

ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00096-06-ЛУ

**СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«ВАЛИДАТА КРИПТОСЕРВЕР» ВЕРСИЯ 4**

АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО УПРАВЛЕНИЯ
КРИПТОГРАФИЧЕСКИМ СЕРВЕРОМ
АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО ФОРМИРОВАНИЯ ОТЧЕТОВ

Руководство администратора

ВАМБ.00096-06 95 01

2020

Аннотация

Настоящий документ содержит сведения о назначении, условиях использования, порядке работы с программным комплексом (ПК) ВАМБ.00096-06 12 02 «Автоматизированное рабочее место управления криптографическим сервером» (далее по тексту — АРМ УКС) и ПК ВАМБ.00096-06 12 03 «Автоматизированное рабочее место формирования отчётов» (далее по тексту — АРМ ФО) из состава ПК ВАМБ.00096-06 «Средство криптографической защиты информации «Валидата Криптосервер» версия 4» (далее по тексту — СКЗИ «Валидата Криптосервер»).

Документ предназначен для администратора криптографического сервера (КС), отвечающего за управление, мониторинг и просмотр журналов КС.

Содержание

1 НАЗНАЧЕНИЕ И УСЛОВИЯ ИСПОЛЬЗОВАНИЯ АРМ УКС	5
2 ЗАПУСК АРМ УКС	6
3 УПРАВЛЕНИЕ СПИСКОМ КС, ПРЕДНАЗНАЧЕННЫХ ДЛЯ МОНИТОРИНГА	8
3.1 Добавление КС	8
3.2 Изменение настроек КС	9
3.3 Удаление КС	10
3.4 Установление соединения с КС	10
3.5 Разрыв соединения с КС	10
4 ПРОСМОТР ПРОТОКОЛОВ КС	11
5 ПРОСМОТР СТАТИСТИК КС	13
6 УПРАВЛЕНИЕ КС	15
6.1 Остановка КС	15
6.2 Загрузка ключей на КС	15
6.3 Управление NLB	15
6.3.1 Остановка NLB	15
6.3.2 Плавная остановка NLB	16
6.3.3 Запуск NLB	16
6.4 Обновление САС	17
6.5 Загрузка сертификата	17
6.6 Загрузка САС	19
6.7 Загрузка сертификатов и САС из каталога	21
6.8 Загрузка обновления	22
6.9 Блокировка криптографической сессии	23
6.10 Разблокировка криптографической сессии	23
6.11 Остановка криптографической сессии	24
6.12 Запуск криптографической сессии	24
6.13 Просмотр сертификатов криптографической сессии	24
6.14 Удаление сертификатов	28
6.15 Удаление аннулированных/прекративших действие сертификатов из сессии криптосервера	28
6.16 Удаление сертификатов с истекшими ключами из сессии криптосервера	29
6.17 Настройка отображения списка сертификатов и САС	30
6.18 Сохранение списка сертификатов и САС	31
6.19 Установка нового рабочего сертификата	31
6.20 Создание отчёта о загруженных объектах по сессии	32
6.21 Установка уровня протоколирования КС	33
6.22 Остановка отображения всплывающих окон	34
7 ПРОСМОТР ПРОТОКОЛА РАБОТЫ АРМ УКС	36

8 НАСТРОЙКА АРМ УКС	37
8.1 Общие настройки	37
8.2 Настройки оповещения	38
8.3 Установка больших кнопок на панели инструментов АРМ УКС	39
9 ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИИ	41
9.1 Получение описания ошибки по коду ошибки	41
9.2 Управление авторизацией сессий	42
10 ЗАВЕРШЕНИЕ РАБОТЫ НА АРМ УКС	44
11 АНАЛИЗ ПРОТОКОЛОВ КС	45
11.1 Запуск АРМ ФО и выход из него	45
11.2 Подключение к базе данных	45
11.3 Импорт протоколов в базу	48
11.4 Очистка базы	51
11.5 Структура базы данных	52
11.6 Выполнение запросов к базе данных и просмотр отчётов	54
11.6.1 Создание, сохранение и открытие запросов	54
11.6.2 Редактирование запросов	54
11.6.3 Выполнение запросов к базе данных	56
11.6.4 Просмотр отчётов	56
11.7 Протокол работы АРМ ФО	60
12 ОПИСАНИЕ ОШИБОЧНЫХ СИТУАЦИЙ	62
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	68
ПЕРЕЧЕНЬ РИСУНКОВ	70
ПЕРЕЧЕНЬ ТАБЛИЦ	72

1 НАЗНАЧЕНИЕ И УСЛОВИЯ ИСПОЛЬЗОВАНИЯ АРМ УКС

Программный комплекс (ПК) ВАМБ.00096-06 12 02 «Автоматизированное рабочее место управления криптосервером» (далее — АРМ УКС) предназначен для управления криптографическим сервером (далее — КС), мониторинга текущего состояния КС, а также для просмотра журналов сообщений и ошибок на всех КС. Взаимодействие между АРМ УКС и КС осуществляется по локальной сети с помощью протокола RPC (Remote Procedure Call).

АРМ УКС устанавливается на компьютере, работающем под управлением операционной системы (ОС) Microsoft Windows. Перечень операционных систем приведён в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

Перед началом установки АРМ УКС необходимо установить и настроить ПК ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее — СКЗИ «Валидата CSP») и ПК ВАМБ.00077-06 «“Валидата Клиент” версия 4» (далее — ПК «Валидата Клиент»). Установка указанных ПК осуществляется в соответствии с документами ВАМБ.00060-06 91 01 «СКЗИ «Валидата CSP» версия 6. Руководство по установке и настройке» и ВАМБ.00077-06 91 01 «“Валидата Клиент” версия 4. Руководство по установке и настройке».

После установки АРМ УКС необходимо организовать контроль целостности АРМ УКС, файлов СКЗИ «Валидата CSP», ПК «Валидата Клиент» и файлов ОС согласно требованиям документа ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

Для корректного функционирования АРМ УКС между данным АРМ и всеми управляемыми им КС должно быть разрешено прохождение следующего сетевого трафика:

- протокол TCP, порт 445 (SMB) - по данному порту АРМ УКС осуществляет чтение файлов протоколов КС;
- протокол TCP, порт 1333 (DCE-RPC) - по данному порту АРМ УКС посылает КС управляющие команды и получает от КС результаты их выполнения.

Более подробно требования к организации сетевого взаимодействия приведены в документе ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

2 ЗАПУСК АРМ УКС

Перед запуском АРМ УКС Администратор АРМ УКС должен, используя ПК «Валидата Клиент», получить собственный сертификат с заданной областью расширенного применения ключа «**Администратор КС**» (OID 1.3.6.1.4.1.10244.4.2.2) и добавить свой сертификат в локальный справочник сессии управления КС (для каждого КС, которым он будет управлять). Ключ электронной подписи (ЭП) сертификата Администратора АРМ УКС используется также в качестве закрытого ключа шифрования для обеспечения возможности удалённой загрузки ключей. Запуск АРМ УКС можно также осуществлять в режиме Оператора, для этого необходим сертификат с заданной областью расширенного применения ключа «**Оператор КС**» (OID 1.3.6.1.4.1.10244.4.2.4).

В режиме Оператора возможны только действия по мониторингу КС, любые административные действия выполняются только в режиме Администратора.

Для запуска АРМ УКС необходимо выбрать пункт системного меню Windows: «**Программы**» - «**СКЗИ Валидата Криптосервер. Версия 4.0**» - «**АРМ УКС**»

При загрузке АРМ УКС требуется загрузить ключ ЭП Администратора АРМ УКС. В зависимости от настроек СКЗИ «Валидата CSP» поиск ключа будет осуществляться на всех доступных носителях или пользователю нужно будет вручную указать считыватель, а затем выбрать ключевой носитель, если их обнаружено несколько и указать требуемый ключ.

Если ключ не обнаружен на подключённых ключевых носителях, АРМ УКС запрашивает установку ключевого носителя с ключом ЭП Администратора АРМ УКС (Рисунок 1)

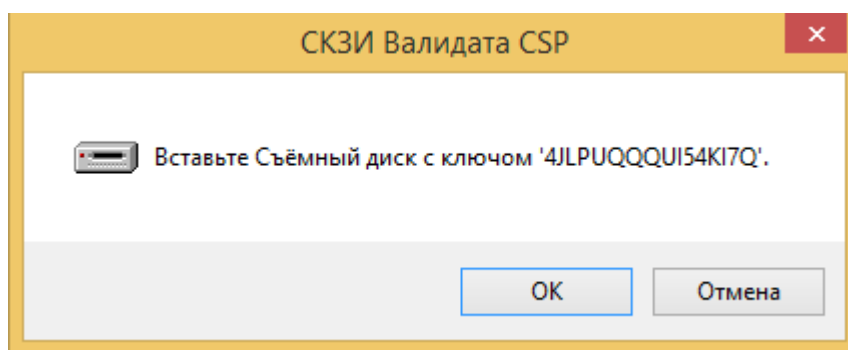


Рисунок 1 – Загрузка ключа

При успешной загрузке ключа ЭП Администратора АРМ УКС на экране появляется основное окно АРМ УКС (Рисунок 2).

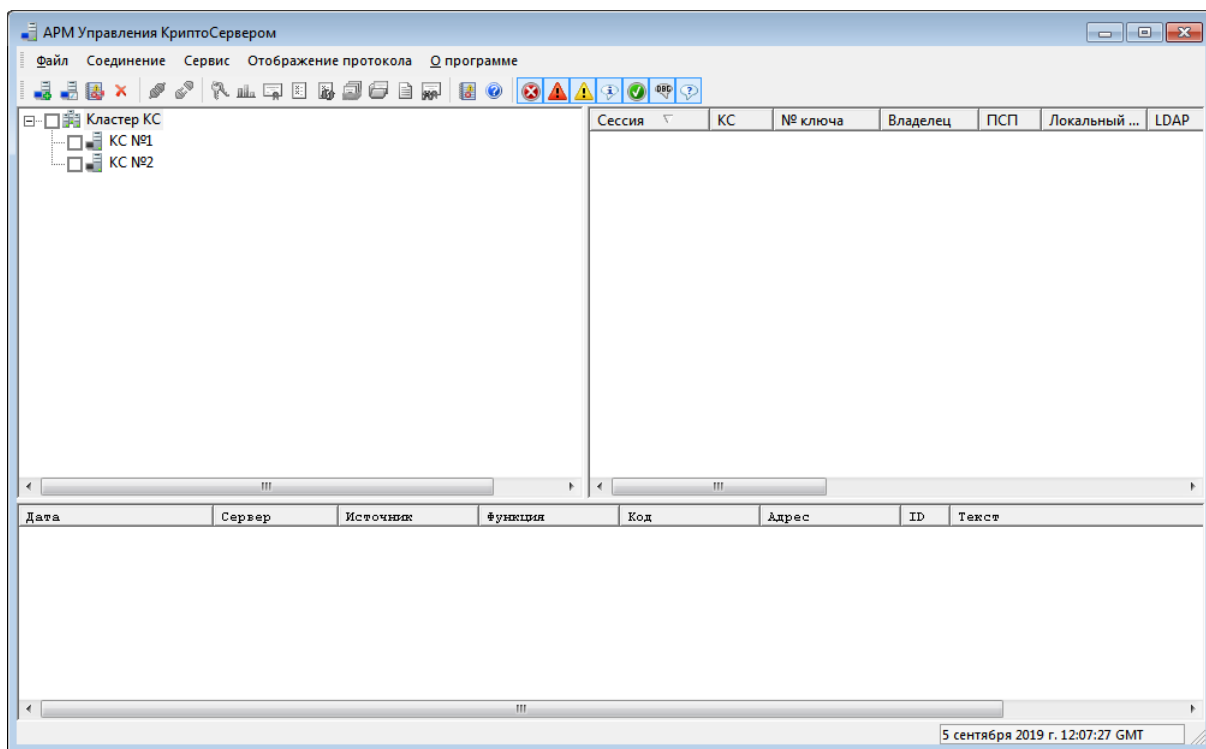



Рисунок 2 – Основное окно АРМ УКС

В левой части основного окна АРМ УКС отображается перечень всех КС, доступных Администратору АРМ УКС с данного АРМ УКС. КС группируются по кластерам. КС, не входящие ни в один кластер, объединяются в группу «Отдельные КС».

3 УПРАВЛЕНИЕ СПИСКОМ КС, ПРЕДНАЗНАЧЕННЫХ ДЛЯ МОНИТОРИНГА

3.1 Добавление КС

Для добавления КС в список для мониторинга Администратору АРМ УКС необходимо нажать кнопку  на панели инструментов или выбрать пункт меню «Соединение» - «Добавить криптосервер».

При этом отображается диалог для добавления КС (Рисунок 3).

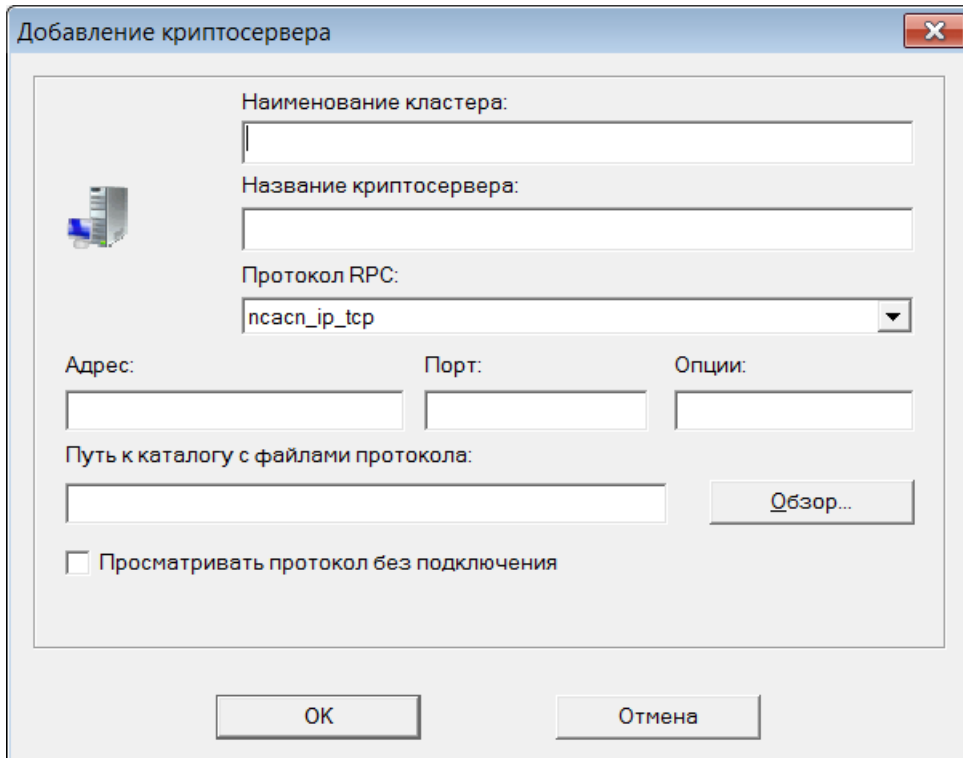


Рисунок 3 – Добавление криптосервера

Для добавления КС необходимо заполнить следующие поля:


- **Наименование кластера** - любое наименование, служит для группировки КС. КС с одинаковым наименованием кластера будут объединяться в группу;
- **Название криптосервера** - любое имя, под которым КС будет отображаться в списке;
- **Протокол RPC** - протокол, по которому будет осуществляться доступ к КС (рекомендуется использовать ncasn_ip_tcp);
- **Адрес** - сетевой адрес КС, по которому будет осуществляться доступ к КС (рекомендуется задавать как IP-адрес);
- **Порт** - сетевой порт службы RPC КС, по которому будет осуществляться доступ Администратора АРМ УКС к КС (рекомендуется задавать);
- **Опции** - опции для подключения по RPC протоколу (можно не задавать);

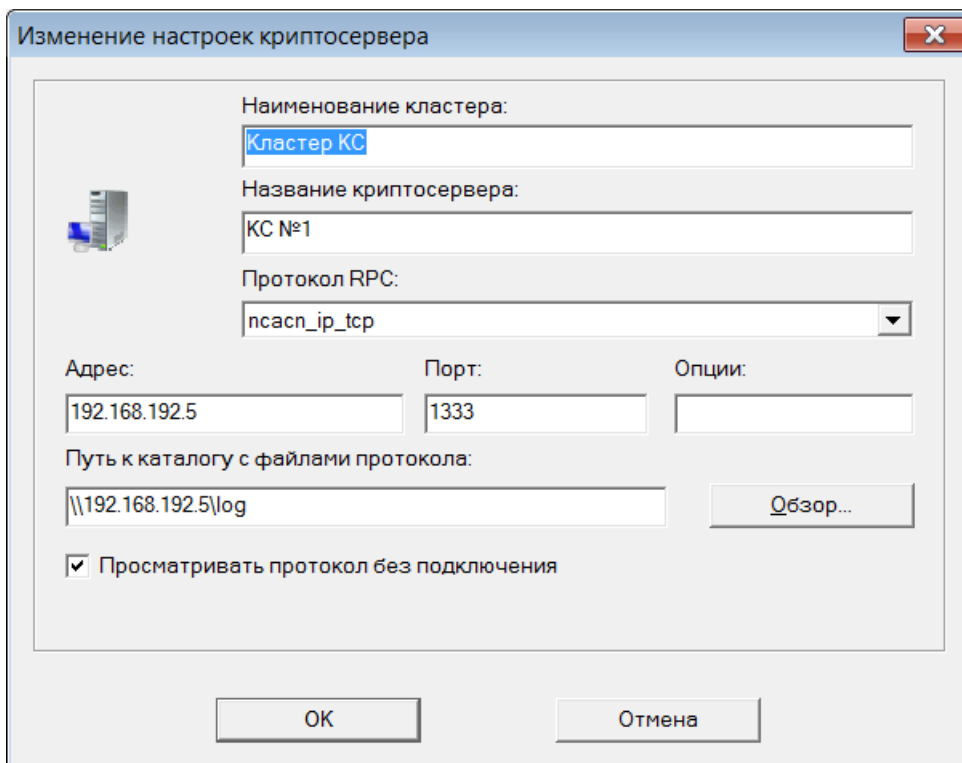
– **Путь к каталогу с файлами протокола** - каталог, в котором хранятся протоколы КС (для этого на КС необходимо настроить сетевой доступ на чтение для Администратора АРМ УКС), для выбора каталога можно воспользоваться кнопкой **«Обзор»**;

– **Просматривать протокол без подключения** - если флаг установлен, то есть возможность просматривать протокол КС без активного подключения к нему (может потребоваться для анализа ошибок запуска КС).

После заполнения всех необходимых полей необходимо нажать кнопку **«ОК»**, и КС будет добавлен в список КС. Нажмите кнопку **«Отмена»**, чтобы отказаться от добавления КС.

3.2 Изменение настроек КС

Для изменения настроек КС Администратору АРМ УКС необходимо выбрать из списка КС необходимый ему КС и нажать кнопку  на панели инструментов или дважды щелкнуть левой кнопкой «мыши» по выбранному КС, или выбрать пункт меню **«Соединение»** – **«Свойства»**. При этом отображается окно для изменения настроек КС (Рисунок 4).



Изменение настроек криптосервера

Наименование кластера:
Кластер КС

Название криптосервера:
КС №1

Протокол RPC:
ncacn_ip_tcp

Адрес: 192.168.192.5 Порт: 1333 Опции:

Путь к каталогу с файлами протокола:
\\192.168.192.5\log Обзор...

☒ Просматривать протокол без подключения


ОК Отмена

Рисунок 4 – Изменение настроек криптосервера

Значение полей описано в подразделе 3.1.


