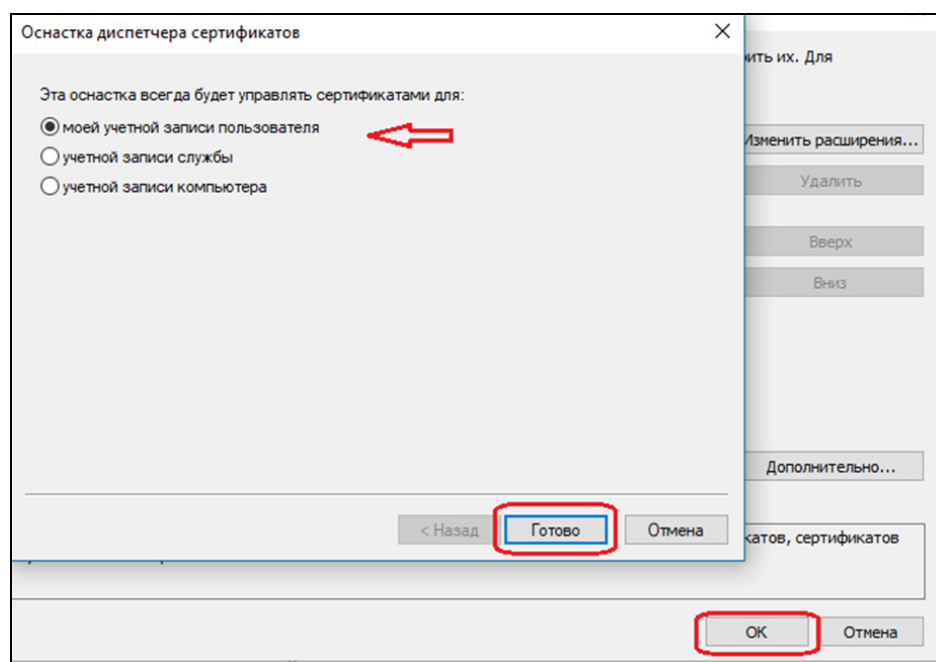


Рисунок 56

Откройте в оснастке Личное→ Сертификаты. Перед вами список сертификатов, «установленных» для данного пользователя.

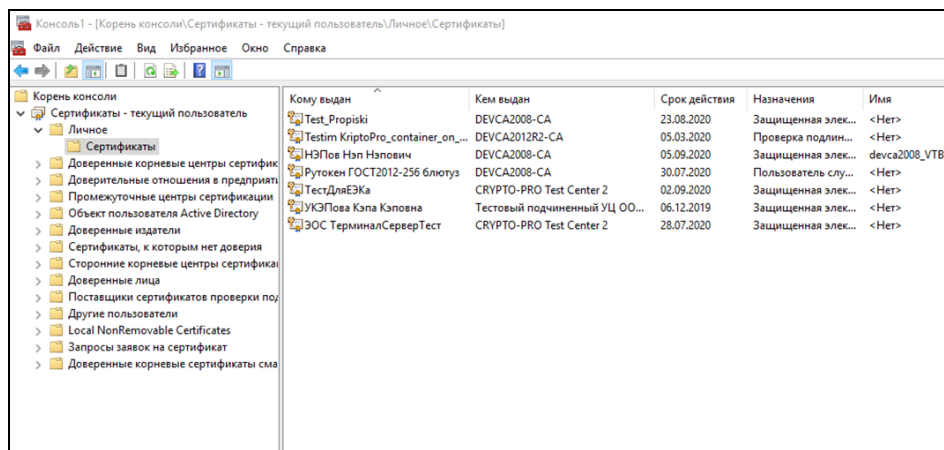


Рисунок 57

Сертификаты в данном представлении отсортированы по алфавиту. Для удобства сертификаты можно отсортировать по дате окончания срока действия, чтобы не добавлять в коллекцию сертификаты, потерявшие актуальность.

Не добавляйте в одну операцию экспорта сертификаты разных категорий (Пользовательские, промежуточных УЦ)

Выделите сертификаты, подлежащие экспорту (приемы выделения аналогичны применяемым в Проводнике Windows).

Кликом правой клавиши мыши на выделенном откройте меню экспорта:

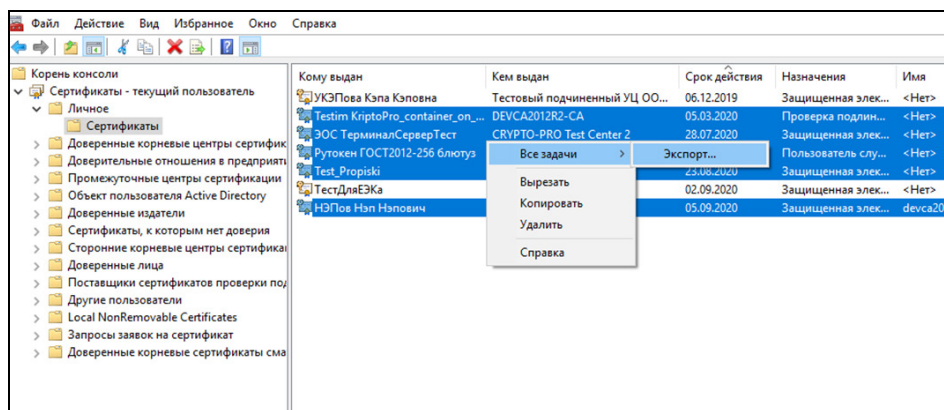


Рисунок 58

Если какие-то сертификаты использовались на данном компьютере для подписания (была организована связь с закрытым ключом, соответствующем открытому из данного сертификата), то, возможно, будут показаны диалоги доступа криптопровайдера к ключевому носителю.