После изменения всех необходимых полей нажмите кнопку **«ОК»** для сохранения изменений или кнопку **«Отмена»** для отказа от изменения настроек.

3.3 Удаление КС

Для удаления КС из списка КС отметьте галочкой нужный КС или группу КС и нажмите кнопку  на панели инструментов или выберите пункт меню «Соединение» – «Удалить криптосервер».


Далее нужно подтвердить действие в появившемся диалоговом окне.

3.4 Установление соединения с КС

Для активного мониторинга КС Администратору АРМ УКС необходимо выполнить соединение с КС. Для соединения с КС выберите требуемый КС или группу КС и нажмите кнопку  на панели инструментов или выберите пункт меню «Соединение» – «Установить соединение с КС».


После установления соединения с КС Администратор АРМ УКС имеет возможность управлять КС и получать статистику о работе КС в целом и по сессиям КС в отдельности.

3.5 Разрыв соединения с КС

Для прекращения активного мониторинга КС Администратору АРМ УКС необходимо выполнить разрыв соединения с КС. Для разрыва соединения выберите требуемый КС или группу КС в списке и нажмите кнопку  на панели инструментов или выберите пункт меню «Соединение» – «Разорвать соединение с КС».

После выполнения разрыва соединения с КС все окна статистик по выбранному КС закрываются. Также заканчивается активный просмотр протокола работы КС (если не установлен флаг **Просмотр протоколов КС без подключения**).

4 ПРОСМОТР ПРОТОКОЛОВ КС

Просмотр протоколов КС включается автоматически после соединения с КС. Если необходимо просматривать протокол без подключения, то нужно установить флаг **Просмотр протоколов без подключения**. Для этого выберите в списке требуемый КС и нажмите кнопку  на панели инструментов или выберите пункт меню «Соединение» – «Протокол без подключения».

Окно просмотра протокола содержит строки протокола, полученного с КС (Рисунок 5).

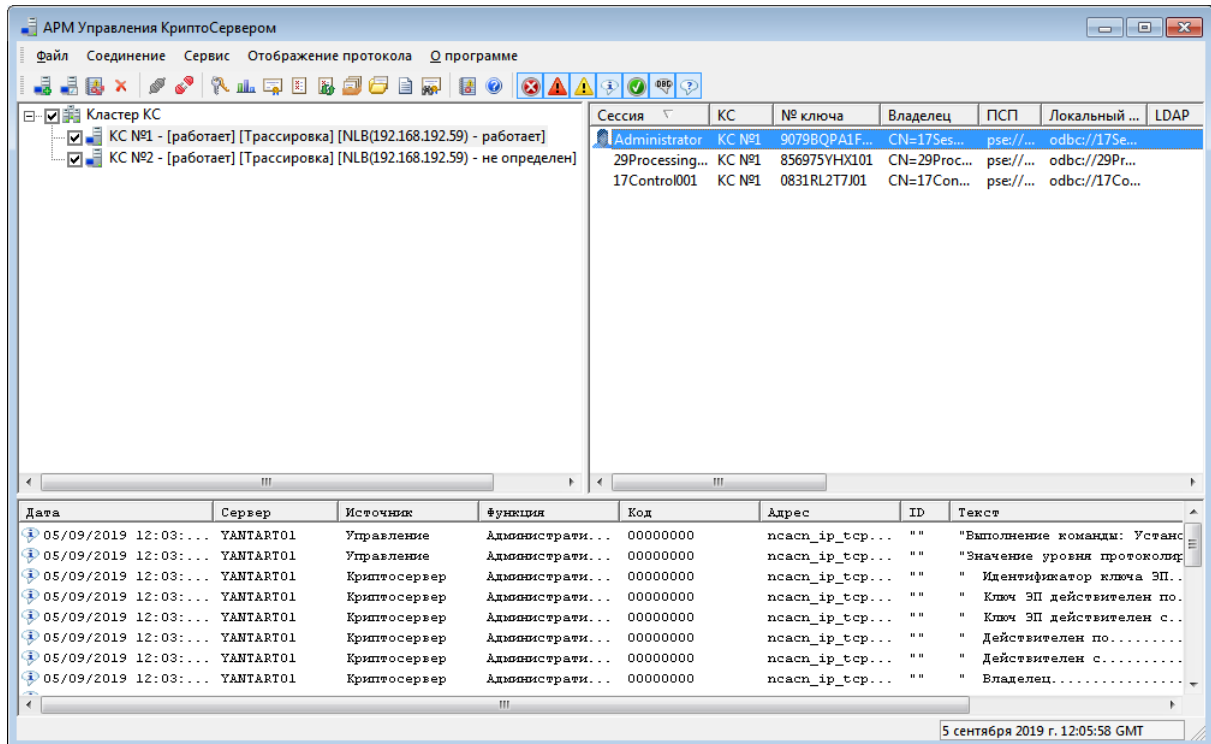









Рисунок 5 – Окно просмотра протоколов

Протокол отображается в виде таблицы со столбцами:

- **Дата** - дата и время события;
- **Сервер** - имя сервера, на котором работает КС;
- **Источник** - код источника события или текст (если имеется);
- **Функция** - код функции или наименование (если имеется), в которой произошло событие;
- **Код** - код возврата функции;
- **Адрес** - строка подключения пользователя;
- **ID** - идентификатор сертификата (X500-имя владельца);
- **Текст** - пояснительный текст к событию.

Строки также имеют иконки в зависимости от значимости события:

-  - фатальная ошибка;

-  - ошибка;
-  - предупреждение;
-  - информационное сообщение;
-  - аудит успехов;
-  - расширенная информация;
-  - неизвестное сообщение.

С помощью соответствующих кнопок на панели инструментов можно фильтровать протокол, отображая или скрывая те или иные типы событий.

Для получения детального отображения о строке протокола необходимо двойным щелчком «мыши» выбрать интересующую строку протокола. Далее откроется окно с отображением события (Рисунок 6).

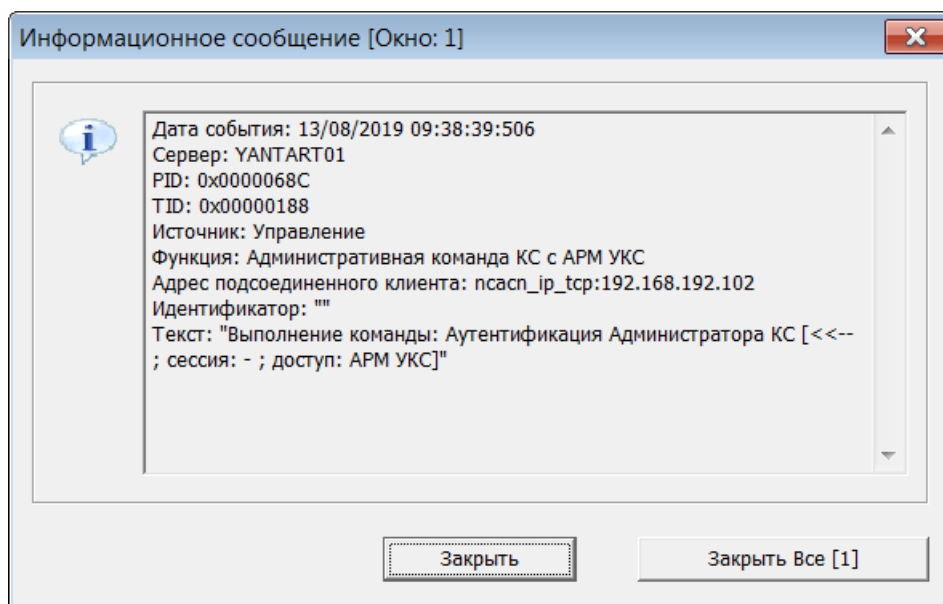



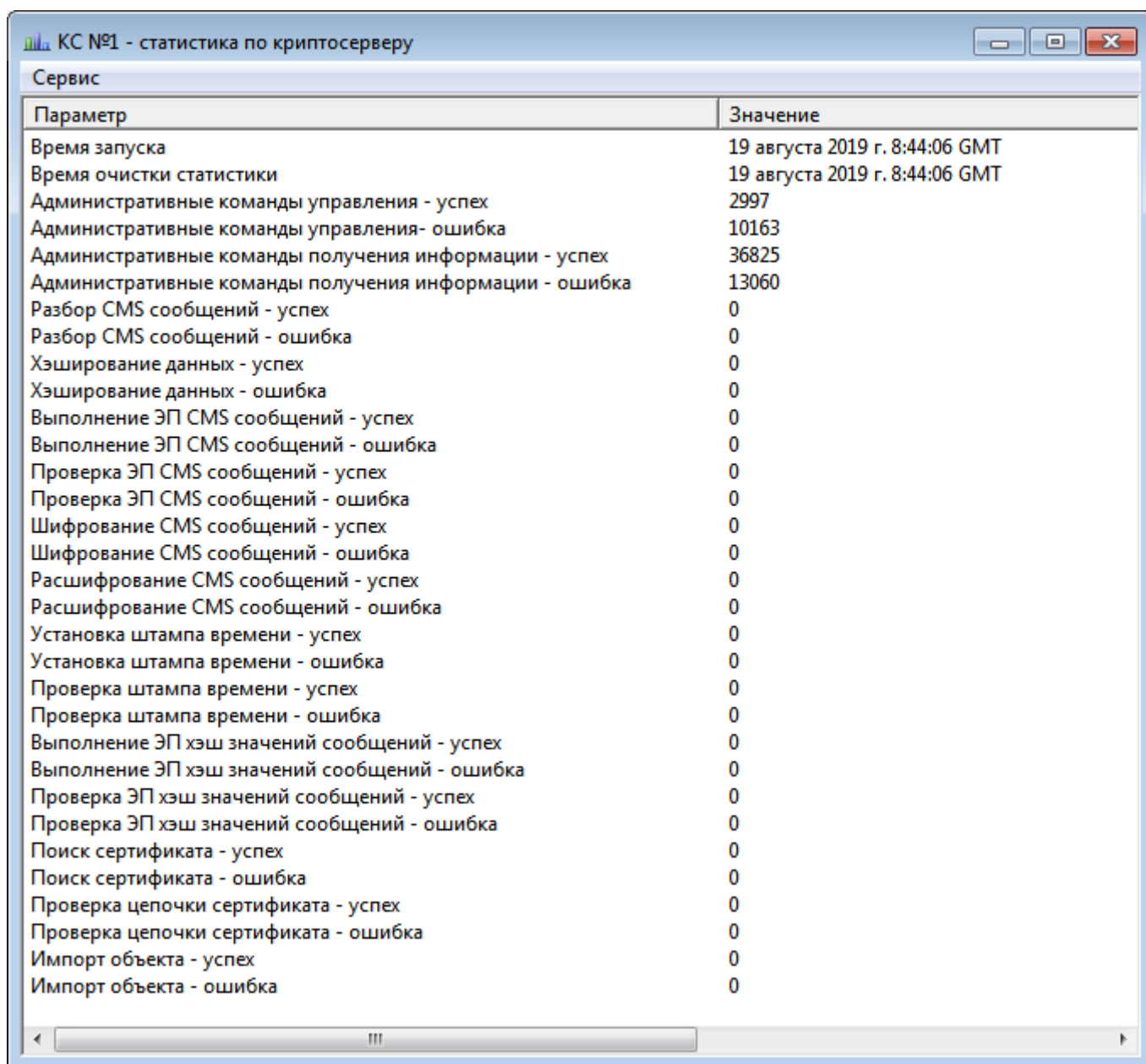
Рисунок 6 – Окно просмотра строки протокола

Для корректной записи протокола работы АРМ УКС Администратору АРМ УКС необходимо увеличить размер файла протокола до 32 МБ. В случае если АРМ УКС не сможет записать в протокол сообщение, то данное сообщение будет продублировано Администратору АРМ УКС на экран.

5 ПРОСМОТР СТАТИСТИК КС

АРМ УКС позволяет Администратору АРМ УКС просматривать текущее состояние каждого доступного КС. Для просмотра статистики Администратору АРМ УКС необходимо выбрать из списка (отметить галочкой) КС необходимый ему КС (с которым установлено соединение) и нажать кнопку  на панели инструментов или выбрать пункт меню «Сервис» - «Посмотреть статистику».


Далее появится немодальное окно со статистикой по КС (Рисунок 7), которое можно использовать для постоянного мониторинга статистики (даже при переключении на другой КС).



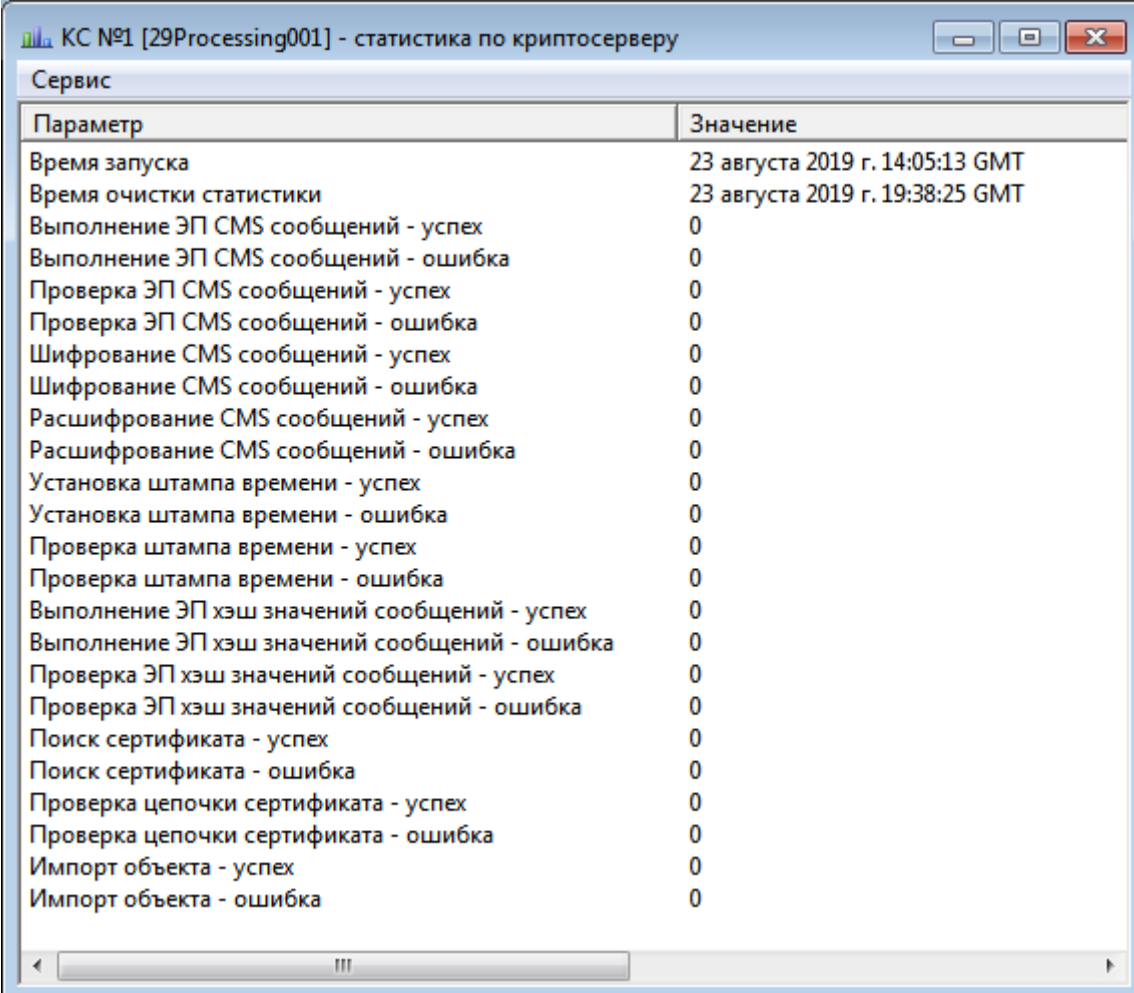
Параметр	Значение
Время запуска	19 августа 2019 г. 8:44:06 GMT
Время очистки статистики	19 августа 2019 г. 8:44:06 GMT
Административные команды управления - успех	2997
Административные команды управления - ошибка	10163
Административные команды получения информации - успех	36825
Административные команды получения информации - ошибка	13060
Разбор CMS сообщений - успех	0
Разбор CMS сообщений - ошибка	0
Хэширование данных - успех	0
Хэширование данных - ошибка	0
Выполнение ЭП CMS сообщений - успех	0
Выполнение ЭП CMS сообщений - ошибка	0
Проверка ЭП CMS сообщений - успех	0
Проверка ЭП CMS сообщений - ошибка	0
Шифрование CMS сообщений - успех	0
Шифрование CMS сообщений - ошибка	0
Расшифрование CMS сообщений - успех	0
Расшифрование CMS сообщений - ошибка	0
Установка штампа времени - успех	0
Установка штампа времени - ошибка	0
Проверка штампа времени - успех	0
Проверка штампа времени - ошибка	0
Выполнение ЭП хэш значений сообщений - успех	0
Выполнение ЭП хэш значений сообщений - ошибка	0
Проверка ЭП хэш значений сообщений - успех	0
Проверка ЭП хэш значений сообщений - ошибка	0
Поиск сертификата - успех	0
Поиск сертификата - ошибка	0
Проверка цепочки сертификата - успех	0
Проверка цепочки сертификата - ошибка	0
Импорт объекта - успех	0
Импорт объекта - ошибка	0

Рисунок 7 – Статистика криптосервера

Значения будут периодически автоматически обновляться (по умолчанию используется период обновления 15 сек). Для просмотра статистики

по конкретной сессии необходимо выбрать нужную сессию в списке сессий и нажать кнопку  на панели инструментов или выбрать пункт меню **«Сервис» - «Посмотреть статистику»**.

Далее появится окно со статистикой по сессии (Рисунок 8).



Параметр	Значение
Время запуска	23 августа 2019 г. 14:05:13 GMT
Время очистки статистики	23 августа 2019 г. 19:38:25 GMT
Выполнение ЭП CMS сообщений - успех	0
Выполнение ЭП CMS сообщений - ошибка	0
Проверка ЭП CMS сообщений - успех	0
Проверка ЭП CMS сообщений - ошибка	0
Шифрование CMS сообщений - успех	0
Шифрование CMS сообщений - ошибка	0
Расшифрование CMS сообщений - успех	0
Расшифрование CMS сообщений - ошибка	0
Установка штампа времени - успех	0
Установка штампа времени - ошибка	0
Проверка штампа времени - успех	0
Проверка штампа времени - ошибка	0
Выполнение ЭП хэш значений сообщений - успех	0
Выполнение ЭП хэш значений сообщений - ошибка	0
Проверка ЭП хэш значений сообщений - успех	0
Проверка ЭП хэш значений сообщений - ошибка	0
Поиск сертификата - успех	0
Поиск сертификата - ошибка	0
Проверка цепочки сертификата - успех	0
Проверка цепочки сертификата - ошибка	0
Импорт объекта - успех	0
Импорт объекта - ошибка	0

Рисунок 8 – Окно статистики сессии криптосервера

В квадратных скобках указано наименование сессии.

Сброс статистики для каждого окна осуществляется через меню окна отображения статистики: **«Сервис» - «Сбросить статистику»**


6 УПРАВЛЕНИЕ КС

6.1 Остановка КС

Для остановки работы КС выберите из списка требуемый КС (поставьте галочкой) и выберите пункт меню «**Соединение**» – «**Остановить криптосервер**».