Игнорируйте все такие диалоги, нажимая в них «Отмена»:

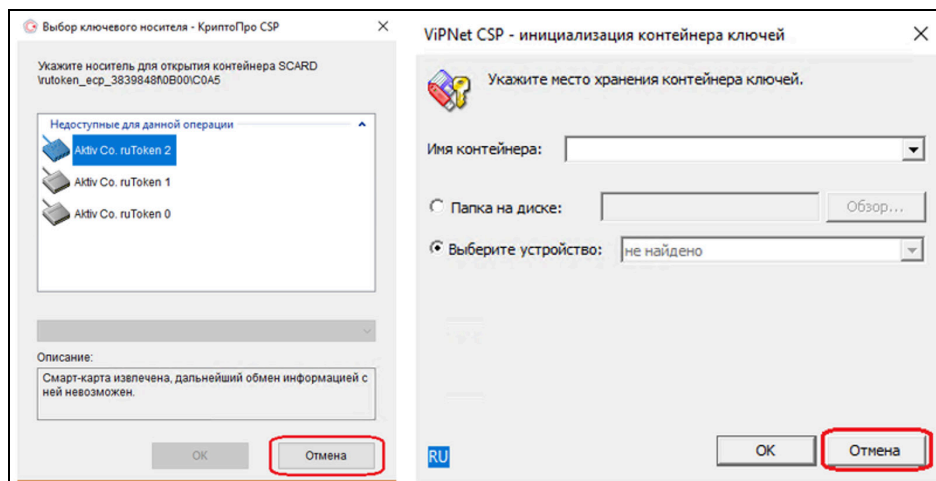


Рисунок 59

Будут показаны диалоговые окна мастера экспорта сертификатов.

НЕ нужно пытаться экспортировать закрытый ключ. Формат файла для экспорта – PKCS#7 (*.p7b)

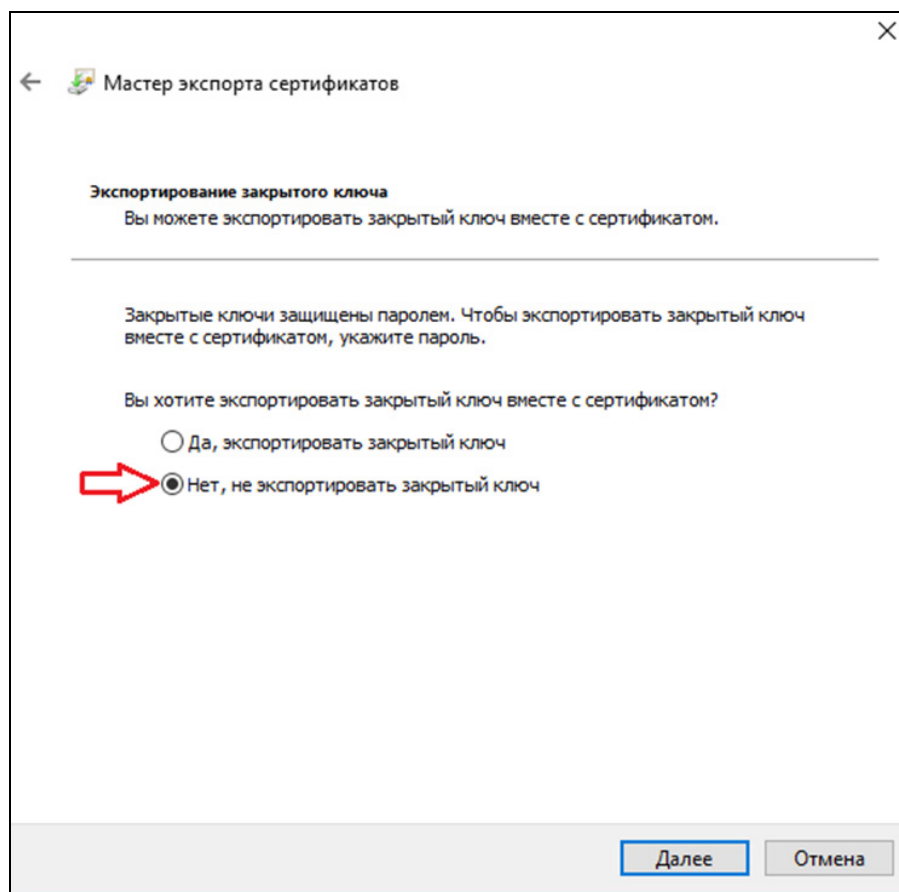


Рисунок 60

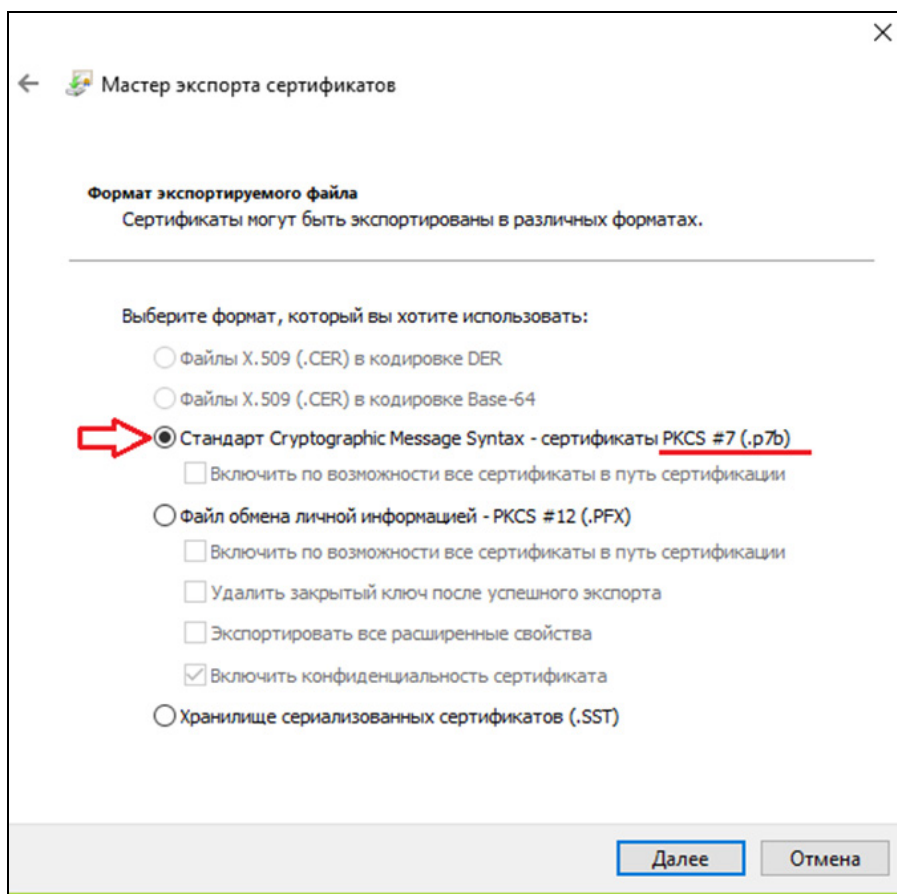


Рисунок 61

По кнопке «Обзор» выберите **место сохранения и имя файла экспорта**:

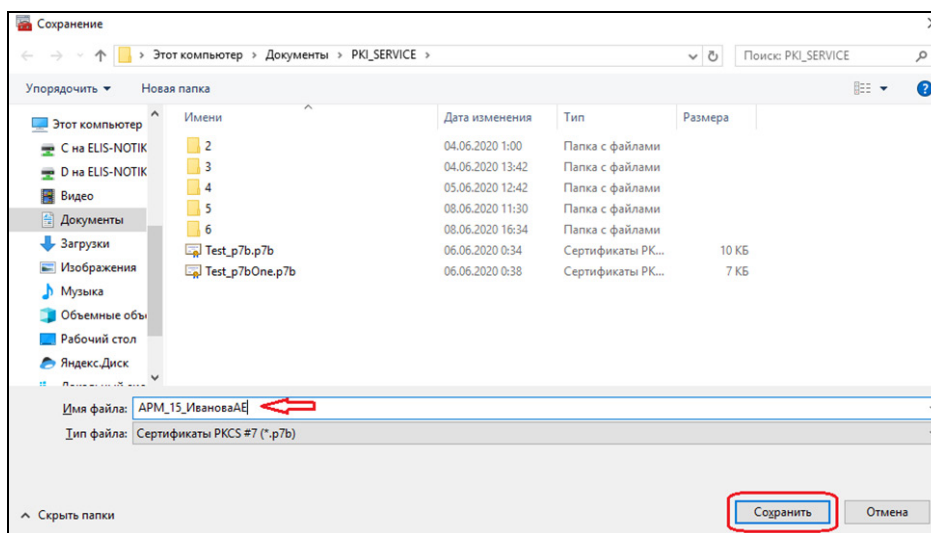


Рисунок 62

Файл будет сохранен с набранным именем и расширением «.p7b»

Проведите аналогичную операцию экспорта для сертификатов категории «Промежуточные Центры Сертификации».

Используйте полученные файлы для импорта в ЭОС РКИ-сервис.

4.10. Приложение 2

4.10.1. Настройка СПО KARMA на компьютерах организации для работы с ЭОС PKI-сервис

Данная функциональность позволяет автоматически получать актуальный статус сертификатов системы квалифицированной ЭП Российской Федерации на компьютерах, не имеющих выхода в сеть Интернет, а так же строить полные актуальные цепочки сертификатов НЭП при отсутствии прямого доступа с АРМ к внутренним УЦ.

Для работы с ЭОС PKI-сервисом на местах пользователей следует использовать СПО KARMA версии **56.2.436** или выше.

4.10.1.1. Настройка связки «ДЕЛО-KARMA» для работы с ЭОС PKI-сервис

Для использования данной функции при работе с системой ДЕЛО должен быть добавлен параметр **CERTMAN_URL** в строку инициализации в настройках опции пользователя «Электронная подпись». Значение данного параметра (url адрес PKI) определяется следующим образом:

Допустим, на сервере развернули PKI - бэк и фронт. Исходные:

- IP машины сервера: **10.10.1.254**
- Порт, указанный в скрипте при установке бэка: **10071**

Тогда в строку инициализации **Объекта поддержки ЭП и шифрования** следует добавить:

CERTMAN_URL=«http://10.10.1.254:10071»

Рисунок 63

Если в строке инициализации присутствуют другие параметры, то данный параметр добавляется после «;»

4.10.1.2. Настройка СПО КАРМА (расширение «Проводника») для работы с ЭОС РКИ-сервис