После остановки КС все окна статистик по выбранному КС закрываются. Также заканчивается активный просмотр протокола работы КС (если не установлен «**Просмотр протоколов криптосервера без подключения**»). Соединение с КС разрывается. Последующий запуск КС может быть выполнен только на самом КС. Для этого необходимо запустить сервис «**CryptoServer**» из панели управления сервисами или выполнить команду **net start cryptoserver**.

6.2 Загрузка ключей на КС

Загрузка ключей на КС выполняется удаленно непосредственно с АРМ УКС. Для загрузки ключа на КС Администратору АРМ УКС необходимо выбрать (отметить галочкой) из списка КС нужный КС (с которым установлено соединение) и нажать кнопку  на панели инструментов или выбрать пункт меню «**Сервис**» – «**Загрузить ключи**».

Далее нужно выбрать считыватель ключа, а затем ключевой носитель, если в настройках СКЗИ «Валидата CSP» не задан автоматический поиск ключей на доступных носителях. Затем появляется диалог (Рисунок 9), отображающий все доступные ключи для загрузки на указанном носителе (или на всех доступных носителях при автоматическом поиске ключей). Для подтверждения загрузки ключа необходимо указать ключ и нажать кнопку «**ОК**».

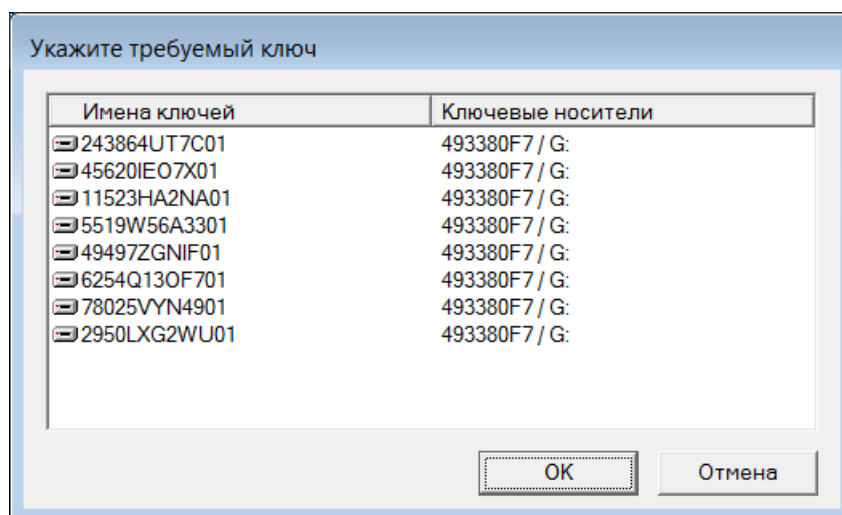


Рисунок 9 – Выбор ключа с носителя

6.3 Управление NLB

6.3.1 Остановка NLB

Для остановки NLB (Network Load Balancing) КС Администратору АРМ УКС нужно выбрать (отметить галочкой) требуемый КС в списке (с которым установлено соединение), а затем выбрать пункт меню «**Сервис**» – «**Остановить NLB**».

После успешной остановки NLB в статусе NLB выбранного КС будет указано «остановлен» (Рисунок 10).

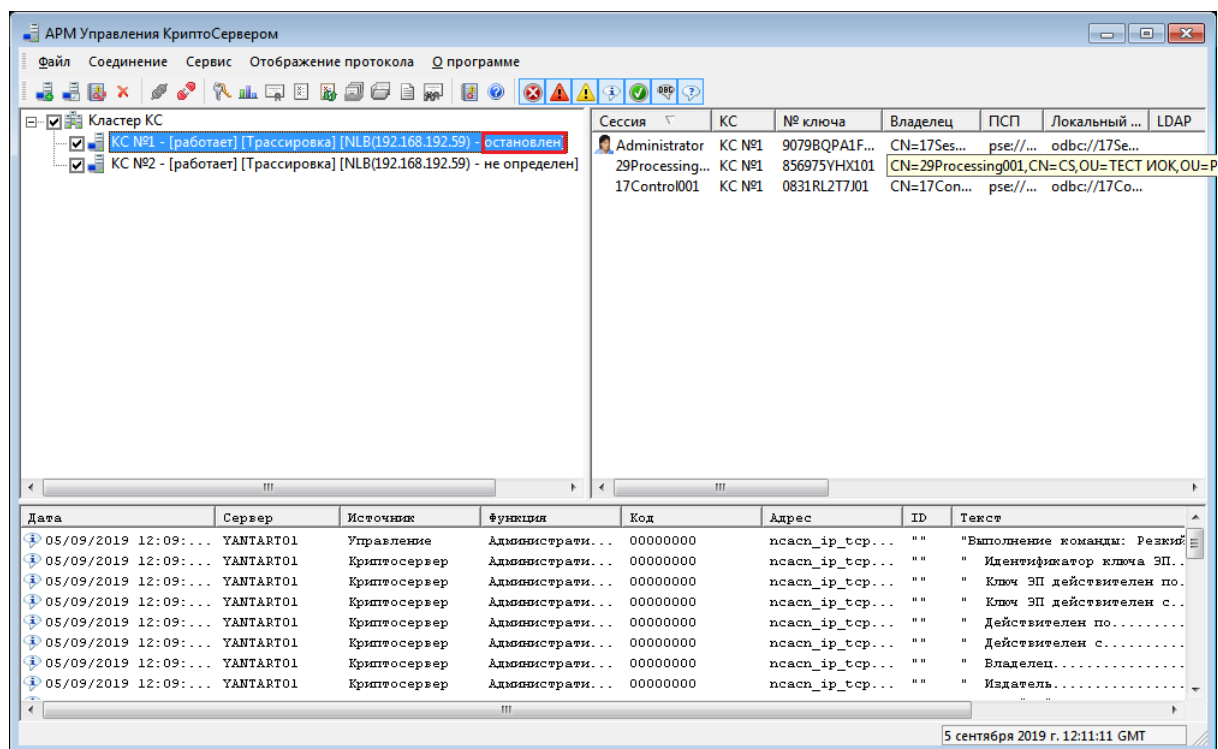


Рисунок 10 – NLB остановлен

6.3.2 Плавная остановка NLB

При обычной остановке NLB (см. п. 6.3.1) производится так называемая «жёсткая» остановка NLB, то есть NLB останавливается вне зависимости от наличия на данном КС обрабатываемых заданий. Администратор АРМ УКС имеет возможность произвести плавную остановку NLB. В этом случае остановка NLB будет произведена после обработки имеющихся заданий. Для плавной остановки NLB нужно выбрать требуемый КС в списке, а затем выбрать пункт меню «Сервис» – «Плавно остановить NLB».

6.3.3 Запуск NLB

Для запуска NLB (Network Load Balancing) КС Администратору АРМ УКС необходимо выбрать (отметить галочкой) требуемый КС в списке (с которым установлено соединение и статус NLB - «остановлен»), а затем выбрать пункт меню «Сервис» – «Запустить NLB». После успешного запуска NLB в статусе NLB выбранного КС будет указано «работает» (Рисунок 11).

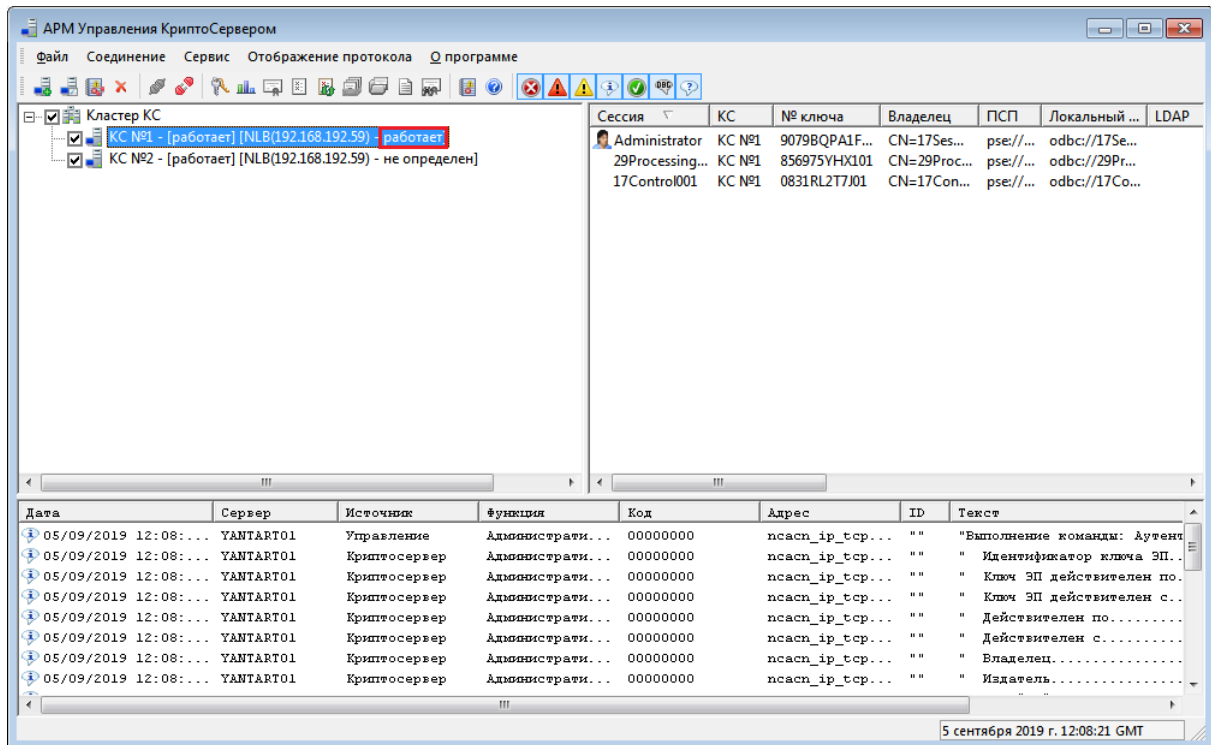




Рисунок 11 – NLB работает


6.4 Обновление САС

Для обновления списка аннулированных сертификатов (САС) КС выберите требуемый КС в списке (с которым установлено соединение) и нажмите кнопку  на панели инструментов или выберите пункт меню «Сервис» – «Обновить САС».

Обновить САС можно также для конкретной сессии КС. Для этого необходимо выбрать требуемую сессию в списке сессий и нажать кнопку  на панели инструментов или выбрать пункт меню «Сервис» – «Обновить САС».

Примечание - Обновление САС происходит из сетевого справочника сертификатов (ССС). После нажатия кнопки или выбора соответствующего пункта меню КС отправляется команда обновить САС из указанной в нем точки распространения САС.

6.5 Загрузка сертификата

Загрузка сертификата производится только на определённую сессию КС. Для загрузки сертификата выберите нужную сессию и нажмите кнопку  на панели инструментов или выберите пункт меню «Сервис» – «Добавить сертификат». Для загрузки сертификатов в кластер необходимо выбирать сессии из списка сессий кластера.

Далее появится файловый диалог (Рисунок 12), предлагающий выбрать файл сертификата или несколько файлов сертификатов для загрузки.

Не допускается добавление сертификата с идентификатором ключа, если сертификат с таким же идентификатором ключа уже существует в

базе сертификатов.

Примечание - При добавлении такого сертификата в DER-кодировке через простой интерфейс или через АРМ УКС выдается ошибка VCERT_E_TOO_MANY_CERTS_FOUND и сертификат не добавляется (в случае КС это сообщение протоколируется как Фатальная ошибка). При добавлении такого сертификата в составе обновления через простой интерфейс или через АРМ УКС сертификат не добавляется, однако обработка обновления продолжается (в случае КС добавляется в протокол фатальная ошибка с кодом VCERT_E_TOO_MANY_CERTS_FOUND).

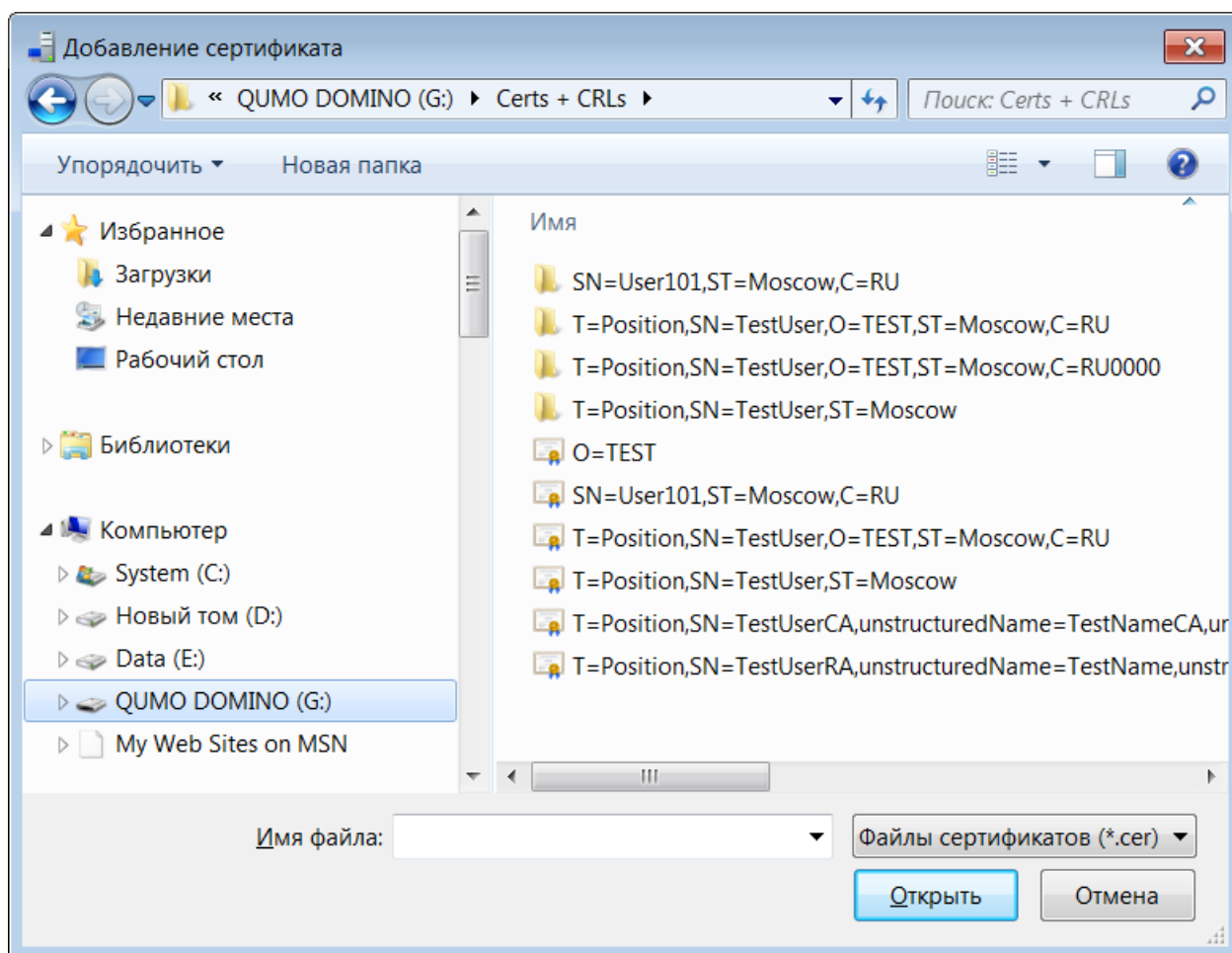


Рисунок 12 - Файловый диалог выбора сертификата

После выбора сертификатов появляется запрос «**Показывать объекты?**». При нажатии кнопки «**Да**» будет отображен каждый загружаемый сертификат (Рисунок 13).

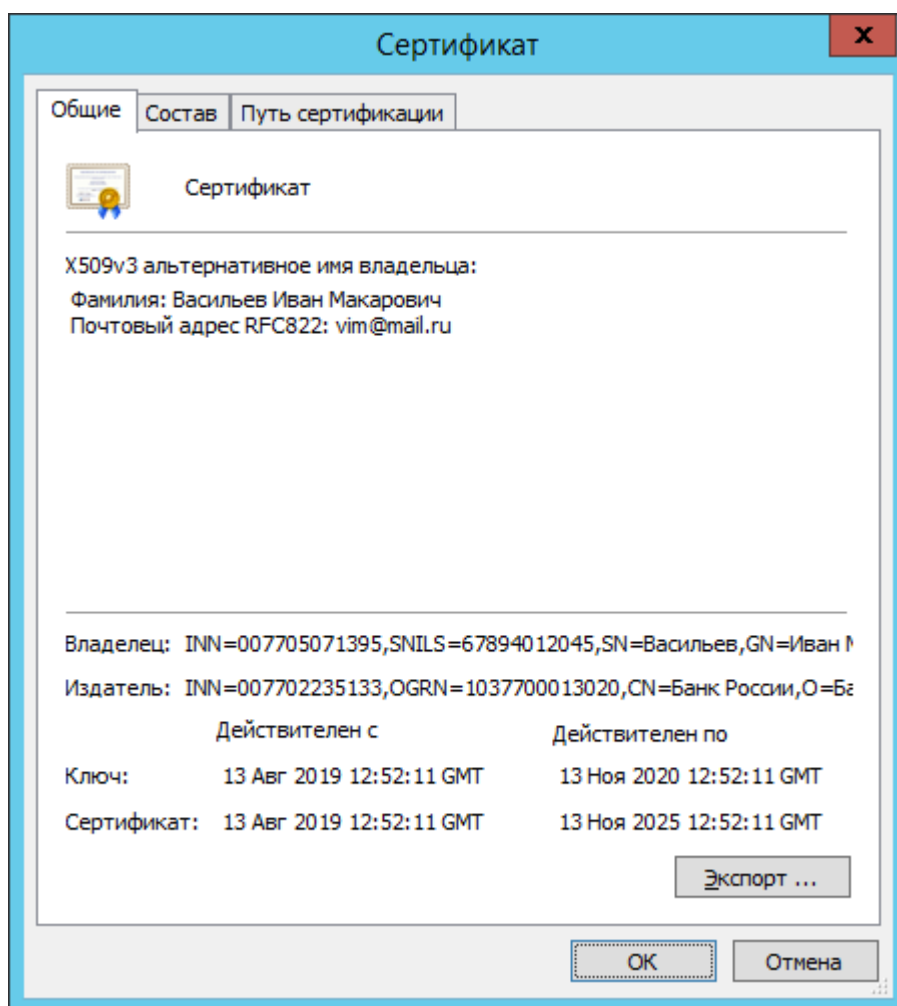



Рисунок 13 – Отображение сертификата

Для подтверждения загрузки нажмите кнопку «**ОК**».

6.6 Загрузка САС

Загрузка САС производится только на определённую сессию КС.

Для загрузки САС выберите нужную сессию и нажмите кнопку  на панели инструментов или выберите пункт меню «**Сервис**» – «**Добавить САС**».

Для загрузки САС в кластер необходимо выбирать сессии из списка сессий кластера.

Далее появится файловый диалог (Рисунок 14), предлагающий выбрать файл САС или несколько файлов САС для загрузки.

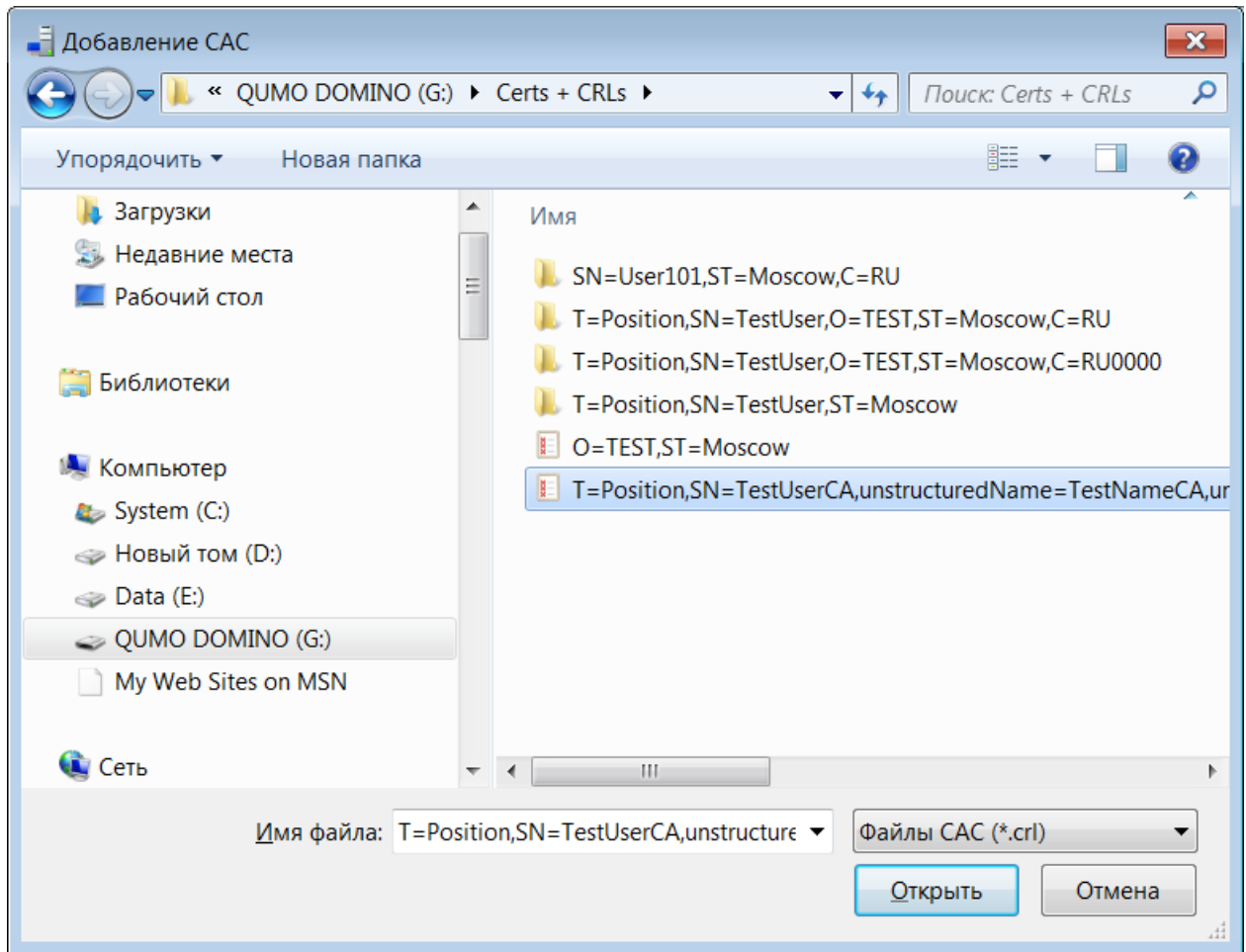


Рисунок 14 – Файловый диалог выбора САС

После выбора САС появляется запрос «**Показывать объекты?**». При нажатии кнопки «**Да**» будет отображен каждый загружаемый САС (Рисунок 15).

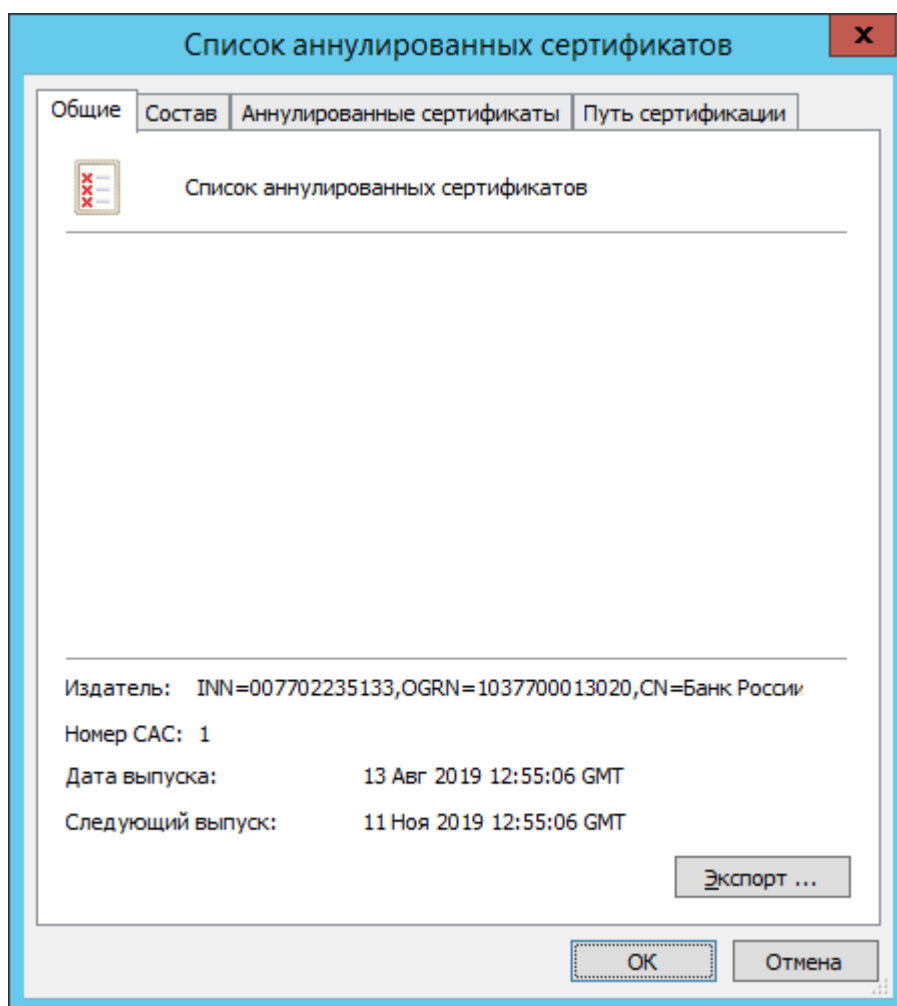



Рисунок 15 – Отображение САС

Для подтверждения загрузки нажмите кнопку «**ОК**».

6.7 Загрузка сертификатов и САС из каталога

Загрузка сертификатов и САС из каталога производится только на определённую сессию КС.

Для загрузки сертификатов и САС из каталога выберите нужную сессию и нажмите кнопку  на панели инструментов или выберите пункт меню «**Сервис**» – «**Загрузить сертификаты и САС из каталога**».

Для загрузки сертификатов и САС из каталога в кластер необходимо выбрать сессии из списка сессий кластера.

Далее появится диалог (Рисунок 16), предлагающий выбрать каталог, из которого будут загружены сертификаты и САС.

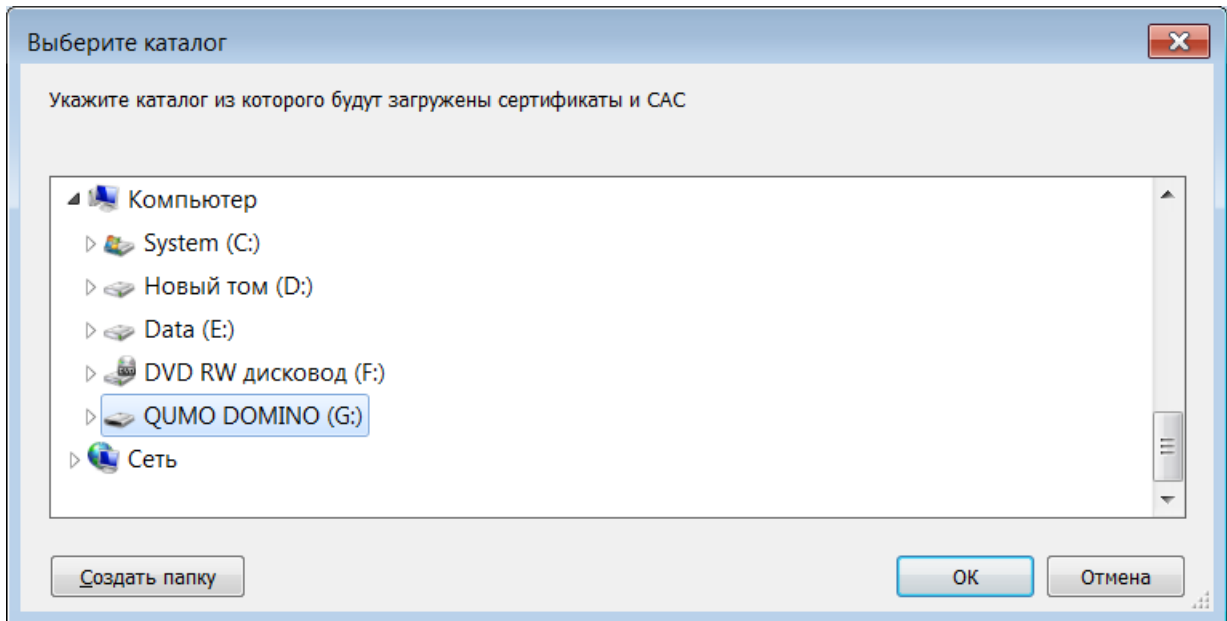



Рисунок 16 – Выбор каталога для загрузки сертификатов и САС

После окончания загрузки будет выдано сообщение о количестве загруженных сертификатов и САС.

6.8 Загрузка обновления

Загрузка обновлений производится только на определённую сессию КС. Для загрузки обновления выберите нужную сессию и нажмите кнопку  на панели инструментов или выберите пункт меню «Сервис» – «Загрузить обновление». Для загрузки обновления в кластер необходимо выбрать сессии из списка сессий кластера.

Далее появится файловый диалог (Рисунок 17), предлагающий выбрать файл с обновлением или несколько файлов с обновлением для загрузки.

Не допускается добавление сертификата с идентификатором ключа, если сертификат с таким же идентификатором ключа уже существует в базе сертификатов.

Примечание - При добавлении такого сертификата в DER-кодировке через простой интерфейс или через АРМ УКС выдается ошибка VCERT_E_TOO_MANY_CERTS_FOUND и сертификат не добавляется (в случае КС это сообщение протоколируется как «Фатальная ошибка»). При добавлении такого сертификата в составе обновления через простой интерфейс или через АРМ УКС сертификат не добавляется, однако обработка обновления продолжается (в случае КС добавляется в протокол фатальная ошибка с кодом VCERT_E_TOO_MANY_CERTS_FOUND).

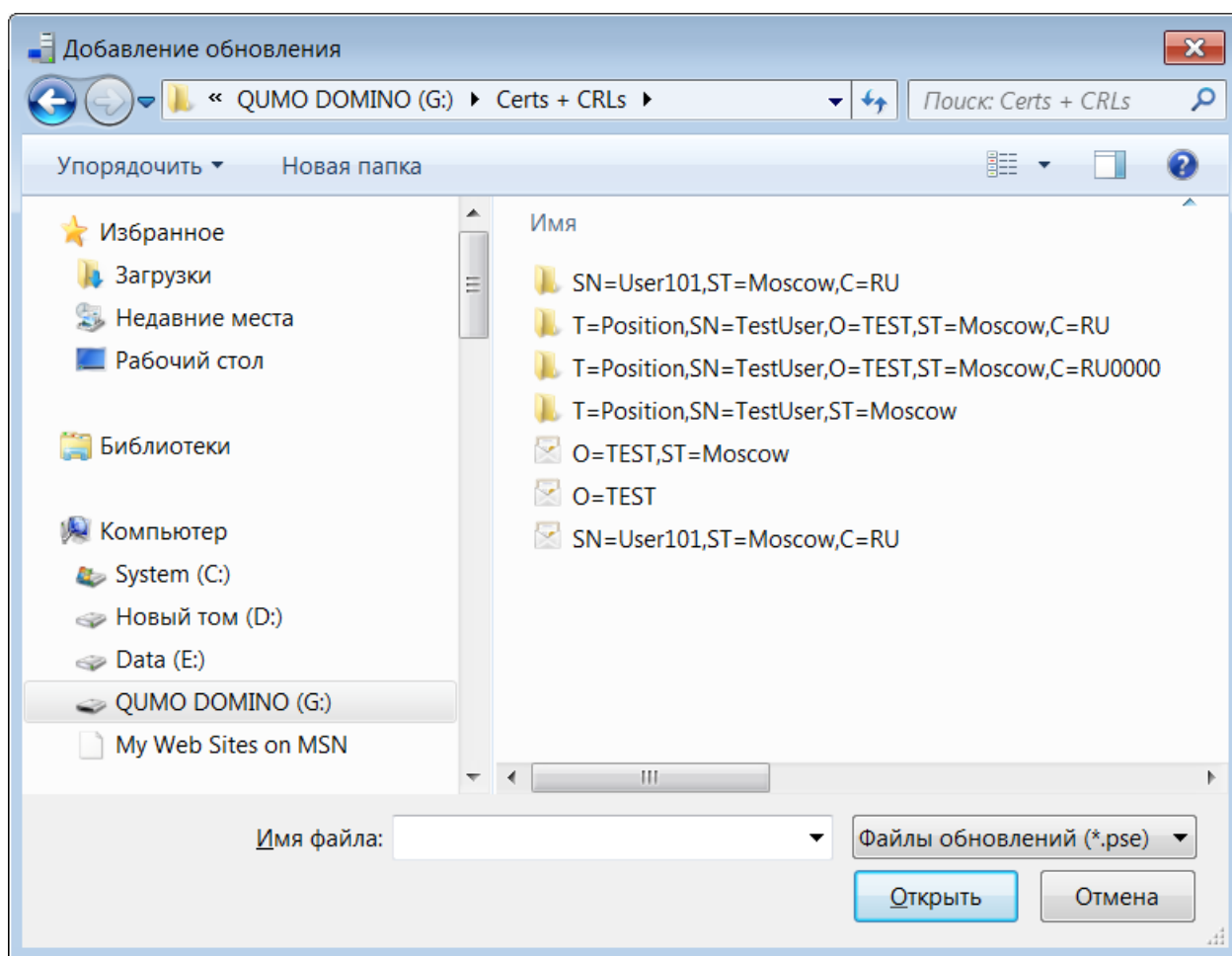


Рисунок 17 – Добавление обновления

Обновление выполняется непосредственно на КС.


6.9 Блокировка криптографической сессии

Для временного прекращения работы сессии можно выполнить блокировку сессии (блокировка сессии управления не допускается). При блокировке сессии все операции, связанные с использованием ключа ЭП, будут невозможны (такие операции как выполнение ЭП, расшифрование и шифрование). Такие операции как проверка ЭП и вычисление хэш-функции (не требующие ключа ЭП) будут выполняться. Для выполнения блокировки необходимо выбрать сессию из списка сессий и выбрать пункт меню «Сервис» – «Заблокировать работу сессии».

6.10 Разблокировка криптографической сессии

Для возобновления работы сессии необходимо выполнить разблокировку сессии. Для выполнения разблокировки нужно выбрать заблокированную сессию из списка сессий и выбрать пункт меню «Сервис» – «Разблокировать работу сессии».

6.11 Остановка криптографической сессии

Для прекращения работы сессии необходимо выполнить остановку сессии (остановка сессии управления не допускается). При остановке сессии все операции с сессией будут невозможны. Также будет выгружен ключ ЭП сессии. Для выполнения блокировки необходимо выбрать сессию из списка сессий и выбрать пункт меню «Сервис» – «Остановить работу сессии». После остановки сессии напротив сессии появится иконка  (Рисунок 18).

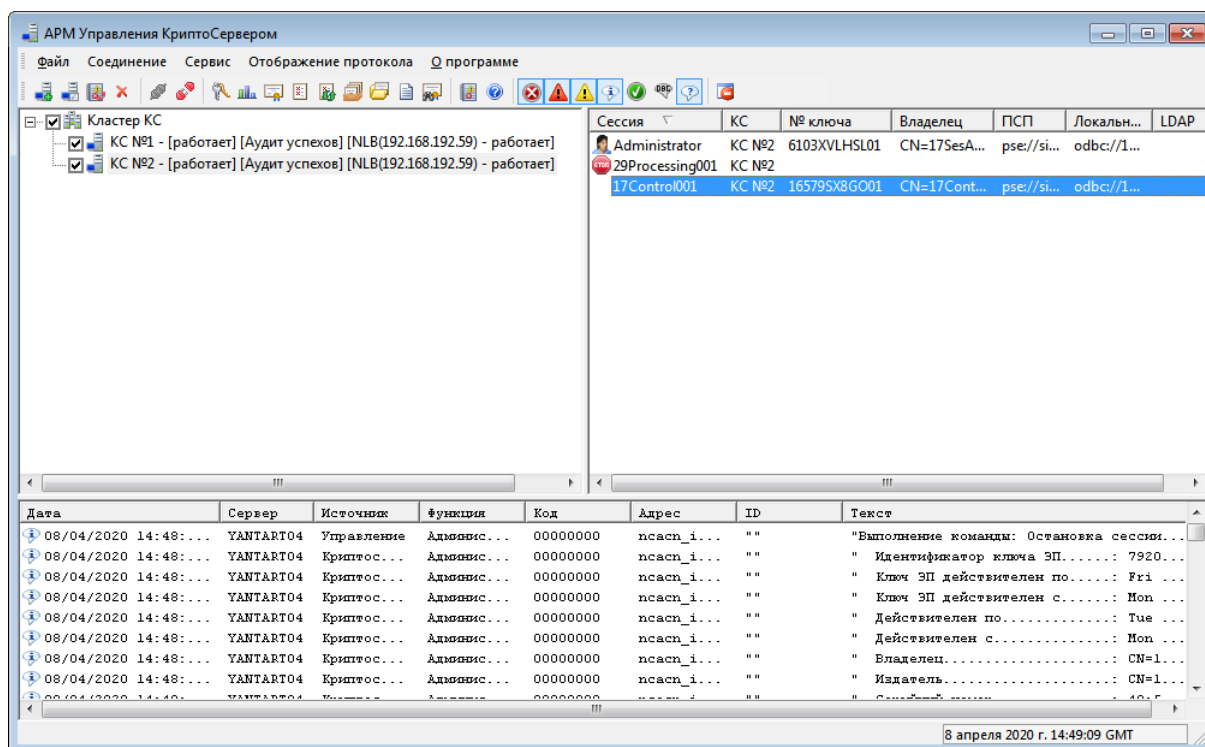






Рисунок 18 – Остановка сессии

6.12 Запуск криптографической сессии

Для запуска криптографической сессии которая была остановлена или не была запущена при старте КС (напротив сессии отображается иконка ) , необходимо выбрать остановленную сессию из списка сессий и выбрать пункт меню «Сервис» – «Стартовать работу сессии». После успешного запуска иконка с  сменится на  (ожидает загрузки ключа). После успешного выполнения загрузки ключа, криптографическая сессия перейдет в рабочее состояние.

6.13 Просмотр сертификатов криптографической сессии

Просмотр сертификатов производится только для определённой сессии КС. Для просмотра сертификатов выберите нужную сессию и нажмите кнопку  на панели инструментов или выберите пункт меню «Сервис» – «Посмотреть загруженные сертификаты».

Если сессия работает со справочником сертификатов через ODBC, то для получения списка сертификатов необходимо установить фильтр, чтобы избежать перекачивания большого объема информации (Рисунок 19). Для фильтрации

[illegible]

Далее появится диалоговое окно (Рисунок 20), показывающее список загруженных сертификатов и САС в соответствии с заданными условиями фильтра.