4.10.1.2.1. Получение доступа для серверной "Кармы"

Допустим, на сервере развернули РКИ - бэк и фронт. Исходные:

- Порт, указанный в скрипте при установке бэка: **10071**

Запустите «**Настройки КАРМА**»

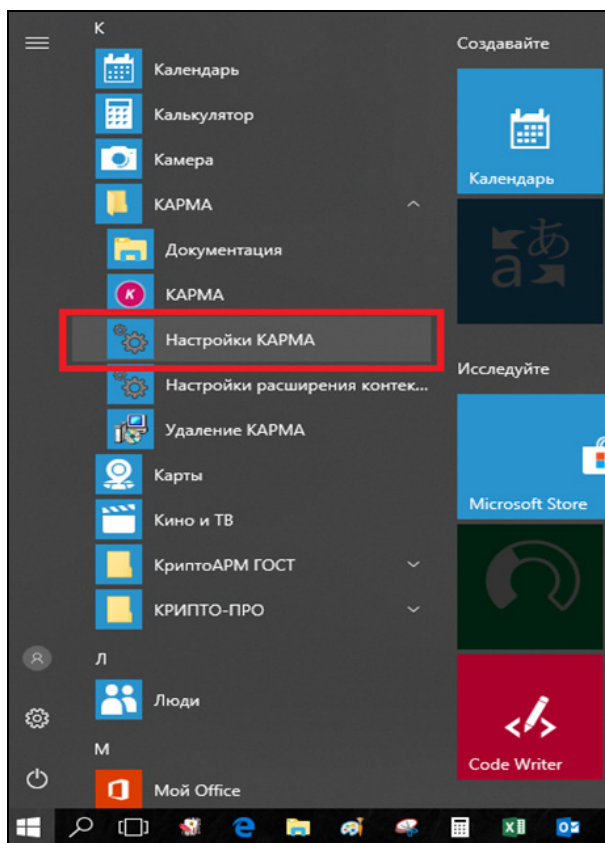


Рисунок 64

Включите чекбокс «Использовать РКИ-сервис», в настройках укажите url бэка: **<http://localhost:10071>**:

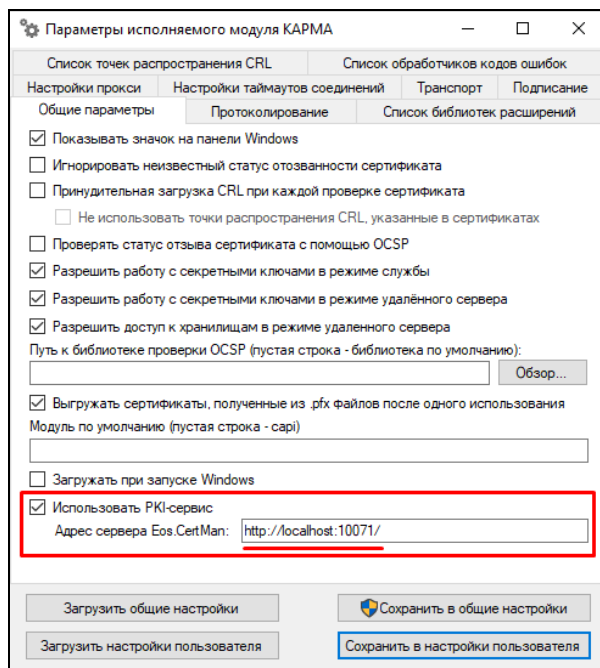


Рисунок 65

Перезапустите KARMA для применения настроек.

4.10.1.2.2. Получение доступа для "Кармы" удалённого ПК

Допустим, на сервере развернули PKI - бэк и фронт. Исходные:

- IP машины сервера: **192.168.0.115**
- Порт, указанный в скрипте при установке бэка: **10071**
- Имя сайта, указанное в скрипте при установке фронта: **pki.devel.loc**

Запустите «**Настройки KARMA**»

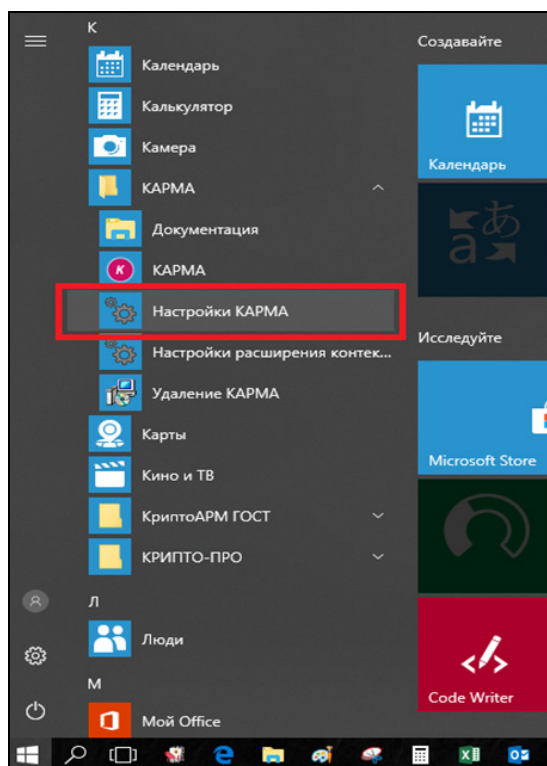


Рисунок 66

Для доступа удалённой Кармы к pki следует включить чекбокс «Использовать PKI-сервис», в настройках указать url бэка: **<http://192.168.0.115:10071>**