Для просмотра конкретного сертификата необходимо выбрать сертификат в списке и нажать кнопку «**Посмотреть**» или дважды щелкнуть «мышкой» по сертификату.

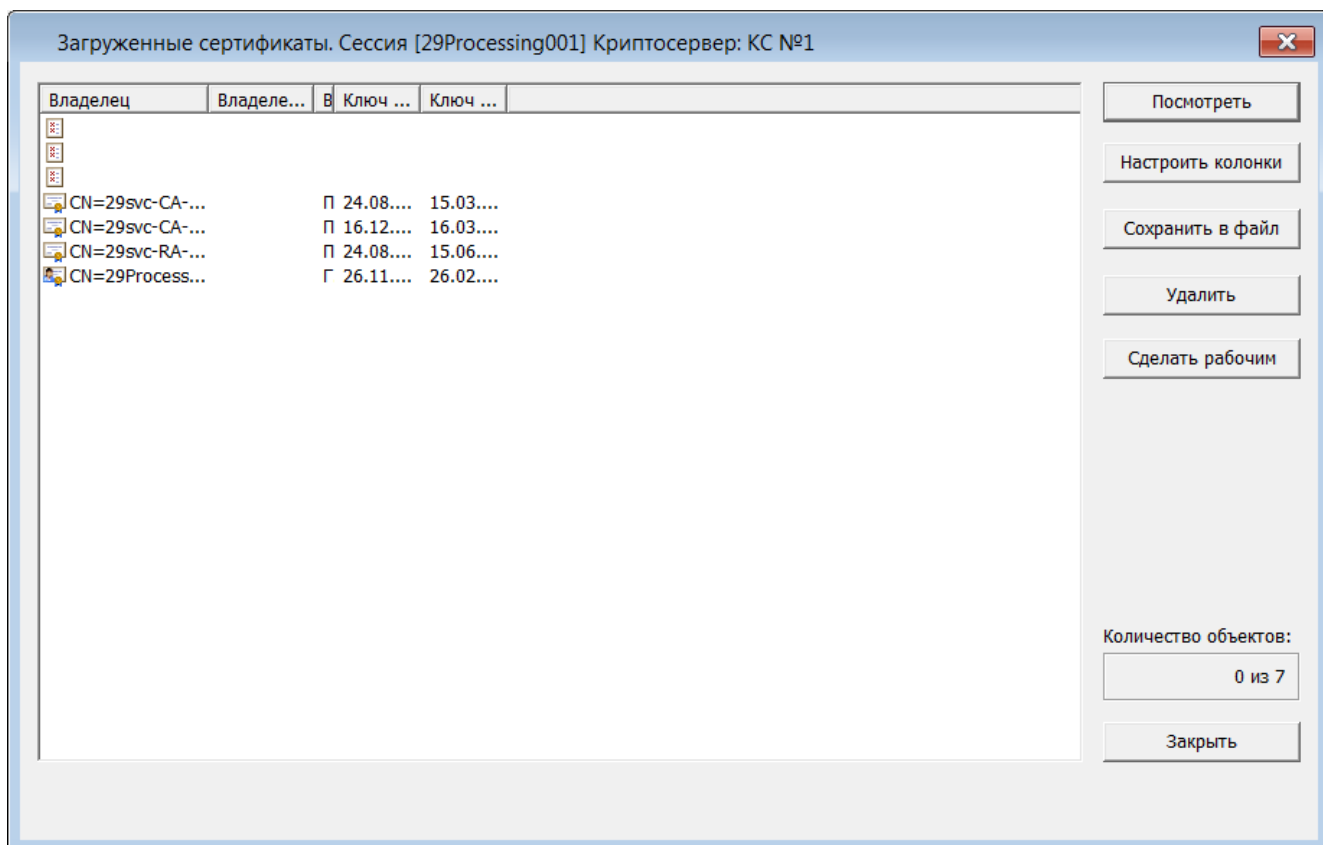


Рисунок 20 – Список загруженных сертификатов и САС

При просмотре сертификатов сессии кластера в случае отсутствия сертификата на одной из сессии кластера сертификат будет помечен иконкой жёлтого цвета и в статусной строке будет указано, на каком из серверов кластера отсутствует объект (Рисунок 21).

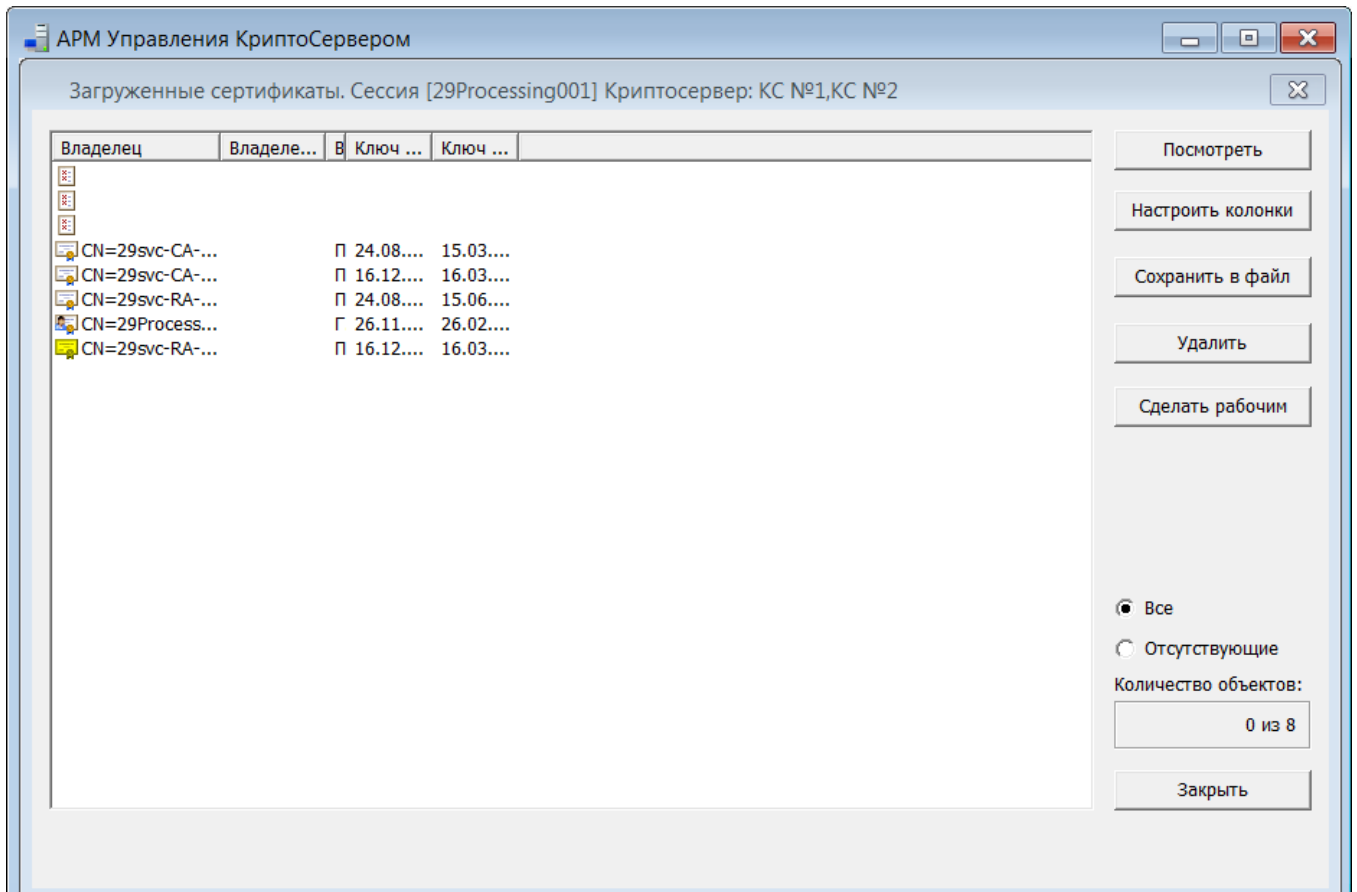


Рисунок 21 – Отсутствующий сертификат на одном из КС

Для просмотра только отсутствующих сертификатов необходимо выбрать опцию «**Отсутствующие**» (Рисунок 22).

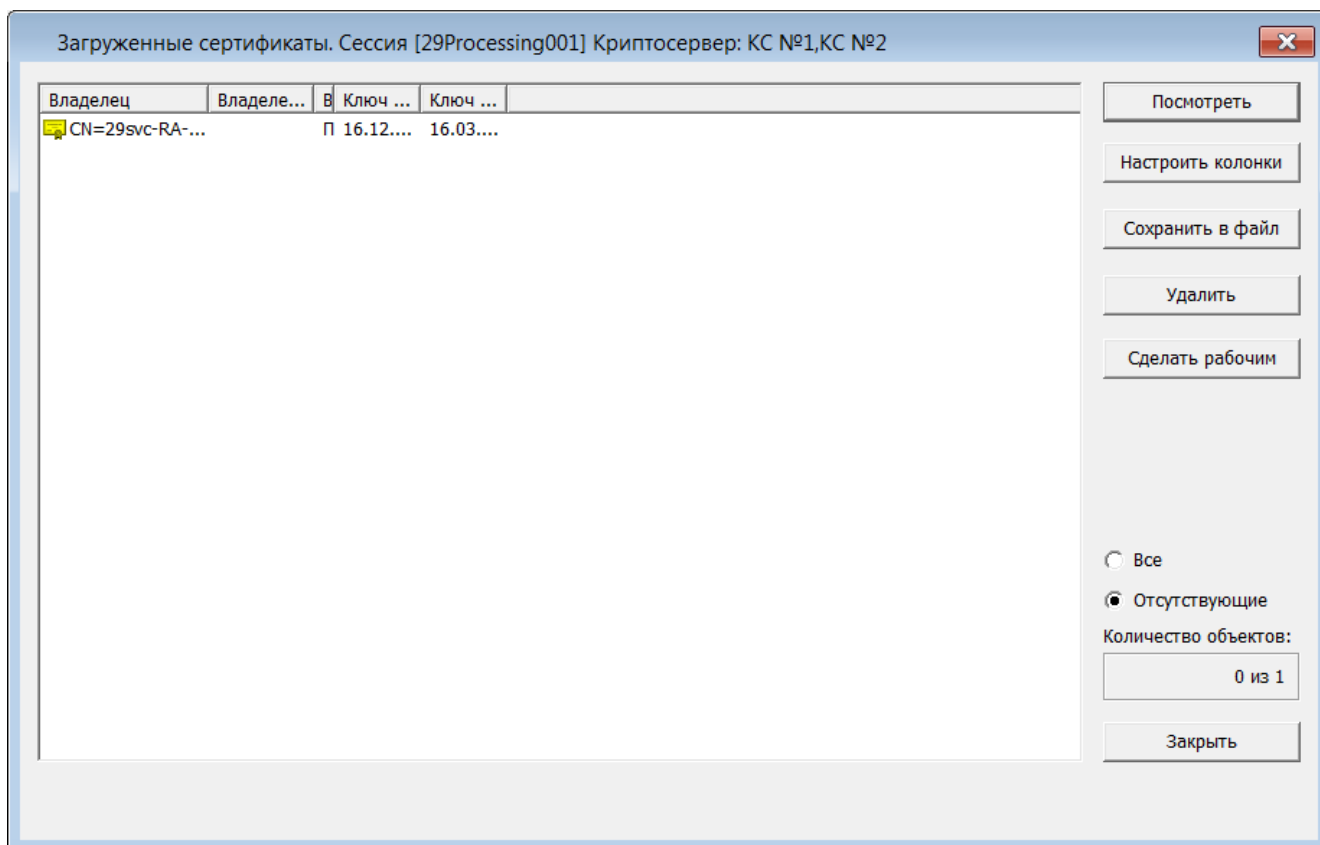


Рисунок 22 - Просмотр только отсутствующих сертификатов

6.14 Удаление сертификатов

Удаление сертификатов производится для выбранной сессии КС. Для удаления сертификата необходимо вызвать окно со списком загруженных сертификатов, т.е. выполнить действия, описанные в подразделе 6.13. Далее появится диалоговое окно со списком загруженных сертификатов (Рисунок 20). Для удаления нужно выделить сертификат или несколько сертификатов в списке и нажать кнопку «Удалить». Далее появляется запрос «Показывать сертификаты перед удалением?». Нажмите кнопку «Да», и каждый сертификат будет показываться перед удалением, и будет удалён только в случае, если при просмотре сертификата Администратор АРМ УКС нажмет кнопку «ОК». При попытке удаления личного сертификата сессии будет выдано предупреждение, что удалять сертификат сессии запрещено.

Примечание – Число отображаемых сертификатов ограничено настройкой АРМ УКС «Максимальное число сертификатов, получаемых при просмотре», описанной в разделе 8.

6.15 Удаление аннулированных/прекративших действие сертификатов из сессии криптосервера

Удаление аннулированных/прекративших действие сертификатов производится для выбранной сессии КС. Для удаления аннулированных/прекративших действие сертификатов выберите нужную сессию, после чего выберите пункт

меню «Сервис» – «Удалить аннулированные сертификаты».

Далее появится диалоговое окно (Рисунок 23), показывающее список аннулированных сертификатов в сессии.

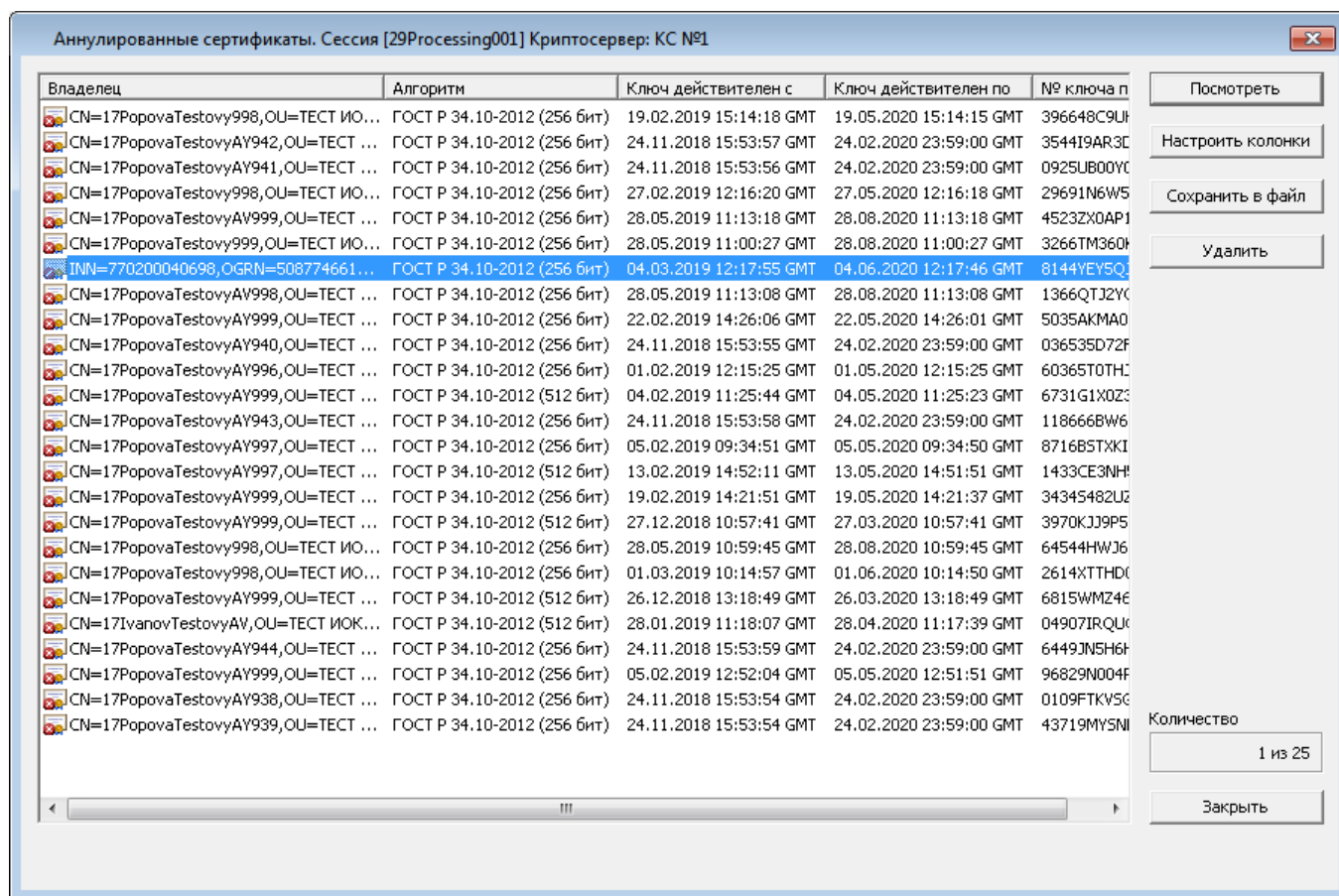


Рисунок 23 – Удаление аннулированных/прекративших действие сертификатов

Для удаления сертификатов необходимо выделить сертификат или несколько сертификатов в списке и нажать кнопку «Удалить».

Примечание – Число отображаемых аннулированных/прекративших действие сертификатов ограничено настройкой АРМ УКС «**Максимальное число сертификатов, получаемых при просмотре**», описанной в разделе 8. Если число аннулированных/прекративших действие сертификатов равно максимальному числу сертификатов, получаемых при просмотре, то после удаления необходимо команду «Сервис» – «Удалить аннулированные сертификаты» выполнить еще раз.

6.16 Удаление сертификатов с истекшими ключами из сессии криптосервера

Удаление сертификатов с истекшими ключами из сессии криптосервера производится для выбранной сессии КС. Для удаления сертификатов выберите нужную сессию, после чего выберите пункт меню «Сервис» – «Удалить истекшие сертификаты».

Далее появится диалоговое окно (Рисунок 24), показывающее список сертификатов с истекшими ключами в сессии.

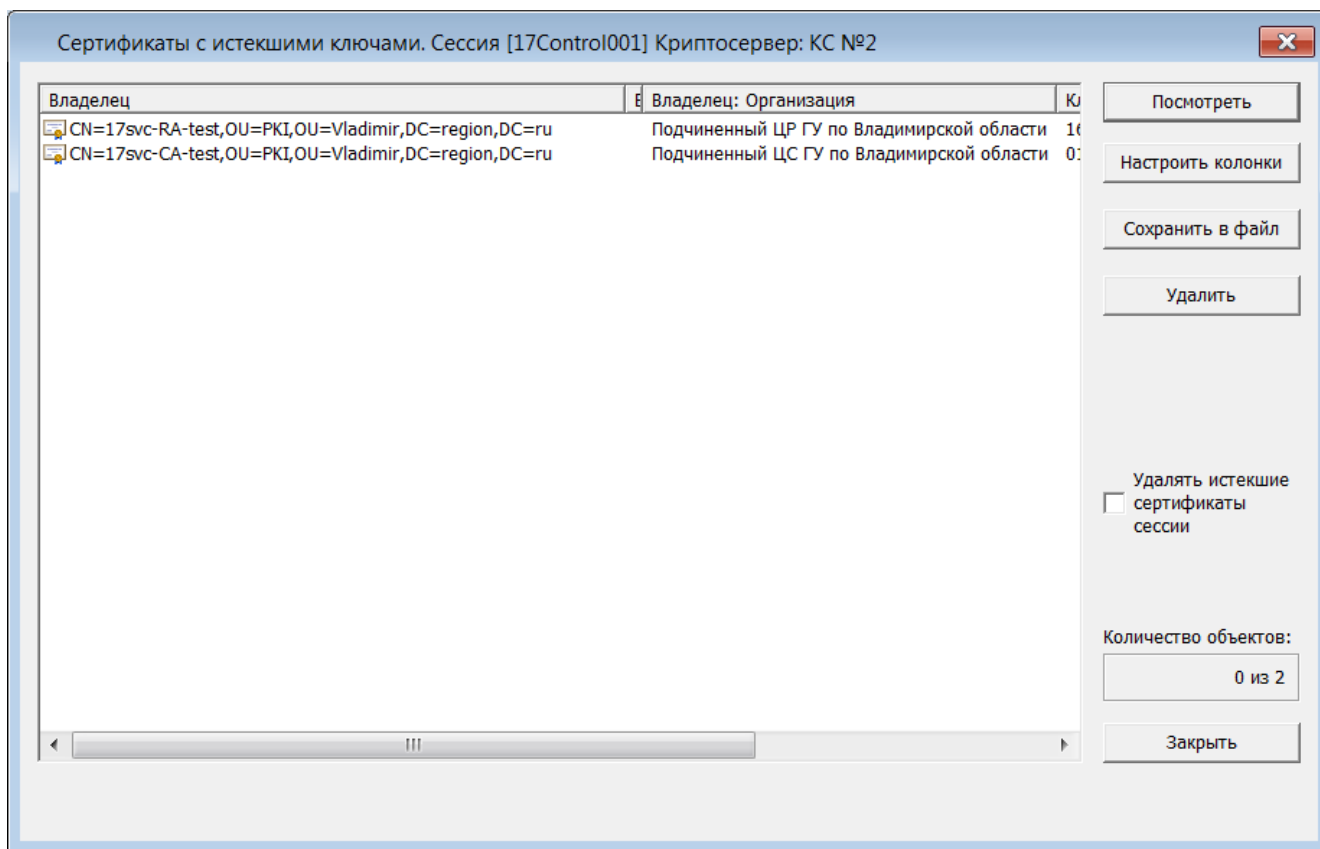


Рисунок 24 – Удаление сертификатов с истекшими ключами

Для удаления сертификатов необходимо выделить сертификат или несколько сертификатов в списке и нажать кнопку «**Удалить**».

Сертификаты Центра сертификации (ЦС) и Центра регистрации с истекшими ключами удалены не будут. Сертификаты сессии (**OID 1.3.6.1.4.1.10244.4.2.1**) с истекшими ключами будут удалены только в том случае, если отмечена опция «**Удалить истекшие сертификаты сессии**».

*Примечание – Число отображаемых сертификатов с истекшими ключами ограничено настройкой АРМ УКС «**Максимальное число сертификатов, получаемых при просмотре**», описанной в разделе 8. Если число сертификатов с истекшими ключами равно максимальному числу сертификатов, получаемых при просмотре, то после удаления необходимо команду «**Сервис**» – «**Удалить истекшие сертификаты**» выполнить еще раз.*

6.17 Настройка отображения списка сертификатов и САС

Для настройки отображения списка необходимо нажать кнопку «**Настроить колонки**». Далее появится диалоговое окно (Рисунок 25).

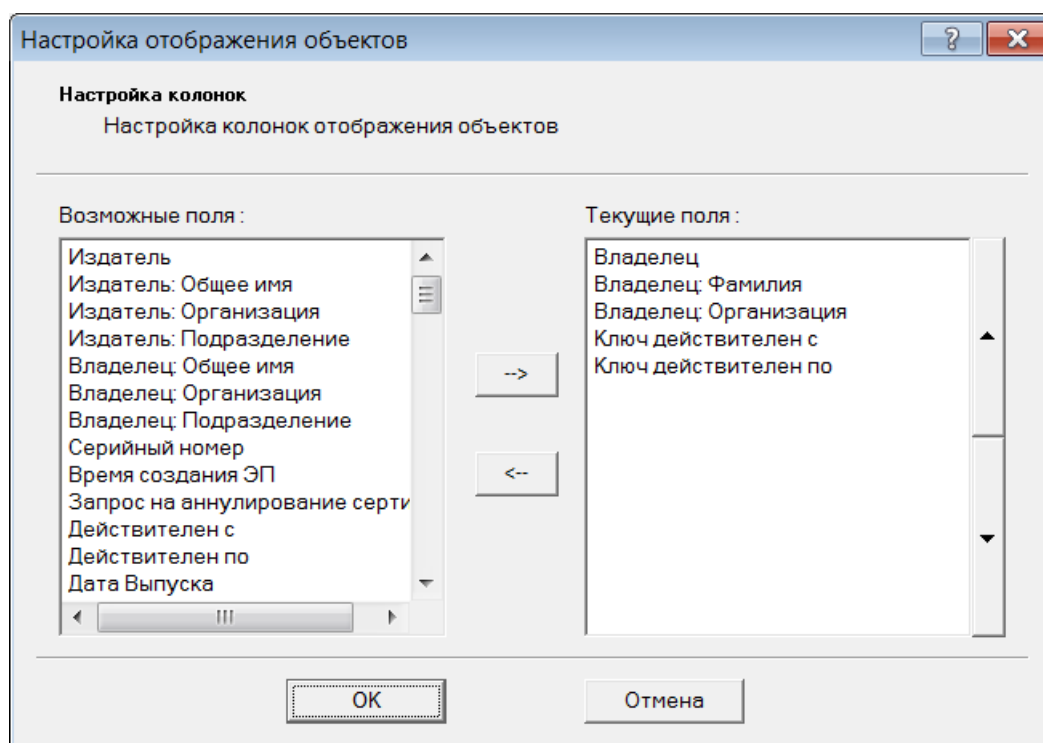


Рисунок 25 – Настройка колонок

Для настройки отображения пользователю предлагается выбрать поля (колонки), которые необходимо отображать. Окно содержит два списка «**Возможные поля**» и «**Текущие поля**». «**Возможные поля**» - это поля, которые можно выбрать для отображения. «**Текущие поля**» - это поля, которые отображаются в данный момент. Для добавления списка полей к текущим необходимо выделить все необходимые поля в списке «**Возможные поля**» и нажать кнопку «**->**». Выбранные поля появятся в списке «**Текущие поля**». Для удаления полей из списка «**Текущие поля**» необходимо выделить все необходимые поля в списке «**Текущие поля**» и нажать кнопку «**<-**». Для изменения порядка отображения используются кнопки, расположенные справа от списка «**Текущие поля**». Для изменения позиции поля в списке необходимо выбрать поле и нажать кнопку «**▲**» (вверх) или кнопку «**▼**» (вниз). Самое верхнее поле в списке «**Текущие поля**» отображается в интерфейсе как самая левая колонка, самое нижнее поле - как самая правая колонка.

6.18 Сохранение списка сертификатов и САС

Для сохранения списка необходимо нажать кнопку «**Сохранить в файл**» (Рисунок 20). Далее указать файл, в который будет сохранен отображаемый список. Сохранение списка производится в текстовом виде.

6.19 Установка нового рабочего сертификата


Установка нового рабочего сертификата производится только для определённой сессии КС. Перед установкой нового рабочего сертификата необходимо выполнить загрузку ключа ЭП сертификата, который собираетесь сделать рабочим. Загрузка ключа ЭП описана в подразделе 6.2. Для установки нового рабо-

чего сертификата необходимо вызвать окно со списком загруженных сертификатов, т.е. выполнить действия, описанные в п. 6.13. Далее появится диалоговое окно со списком загруженных сертификатов (Рисунок 20).

Для установки необходимо выбрать сертификат и нажать кнопку «Сделать рабочим».

6.20 Создание отчёта о загруженных объектах по сессии

Создание отчёта о загруженных объектах по сессии производится только для определённой сессии КС.

Для создания отчёта выберите нужную сессию и нажмите кнопку  на панели инструментов или выберите пункт меню «Сервис» – «Создать отчет о загруженных объектах по сессии».

Для создания отчёта по сессиям кластера необходимо выбрать сессии из списка сессий кластера.

Далее появится диалог (Рисунок 26), предлагающий выбрать каталог, в котором будут сформированы отчёты.

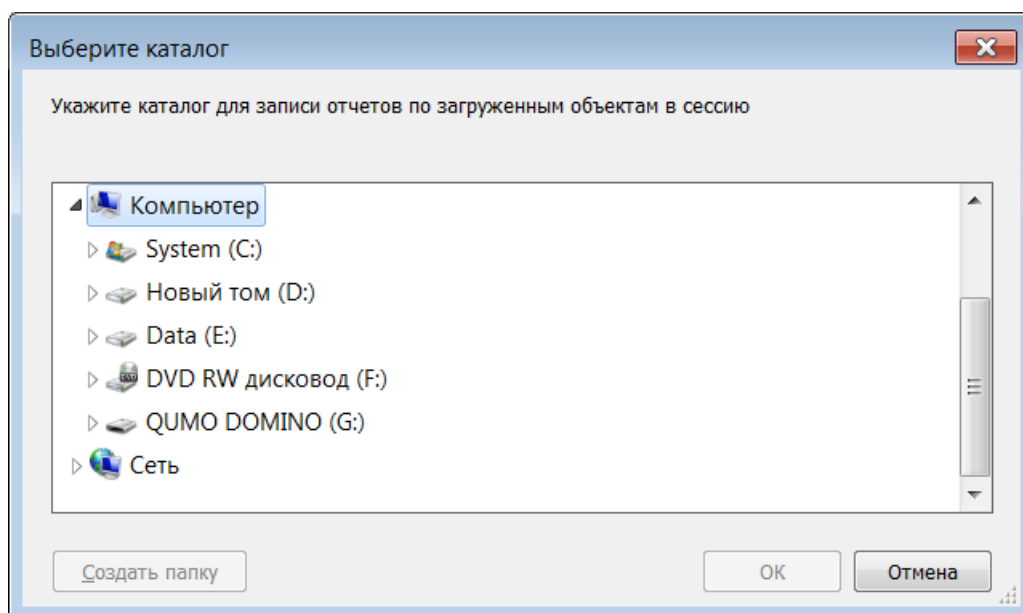


Рисунок 26 – Создание отчёта о загруженных объектах

Файлы отчётов сохраняются на жёстком диске в указанном каталоге в упакованном виде. Файлы имеют расширение .CAB. Для распаковки файла отчётов можно использовать команду **extrac32.exe [имя архива]**, входящую в состав операционной системы, или архиваторы WinRAR или WinZIP.

Для каждого подчинённого ЦС, сертификаты которого находятся в справочнике выбранной криптографической сессии указанного узла КС, создается один текстовый файл с информацией о сертификатах и САС, изданных данным подчинённым ЦС, а также информация о собственных сертификатах данного подчинённого ЦС.

Вместе с информацией о сертификатах и САС в файл записываются имя узла КС и имя криптографической сессии.

Для сертификата корневого ЦС, сертификаты которого находятся в справочнике выбранной криптографической сессии указанного узла КС, создается один

текстовый файл с информацией обо всех сертификатах подчинённых ЦС, их САС, САС корневого ЦС, всех сертификатов, выпущенных подчинёнными ЦС, и информация о сертификатах корневого ЦС.

Имя файла отчёта содержит имя ЦС (Subject Name), а также дату и время создания отчёта. Файл отчёта содержит следующие поля с информацией об объектах, разделённых знаком табуляции.

Для сертификатов:

- имя сертификата издателя;
- издатель. Описание;
- имя сертификата;
- ключ действителен с;
- ключ действителен по;
- сертификат действителен с;
- сертификат действителен по;
- № ключа подписи;
- X509 v3 расширенная область применения ключа;
- Владелец. Описание;
- Владелец. Организация;
- серийный номер сертификата;
- уровень ограничения иерархии;
- статус сертификата (действующий или отозванный).

Для САС:

- имя сертификата издателя;
- издатель. Описание;
- номер САС;
- количество отозванных сертификатов;
- следующий выпуск;
- № ключа подписи издателя.

Информация о сертификатах отсортирована по полю «**Ключ действителен с**».

6.21 Установка уровня протоколирования КС

Для установки уровня протоколирования КС Администратору АРМ УКС необходимо выбрать (отметить галочкой) из списка КС нужный КС (с которым установлено соединение) выбрать пункт меню «**Сервис**» – «**Установить уровень протоколирования**» и далее выбрать необходимый уровень протоколирования (Рисунок 27).

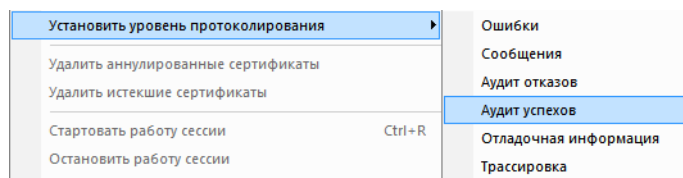


Рисунок 27 – Установка уровня протоколирования КС

После успешного выполнения команды по изменению уровня протоколирования КС, в строке КС будет отображен установленный уровень протоколирования (Рисунок 28).

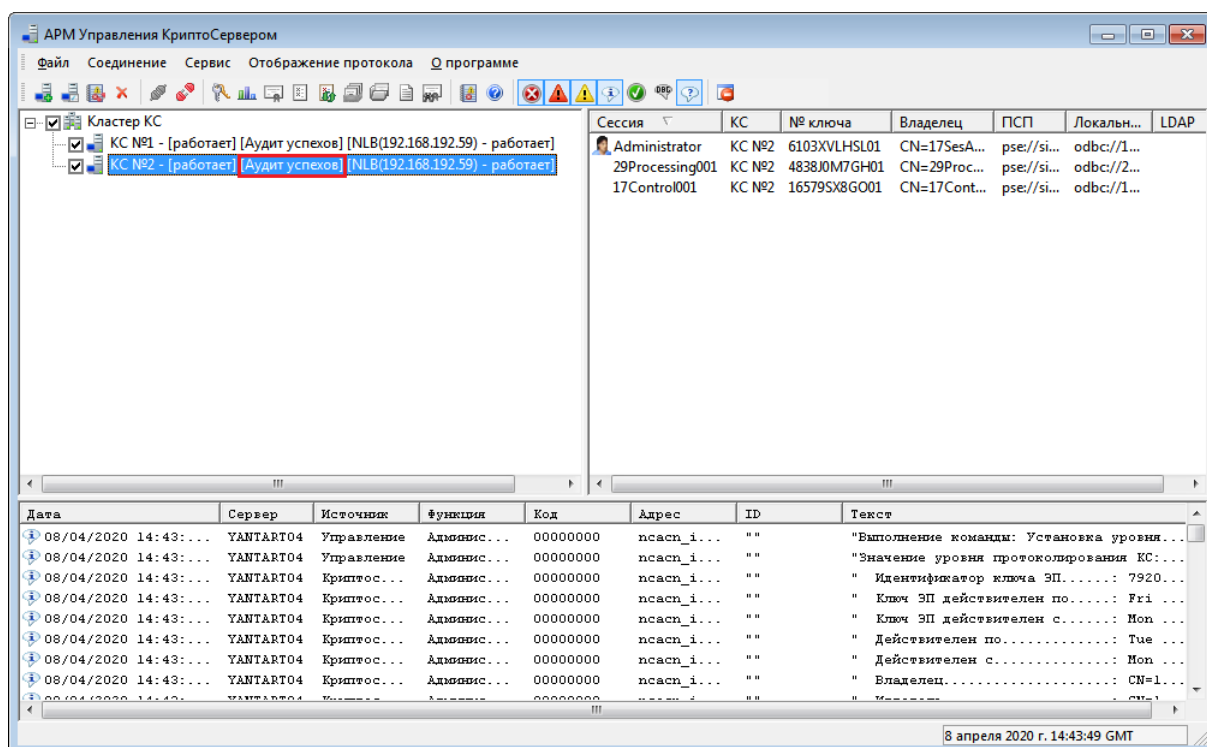



Рисунок 28 – Уровень протоколирования КС

6.22 Остановка отображения всплывающих окон

При настройке оповещения АРМ УКС посредством звуковой сигнализации на определенный тип событий в протоколе КС, АРМ УКС также отображает событие в диалоговом окне (Рисунок 29). Иногда данных окон может быть очень много. Для временного отключения оповещения посредством звуковой сигнализации и отображения диалоговых окон, необходимо нажать кнопку  на панели инструментов или выбрать пункт меню «Отображение протокола» – «Остановить отображение всплывающих окон» или нажать кнопку на отображаемом окне «Остановить отображение».

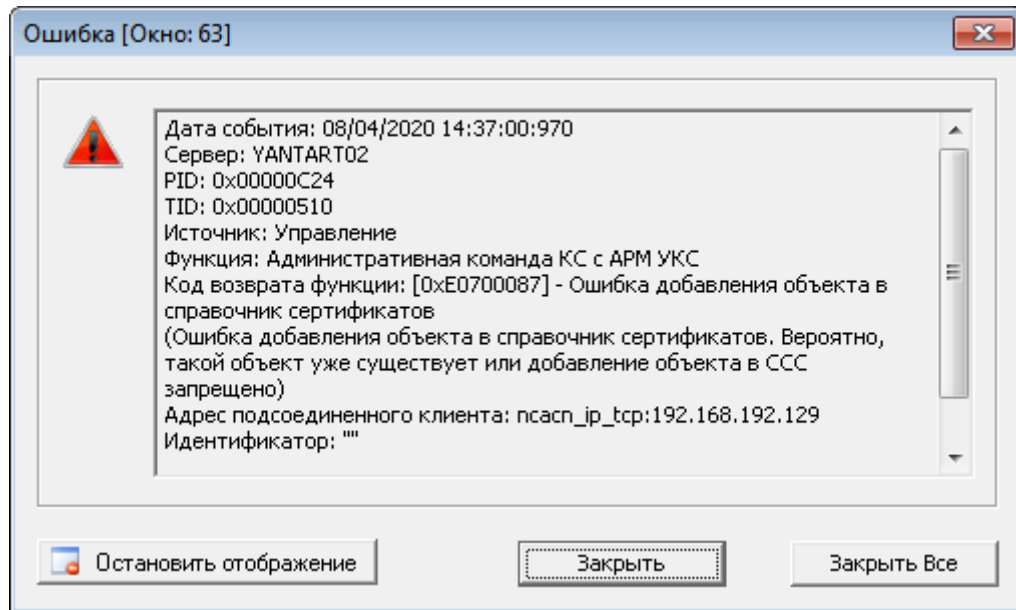




Рисунок 29 – Диалоговое окно оповещения о событии

Для возобновления оповещения посредством звуковой сигнализации и отображения диалоговых окон, необходимо отжать кнопку  на панели инструментов или выбрать пункт меню «**Отображение протокола**» – «**Остановить отображение всплывающих окон**» повторно.

7 ПРОСМОТР ПРОТОКОЛА РАБОТЫ АРМ УКС

Для просмотра протокола работы АРМ УКС нужно нажать кнопку  на панели инструментов или выбрать пункт меню «Сервис» – «Посмотреть протокол работы АРМ УКС».

Далее будет отображено окно просмотра протокола (Рисунок 30).