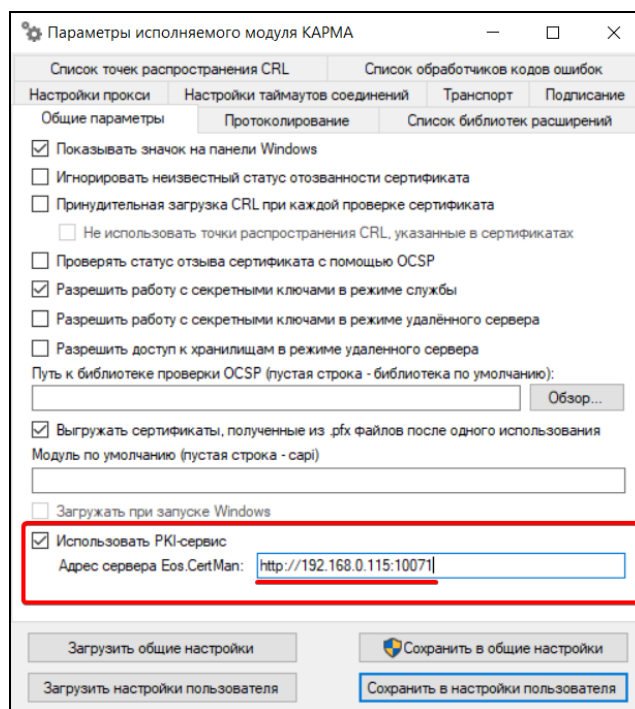


Рисунок 67

Перезапустите КАРМА для применения настроек.

Для доступа к веб сайту с удалённого ПК требуется ввести url: **<https://pki.devel.loc/app/pki>**

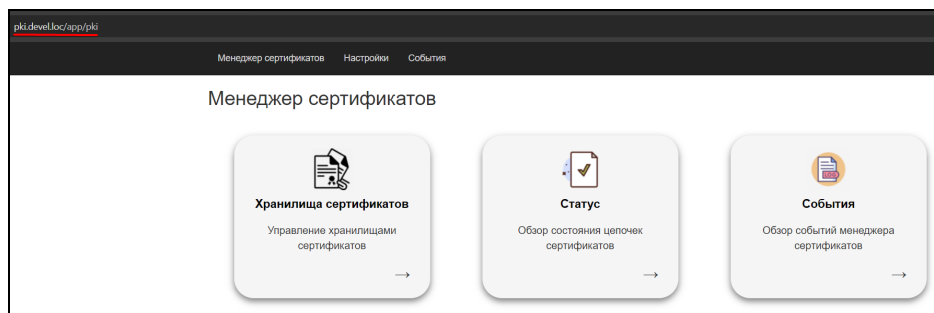


Рисунок 68

4.11. Приложение 3

4.11.1. Пример E-mail-оповещения от ЭОС PKI-сервис

Сообщения об окончании срока действия сертификата и срока действия закрытого ключа приходят разными сообщениями

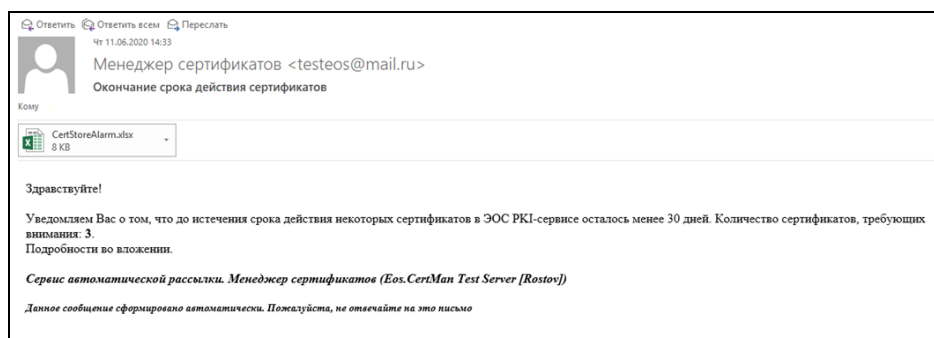


Рисунок 69

Сертификаты, до окончания действия которых осталось менее 30 дней:			
Сертификат	Идентификатор	Действителен до	Владельцы сертификата
ОчСлужба PKI Test Certificate 1	1	10.06.2020 9:20	Служба PKI Test Certificate 1

Сертификаты, до окончания действия которых осталось менее 30 дней:			
Сертификат	Идентификатор	Действителен до	Владельцы сертификата
ОчСлужба PKI Test Certificate 1	1	10.06.2020 9:20	Служба PKI Test Certificate 1
ОчСлужба PKI Test Certificate 2	2	10.06.2020 9:20	Служба PKI Test Certificate 2

Рисунок 70

4.12. Приложение 4

4.12.1. Описание использования фильтров полей сертификатов при рассылке e-mail уведомлений

Содержимое строки фильтрации в таблице - перечень токенов, разделённых знаком запятой "," - для применения фильтрации в логическом режиме "и" или двумя косыми чертами "//" - логический режим "или".