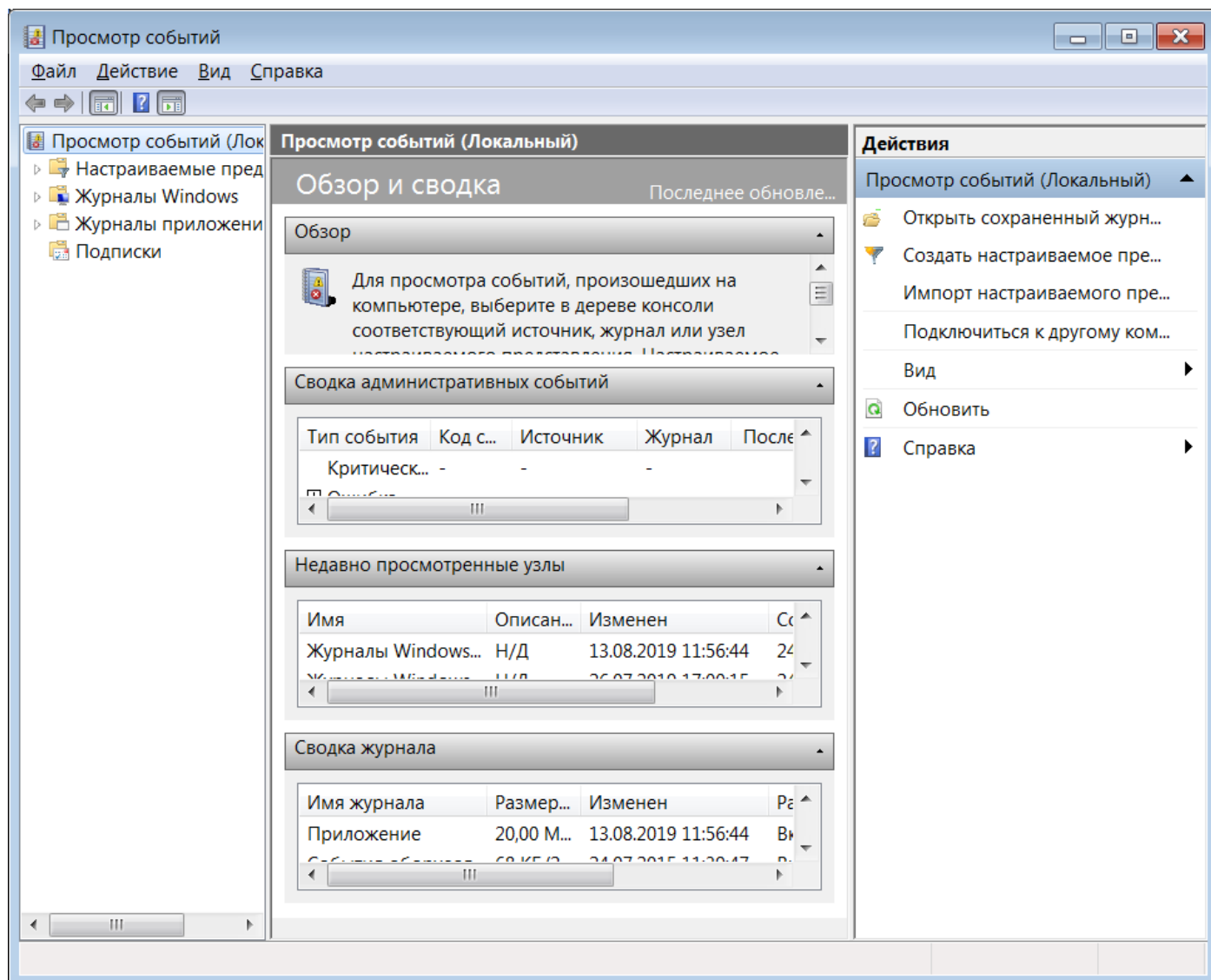


Рисунок 30 – Протокол работы АРМ УКС

Описание полей протокола и информации, содержащейся в них, можно посмотреть в документации на ОС Windows.

8 НАСТРОЙКА АРМ УКС

8.1 Общие настройки

Для настройки АРМ УКС выберите пункт меню «Сервис» – «Настроить АРМ УКС».

Далее будет отображено окно настройки АРМ УКС (Рисунок 31).

В этом окне можно установить следующие параметры:

- **Интервал для чтения протоколов** - интервал опроса КС по чтению протоколов (по умолчанию 5 сек.);
- **Предупреждать об истечении закрытого ключа сессии за** - за сколько дней будет выдаваться предупреждение об истечении закрытого ключа сессии КС. (по умолчанию 30 дней);
- **Максимальное число сертификатов, получаемых при просмотре** - максимальное количество сертификатов сессии, которое можно посмотреть с АРМ УКС (по умолчанию 20000);
- **Максимальное отображаемое число строк протокола** - максимальное число строк протокола КС, которые будет отображать АРМ УКС. В целях экономии оперативной памяти это значение рекомендуется уменьшать (по умолчанию 20000);
- **Интервал для опроса статуса NLB** - интервал, через который будет обновляться статус кластера NLB (по умолчанию 120 секунд). Не рекомендуется ставить данный интервал очень маленьким, так как эта процедура занимает некоторое время и может сказаться на производительности АРМ УКС;
- **Читать только протокол ошибок, если фильтруются только ошибки** - данная опция позволяет читать только протокол ошибок (и не читать общий протокол КС) когда установлена фильтрация по типу события только «**Фатальная ошибка**» и/или «**Ошибка**», что позволяет снизить нагрузку на АРМ УКС при чтении протоколов КС.

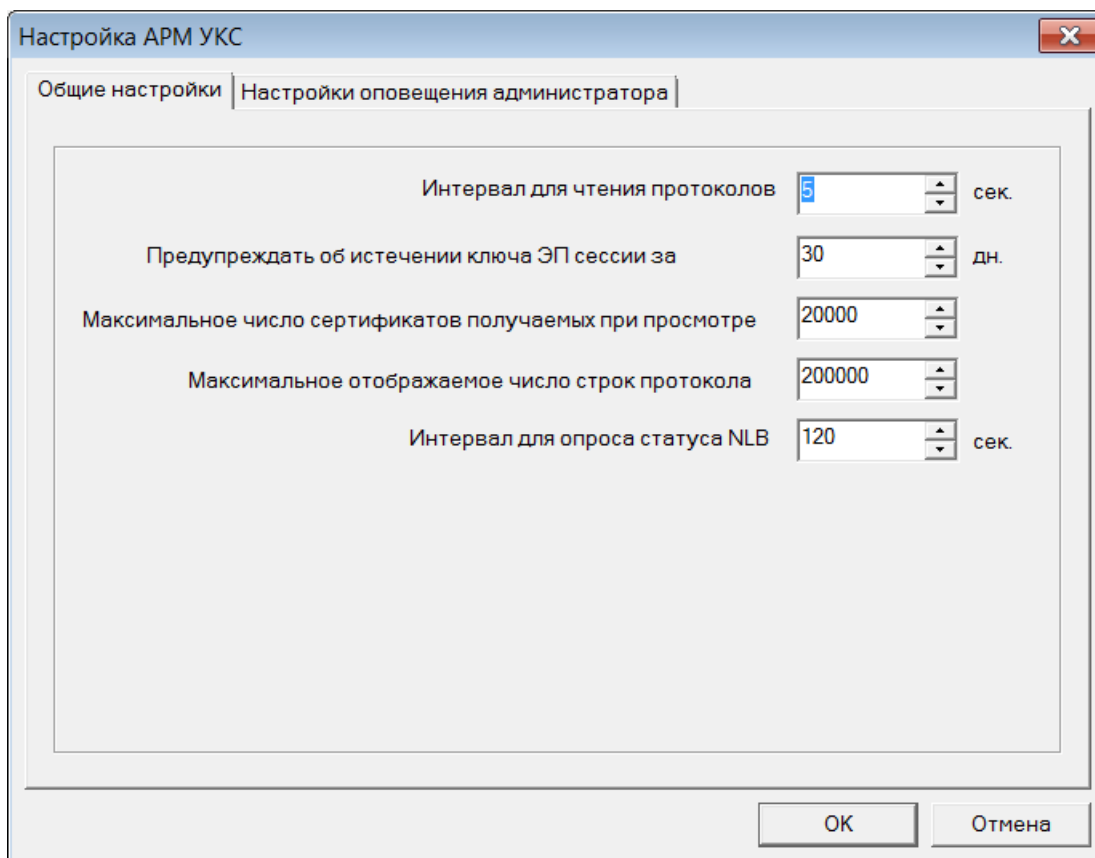


Рисунок 31 – Окно настройки АРМ УКС

8.2 Настройки оповещения

На закладке «**Настройки оповещения администратора**» (Рисунок 32) выполняется настройка методов оповещения Администратора АРМ УКС для каждого типа событий. Оповещение производится следующими способами:

- SNMP;
- посредством звуковой сигнализации.

Для установки оповещения необходимо напротив типа события установить значение «**ДА**» для способа оповещения.

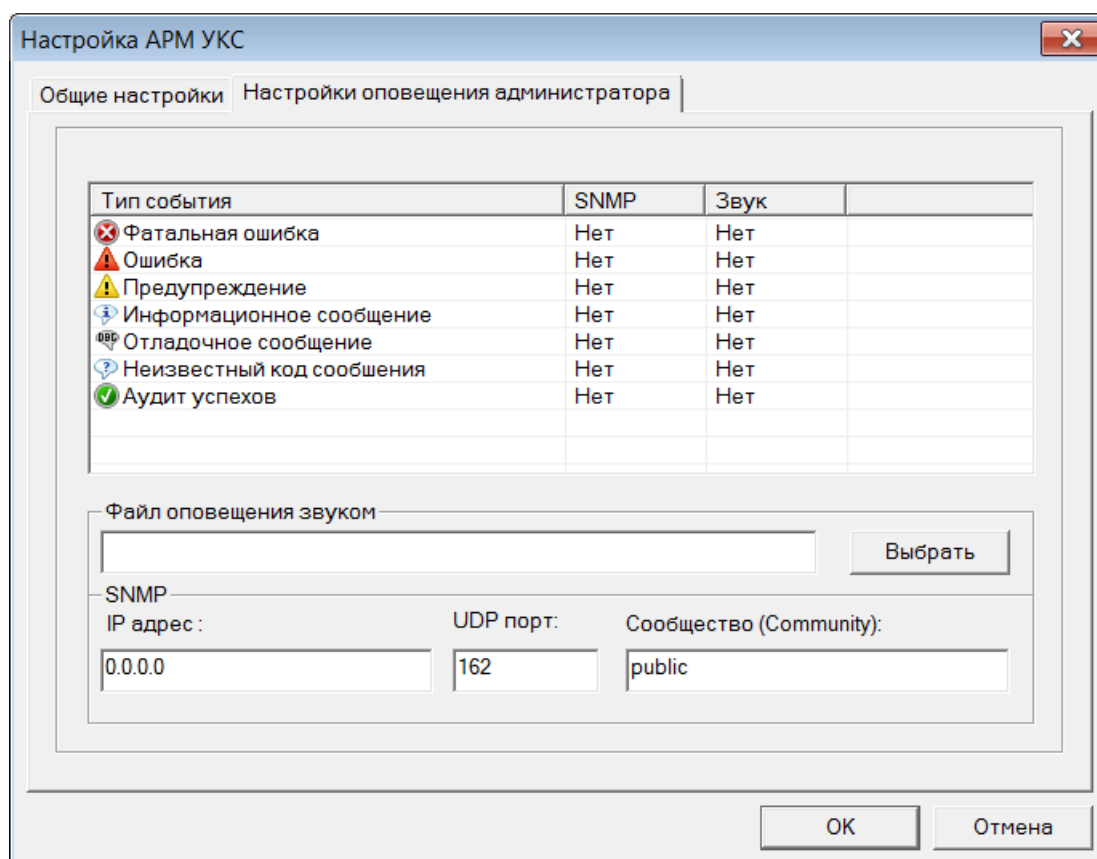


Рисунок 32 – Настройка оповещения Администратора АРМ УКС

При оповещении по SNMP на указанный IP-адрес и порт высылается SNMP-сообщение со строкой протокола, если тип события совпадает с настройками оповещения.

При оповещении звуком, в случае если тип события совпадает с настройками оповещения, выводится диалоговое окно с просмотром строки протокола (Рисунок 6). Например, проигрывается звуковое сообщение, указанное в настройке.

8.3 Установка больших кнопок на панели инструментов АРМ УКС

Для установки больших кнопок на панели инструментов нужно выбрать пункт меню «Сервис» – «**Большие кнопки панели инструментов**». Если установлена галочка напротив этого пункта, то отображаются большие кнопки на панели инструментов (Рисунок 33), если не установлена, то - маленькие.

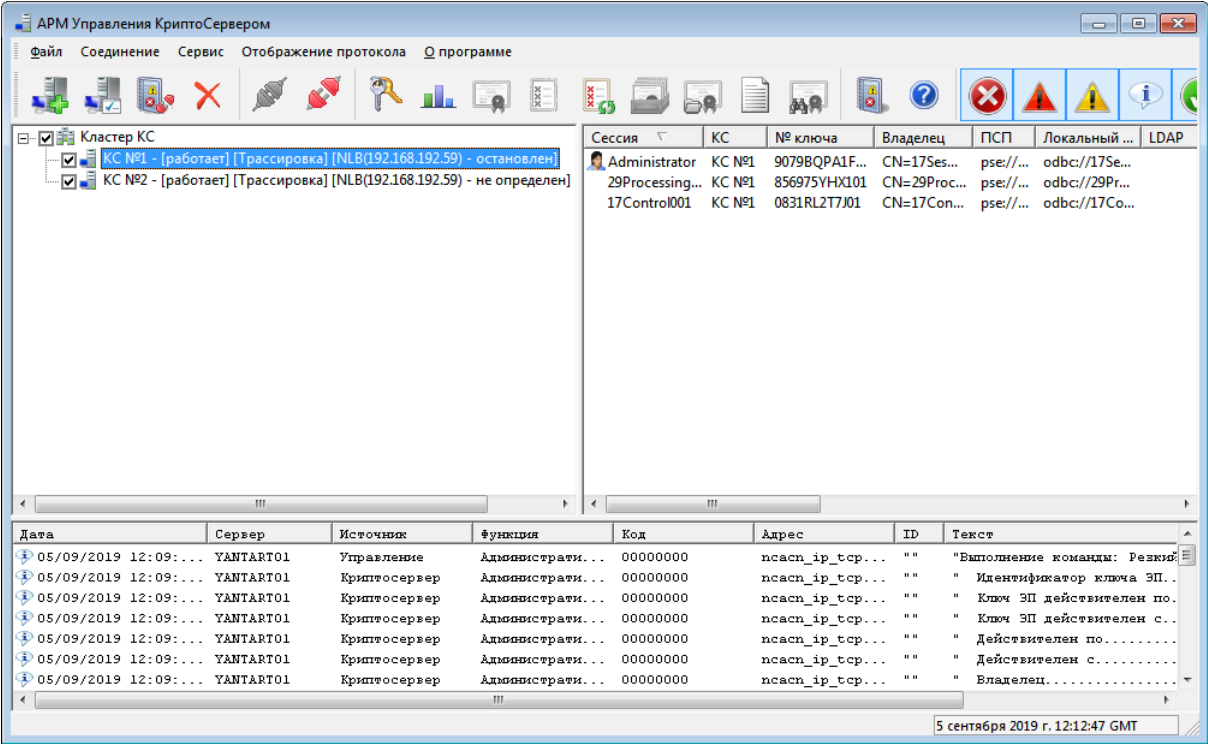


Рисунок 33 – Большие кнопки панели инструментов

9 ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИИ

9.1 Получение описания ошибки по коду ошибки

Для получения информации об ошибке по ее коду нужно выбрать пункт меню «Сервис» – «Получить описание ошибки по коду». Далее откроется диалоговое окно для ввода кода ошибки (Рисунок 34).

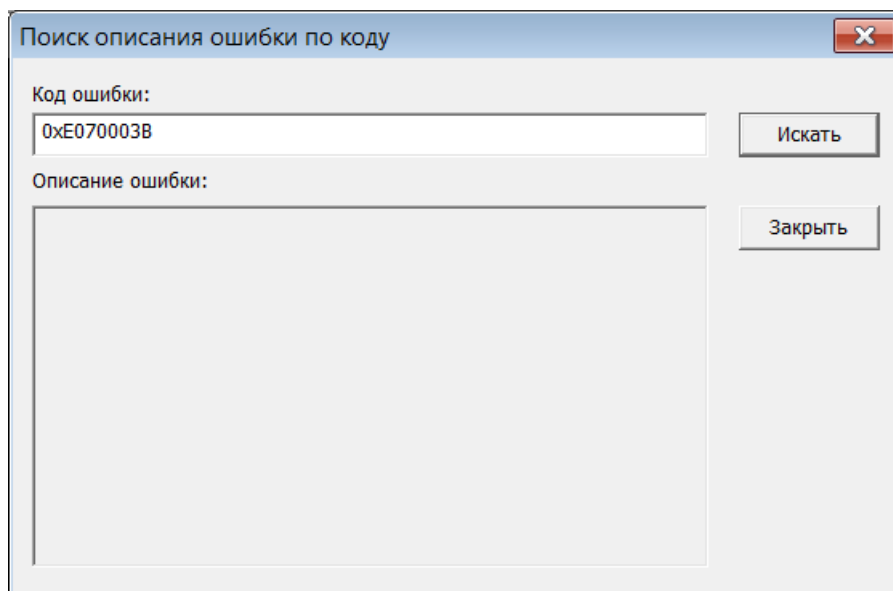


Рисунок 34 – Ввод кода ошибки для получения описания

После ввода кода ошибки нужно нажать кнопку «Искать», после чего в поле «Описание ошибки» будет отображено ее описание (Рисунок 35).

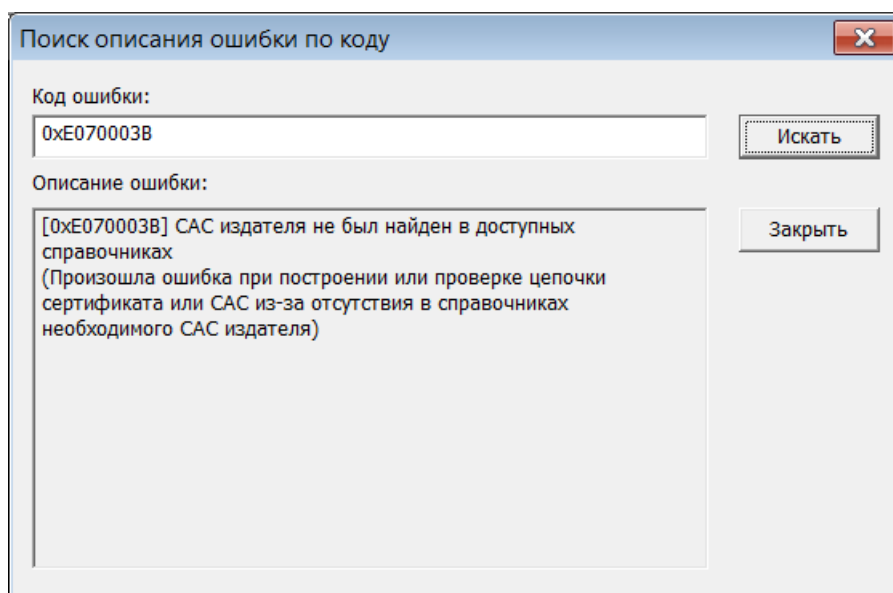


Рисунок 35 – Отображение описания ошибки

9.2 Управление авторизацией сессий

Управление авторизацией сессии производится только для определённой сессии КС.

Для настройки авторизации сессии выберите нужную сессию, после чего выберите пункт меню «Сервис» – «Управление авторизацией сессий» (Рисунок 36).