Приоритет логических операций фильтрации следующий:

- // (ИЛИ)
- , (И)

Каждый токен должен быть вида `<Key>.<Attr>=<AttrVal>`

`<Key>` - область поиска, принимает значения **Issuer** - для поиска по имени издателя или **Subject** - для поиска по имени владельца

`<Attr>` - имя фильтруемого X.500 атрибута

`<AttrVal>` - значение фильтруемого X.500 атрибута

Например: Issuer.E=minsvyaz@mail.ru, Subject.C=RU

Таким образом, строка фильтрации содержит в себе совокупность токенов, комбинируемых через логическое И или логическое ИЛИ, используемая для фильтрации общего количества сертификатов, по которым требуется разослать уведомления.

Внимание! Фильтры регистрозависимы, лучшей практикой будет копировать выбираемые поля из «подопытного» сертификата (**copy-past**).

4.12.1.1. Подстановочный знак *

В фильтрации должна быть реализована возможность использования в токене фильтра, а именно в `AttrVal` подстановочного знака * для поиска подстрок в конечной строке выбранного атрибута.

Примеры:

- Subject.E=minsvyaz* - под фильтр попадут сертификаты, владельцы которых имеют e-mail адреса, начинающиеся с "minsvyaz"
- Subject.STREET=*Ленина* - под фильтр попадут сертификаты, владельцы которых в своём адресе имеют слово "Ленина", например, улица Ленина или проспект Ленина
- Subject.SN=*ов - под фильтр попадут сертификаты, владельцы которых имеют фамилии, оканчивающиеся на "ов", например, Иванов, Петров, Сидоров

4.12.1.2. Примеры строк фильтрации таблицы адресов

Скобки [и] используются в некоторых местах ниже для наглядного разделения условий фильтрации

Issuer.E=*svyaz.ru, Subject.C=RU // Subject.O=*Москва* - попадут сертификаты: [издатель имеет e-mail адрес, оканчивающийся на "svyaz.ru" И страна владельца - RU (Россия)] ИЛИ [в имени организации владельца есть слово "Москва"]

Issuer.E=*mail.ru // Issuer.E=*yandex.ru // Subject.C=RU, Subject.O=*Москва* - попадут сертификаты: [издатель имеет e-mail адрес, оканчивающийся на "mail.ru"] ИЛИ [издатель имеет e-mail адрес, оканчивающийся на "yandex.ru"] ИЛИ [страна владельца - RU (Россия) И в имени организации владельца есть слово "Москва"]

Issuer.E=*minsvyaz*, Issuer.C=RU, Issuer.ST=*Москва* // Subject.CN=Минкомсвязь* - попадут сертификаты: [издатель имеет e-mail адрес, содержащий в себе слово "minsvyaz" И страна издателя - RU (Россия) И в адресе издателя есть слово "Москва"] ИЛИ [обычное имя (commonName) владельца начинается с "Минкомсвязь"]

Соответствующему адресату будут отправлены уведомления обо всех истекающих сертификатах с **фамилиями**, заканчивающимися на “нов” или «ейко»:

Subject.SN=*нов

Subject.SN=*ейко

Соответствующему адресату будут отправлены уведомления обо всех истекающих сертификатах с **полем ИНН (физлица, 12 знаков), строго** с этим номером:

Subject.INN=798879879874

Будут отправлены уведомления обо всех истекающих сертификатах по Псковской области с именем и отчеством (строго) «Эдуард Вячеславович» и фамилиями, начинающимися на «Пер»:

Subject.S=*Псковская*, Subject.SN=Пер*, Subject.GN=Эдуард Вячеславович

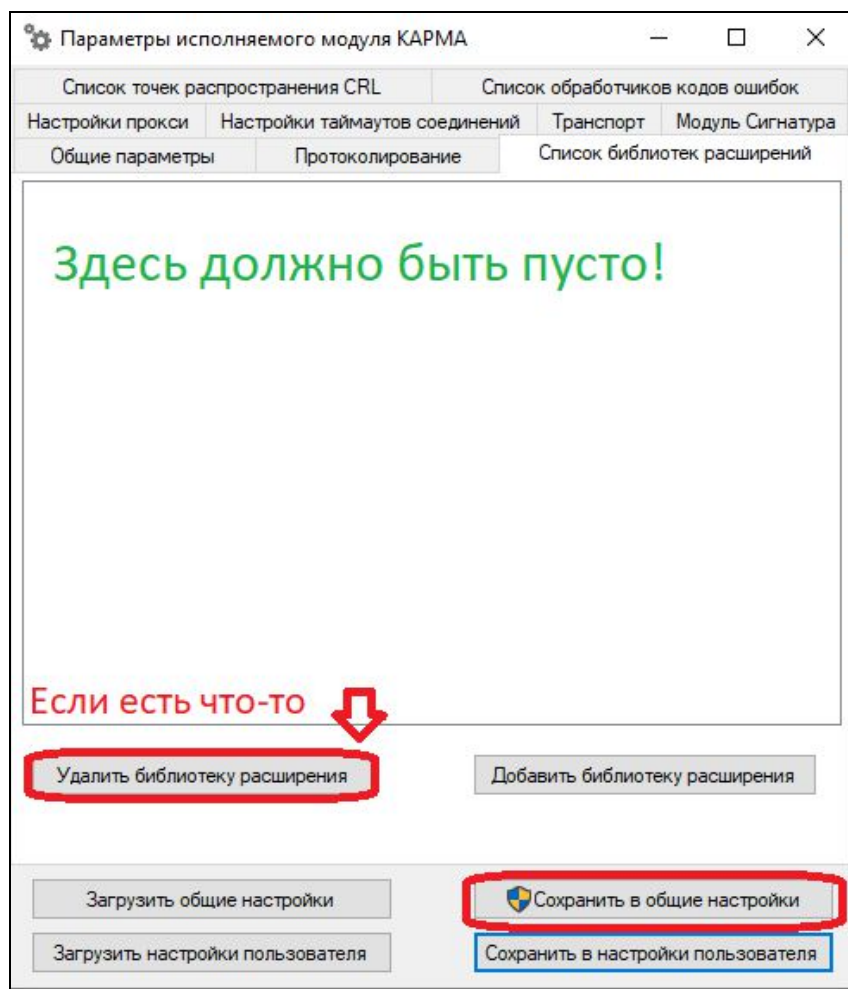


Рисунок 71

- В Карме отключено полное логирование
- На время импорта рекомендуется отключить логирование операций в КАРМЕ, работающей на РКІ-сервисе (запись логов замедляет операции)

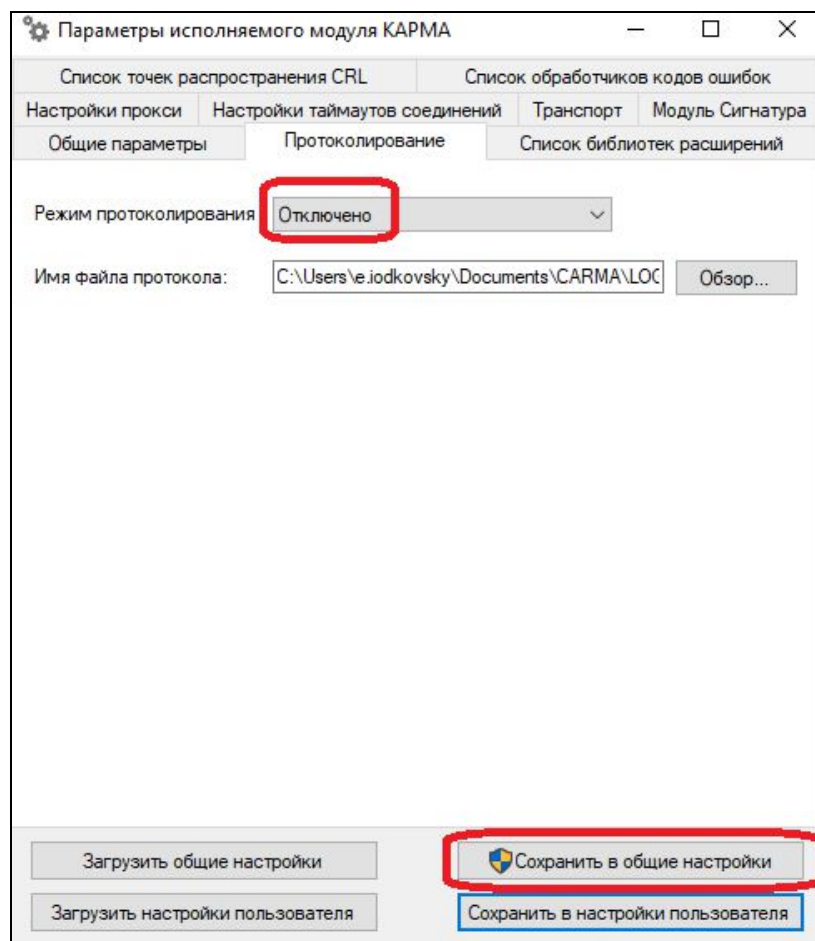


Рисунок 72

- Сервис продолжает работать
- Во время импорта РКІ-сервис продолжает полноценно работать, и к его интерфейсу можно обращаться, например, в другой вкладке браузера

Для запуска процесса импорта нажмите кнопку «Запустить импорт»



Рисунок 73

Внимание!

Импорт может занимать продолжительное время...

Во время импорта выводится информация о прогрессе процесса импорта – «прогресс-бар», численное выражение обработанных файлов ЭП и предполагаемое время до окончания процесса.

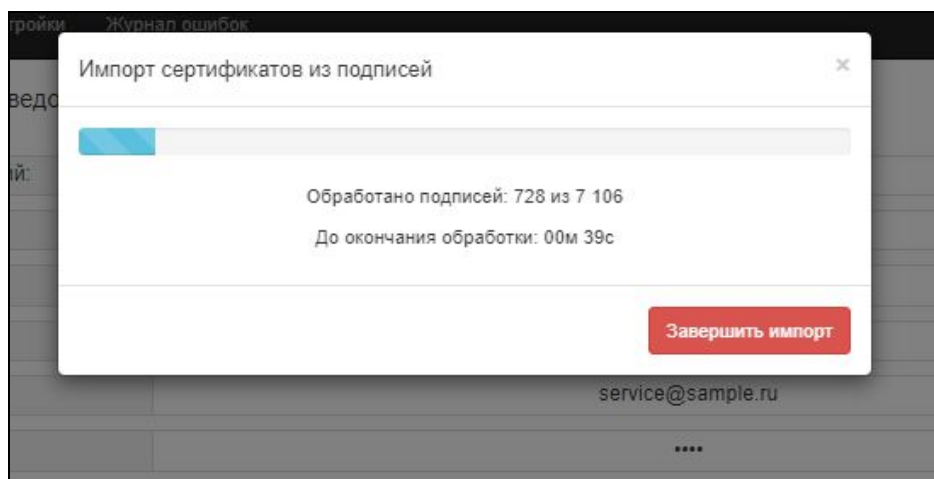


Рисунок 74

В случае необходимости процесс импорта можно прервать (кнопка «Завершить импорт»), при этом будет выведена статистика обработанных сертификатов, а обработанные файлы ЭП будут удалены из папки импорта. Соответственно, в подходящий момент импорт может быть возобновлен снова кнопкой «Запустить импорт».



Рисунок 75

По окончании импорта будет выведена статистика импорта

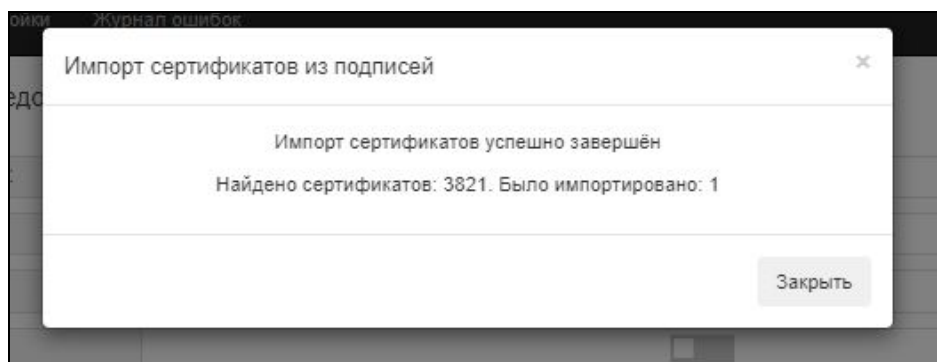


Рисунок 76

При импорте, если активна опция "Удалять успешно обработанные подписи:" (см. блок "Панель «Импорт сертификатов из подписей»" в руководстве пользователя РКІ-сервиса), обработанные файлы электронных подписей из папки импорта удаляются, и остаются только те файлы ЭП (*.sig), которые по каким-либо причинам не были импортированы (смотри условия импорта в начале инструкции). Такие файлы можно посмотреть в ручном режиме в КАРМЕ, в том числе информацию о сертификате подписи, и сделать выводы, почему данный сертификат не был импортирован.

5. РУКОВОДСТВО ПО ИМПОРТУ СЕРТИФИКАТОВ ПОЛЬЗОВАТЕЛЕЙ ИЗ БД СЭД «ДЕЛО»

5.1. Назначение

Способ импорта сертификатов пользователей из базы данных СЭД «ДЕЛО», описываемый в данной инструкции, необходим для **автоматизации** массового первичного или инкрементного импорта сертификатов в ЭОС РКИ-сервис.

5.2. Установленные ограничения

Импортируются только те сертификаты, для которых ЭОС РКИ-сервис может построить полные цепочки доверия.

Для квалифицированных сертификатов «работает само»^[1], для неквалифицированных (тестовых, доменных и прочих) необходимо поместить корневые и промежуточные сертификаты подобных цепочек в соответствующие хранилища ЭОС РКИ-сервиса и обеспечить возможность получения сервисом списков отзыва

[1] При загруженных сертификатах аккредитованных УЦ системы квалифицированной ЭП РФ (см. блок "Автоматический импорт сертификатов Аккредитованных УЦ РФ (КЭП)" в руководстве пользователя РКИ-сервиса).

5.3. Описание процесса импорта

Импорт сертификатов производится в два шага:

- Из базы данных экземпляра СЭД «ДЕЛО» выгружаются данные профилей сертификатов пользователей и массив электронных подписей^[2]
- Полученные на предыдущем шаге данные обрабатываются ЭОС РКИ-сервисом, и сертификаты, удовлетворяющие установленным ограничениям, импортируются в хранилище «Основные пользовательские»

[2] Подробное описание и инструкцию содержит файл "ЭОС РКИ-сервис. Руководство по работе с утилитой по выгрузке подписей из БД СЭД «ДЕЛО».pdf" - поставляется с дистрибутивом РКИ.

5.4. Порядок импорта

5.4.1. Шаг 1. Экспорт из базы данных ДЕЛО

Подробное описание можно посмотреть в файле "ЭОС РКИ-сервис. Руководство по работе с утилитой по выгрузке подписей из БД СЭД «ДЕЛО».pdf" - поставляется с дистрибутивом РКИ.

5.4.2. Шаг 2. Импорт в ЭОС РКИ-сервис

Полученный после выгрузки из "Дела" каталог должен быть перемещён на локальный диск сервера РКИ-сервиса, если выгрузка происходила на другой машине.

Как альтернатива - можно настроить путь к каталогу импорта, расположенному на другой машине сети, используя сетевой диск со всеми необходимыми разрешениями (чтение и запись), но скорость импорта будет гораздо ниже.

Внимание!

Для корректной работы службы импорта требуется выдать полные права на каталог выгрузки из "Дела" (например, DeloExp) для пользователя с именем <AppName>-pkisrv, где <AppName> - имя приложения, заданное в параметре при запуске скриптов инсталляции приложения

На странице настроек РКИ-сервиса необходимо заполнить адрес каталога выгрузки (параметр "Путь до папки с подписями") и сохранить изменения конфигурации.

Внимание!

В каталоге с подписями также необходимо разместить файл с идентификаторами сертификатов **Certs_List.csv**, поэтому, если он выгружался в отдельный каталог - следует переместить его к файлам подписей.

Рисунок 77

«Чеклист» перед проведением импорта:

- Карма без расширений
- На время импорта в КАРМЕ, работающей на РКИ-сервисе, должны быть отключены все дополнительные расширения (таймштамп, графическая подпись, etc.)