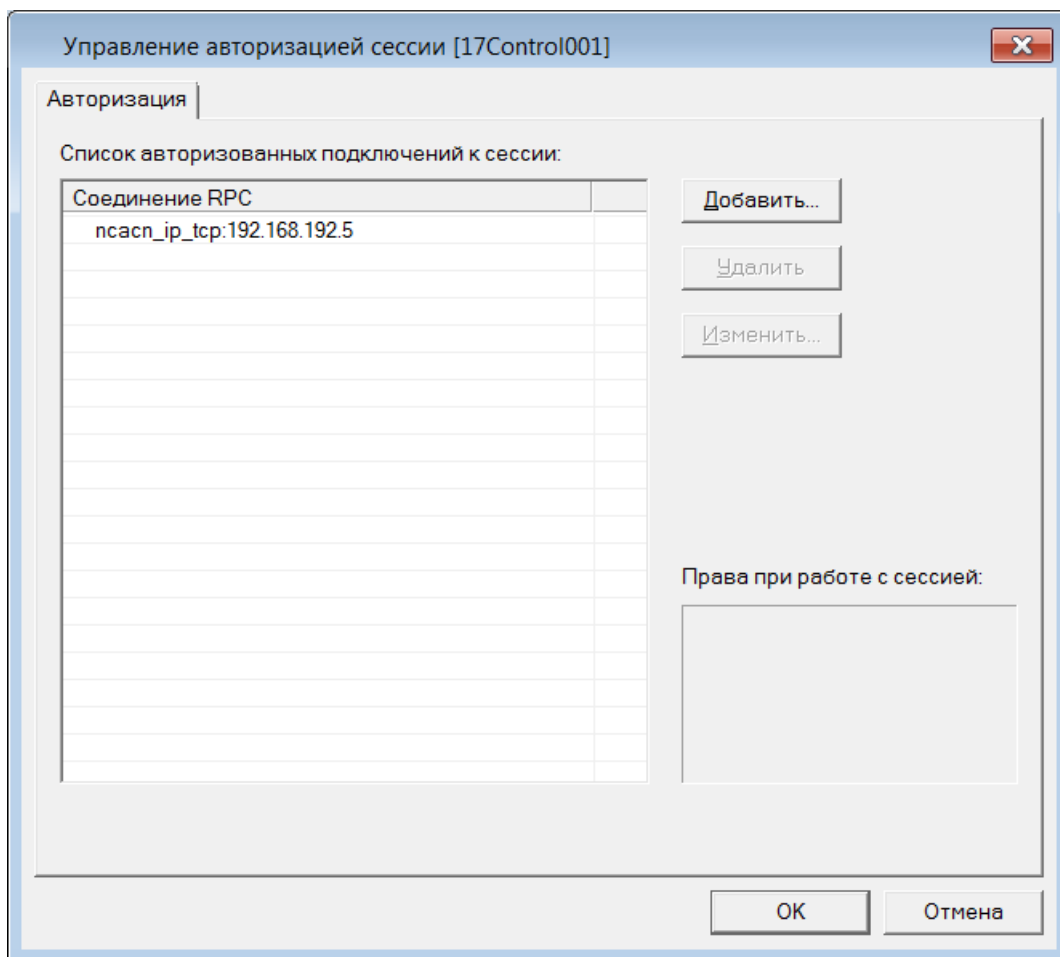
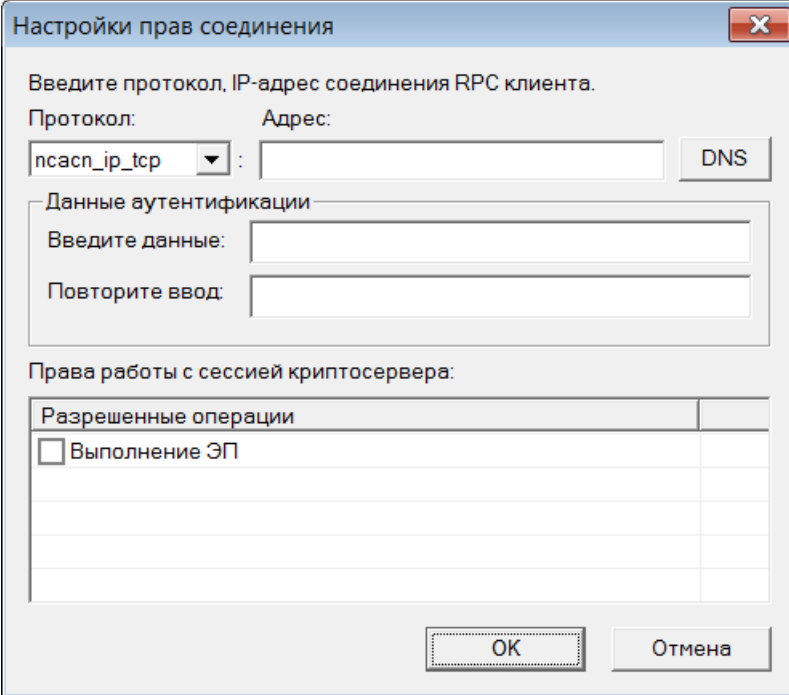


Рисунок 36 – Управление авторизацией сессии

Для добавления новой записи в список авторизации нужно нажать кнопку «**Добавить**», далее отобразится диалоговое окно (Рисунок 37) для добавления новой записи. Для удаления записей нужно выделить записи в списке «**Соединение RPC**» и нажать кнопку «**Удалить**», после чего подтвердить действие в соответствующем диалоге. Для изменения записи (например, для смены пароля авторизации) нужно выделить требуемую запись и нажать кнопку «**Изменить**» (Рисунок 36). Далее отобразится диалог, в котором можно изменить параметры авторизации (Рисунок 38).



Настройки прав соединения

Введите протокол, IP-адрес соединения RPC клиента.

Протокол: Адрес:

ncascp_ip_tcp : DNS

Данные аутентификации

Введите данные:

Повторите ввод:

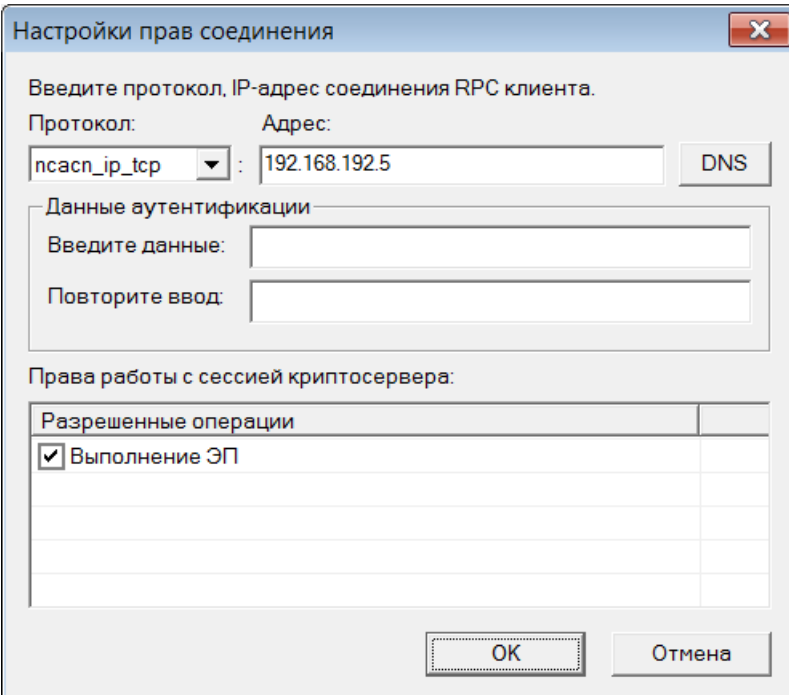
Права работы с сессией криптосервера:

Разрешенные операции	
<input type="checkbox"/> Выполнение ЭП	

OK Отмена

Рисунок 37 - Добавление записи авторизации

При управлении авторизацией кластерной сессии (сессии, которая присутствует на нескольких узлах кластера) в случае, если запись авторизации отсутствует для какой-либо сессии КС, такая запись отмечается иконкой с восклицательным знаком в красном треугольнике. Для того чтобы исправить рассинхронизацию, необходимо выделить проблемную запись и нажать кнопку «**Изменить**», далее установить новый пароль и нажать кнопку «**ОК**». Запись будет добавлена на все узлы кластера.



Настройки прав соединения

Введите протокол, IP-адрес соединения RPC клиента.

Протокол: Адрес:

ncascp_ip_tcp : 192.168.192.5 DNS

Данные аутентификации

Введите данные:

Повторите ввод:

Права работы с сессией криптосервера:

Разрешенные операции	
<input checked="" type="checkbox"/> Выполнение ЭП	

OK Отмена

Рисунок 38 - Изменение записи авторизации

10 ЗАВЕРШЕНИЕ РАБОТЫ НА АРМ УКС

Для завершения работы с АРМ УКС в основном окне программы нужно выбрать пункт меню «**Файл**» – «**Выход**».

После этого соединения с КС будут разорваны и будет выгружен ключ ЭП Администратора АРМ УКС.

11 АНАЛИЗ ПРОТОКОЛОВ КС

Программа «АРМ формирования отчётов» (АРМ ФО) входит в состав СКЗИ «Валидата Криптосервер» и предназначена для преобразования протоколов КС в формат базы данных MS SQL или ORACLE с целью дальнейшей фильтрации, выполнения запросов и просмотра отчётов.

11.1 Запуск АРМ ФО и выход из него

Для запуска АРМ ФО выберите пункт системного меню «Программы» – «СКЗИ Валидата Криптосервер. Версия 4.0» – «АРМ ФО». После этого появится главное окно программы (Рисунок 39).

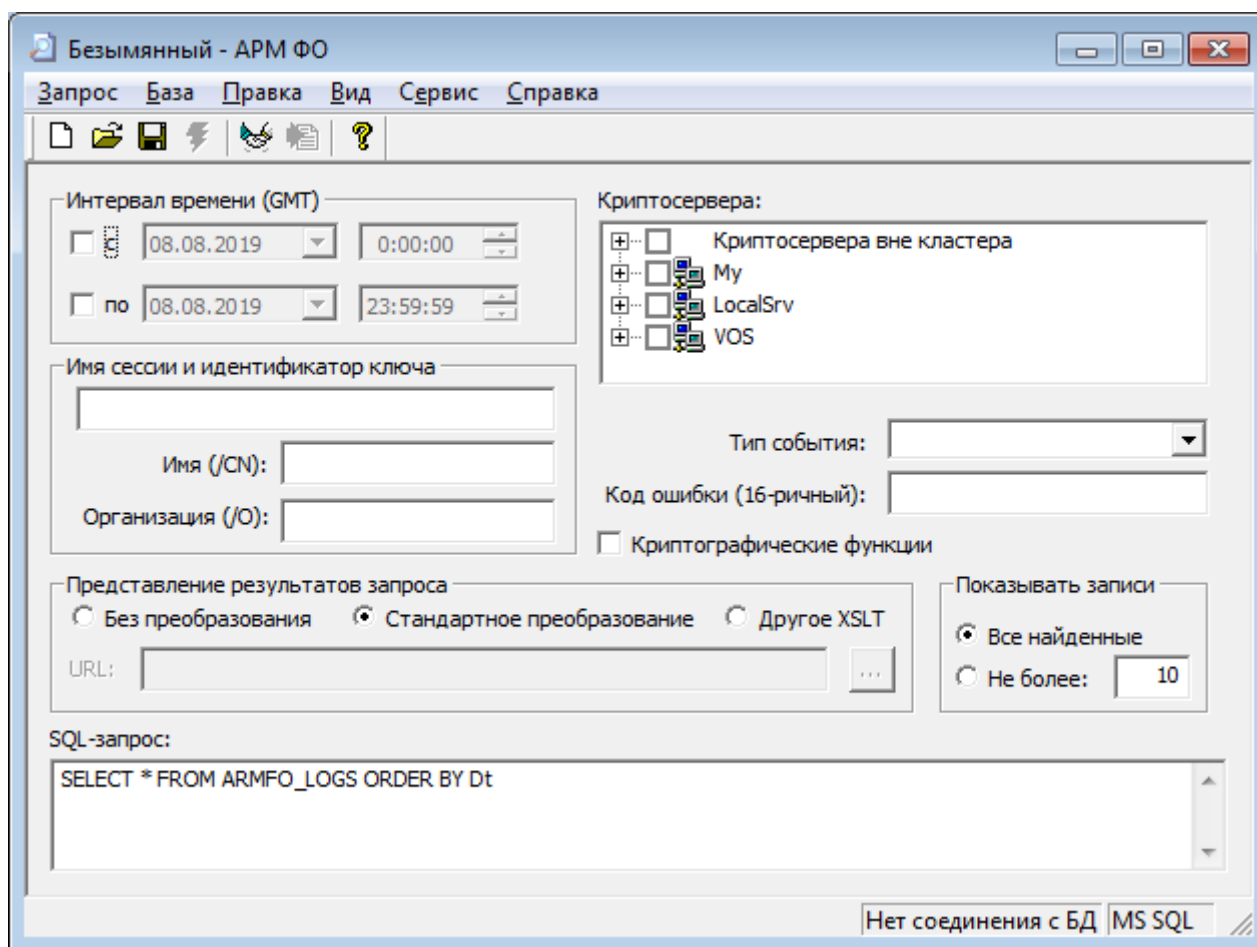


Рисунок 39 – Главное окно АРМ ФО

Для выхода из программы АРМ ФО выберите пункт меню «Запрос» – «Выход» или воспользуйтесь одним из стандартных способов завершения программ в ОС Windows.

11.2 Подключение к базе данных

Прежде чем подключиться к базе данных (БД), надо создать источник данных ODBC и настроить параметры подключения АРМ ФО к этому источнику.

Для создания источника данных воспользуйтесь стандартным Администратором источников данных ODBC (Рисунок 40).

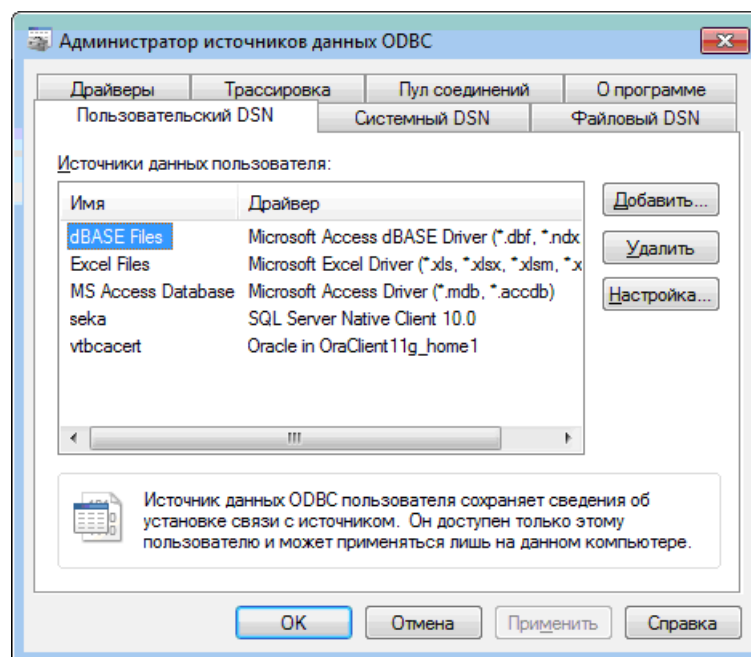


Рисунок 40 – Администратор источников данных ODBC

Предупреждение - Разрядность используемого Администратора источников данных ODBC (x64 или x86) должна совпадать с разрядностью АРМ ФО.

Для настройки параметров подключения АРМ ФО выберите пункт меню «База» – «Настроить», при этом на экране появляется окно настройки (Рисунок 41).

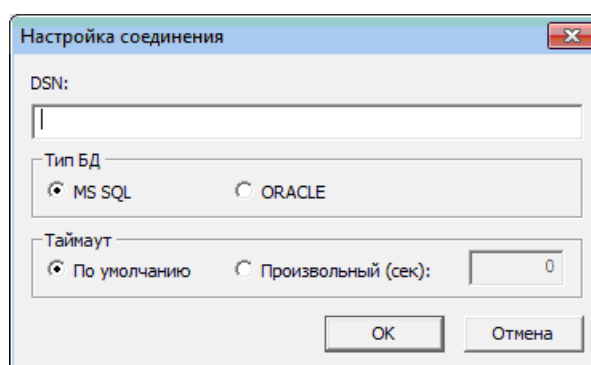



Рисунок 41 – Диалог настройки соединения с БД

Выберите тип используемой БД и укажите существующий источник данных ODBC.

В этом же диалоге можно изменить значение таймаута на выполнение SQL-запроса. В случае, если при выполнении запроса к БД (поиск или очистка записей) возникает ошибка «**Время ожидания истекло**», переключитесь на режим

«**Произвольный**» и задайте увеличенный таймаут – несколько десятков или сотен секунд, подбирается экспериментально.

После того, как настройка произведена, для соединения с БД выберите пункт меню «**База**» – «**Соединиться**» или нажмите кнопку  на панели инструментов. Если до этого соединение не было настроено, на экране появится стандартный диалог выбора источника данных ODBC, в котором можно выбрать существующий или создать новый источник данных (Рисунок 42).

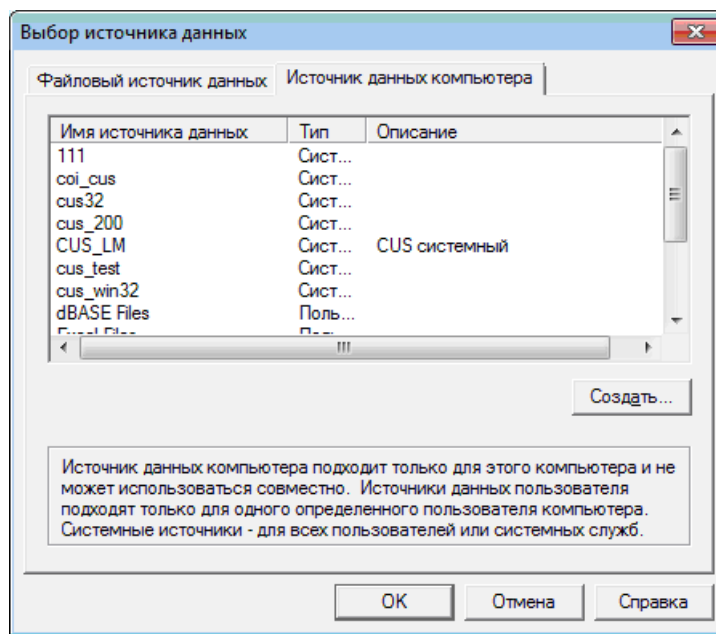


Рисунок 42 – Диалог выбора источника данных ODBC

Если тип выбранного источника данных не соответствует типу, заданному в настройках, соединение не будет установлено и будет выдано сообщение об ошибке (Рисунок 43).

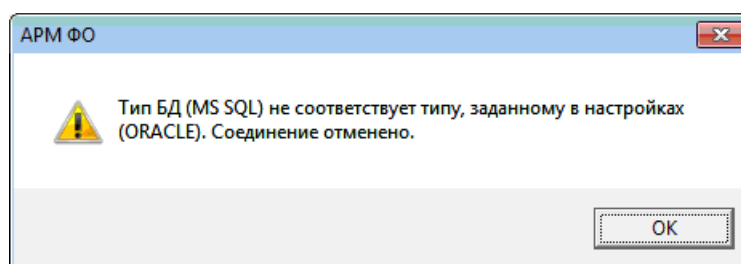


Рисунок 43 – Сообщение о несовпадении типов БД в источнике данных и в настройке

Если соединение с базой выполнилось успешно, вид панели инструментов изменится, кнопка «Соединиться» станет недоступной, а кнопки «Выполнить запрос» и «Импортировать протоколы» – доступными. Кроме того, в нижнем правом углу появится информация о типе БД, к которой подключён АРМ ФО и имя соответствующего источника данных (Рисунок 44).

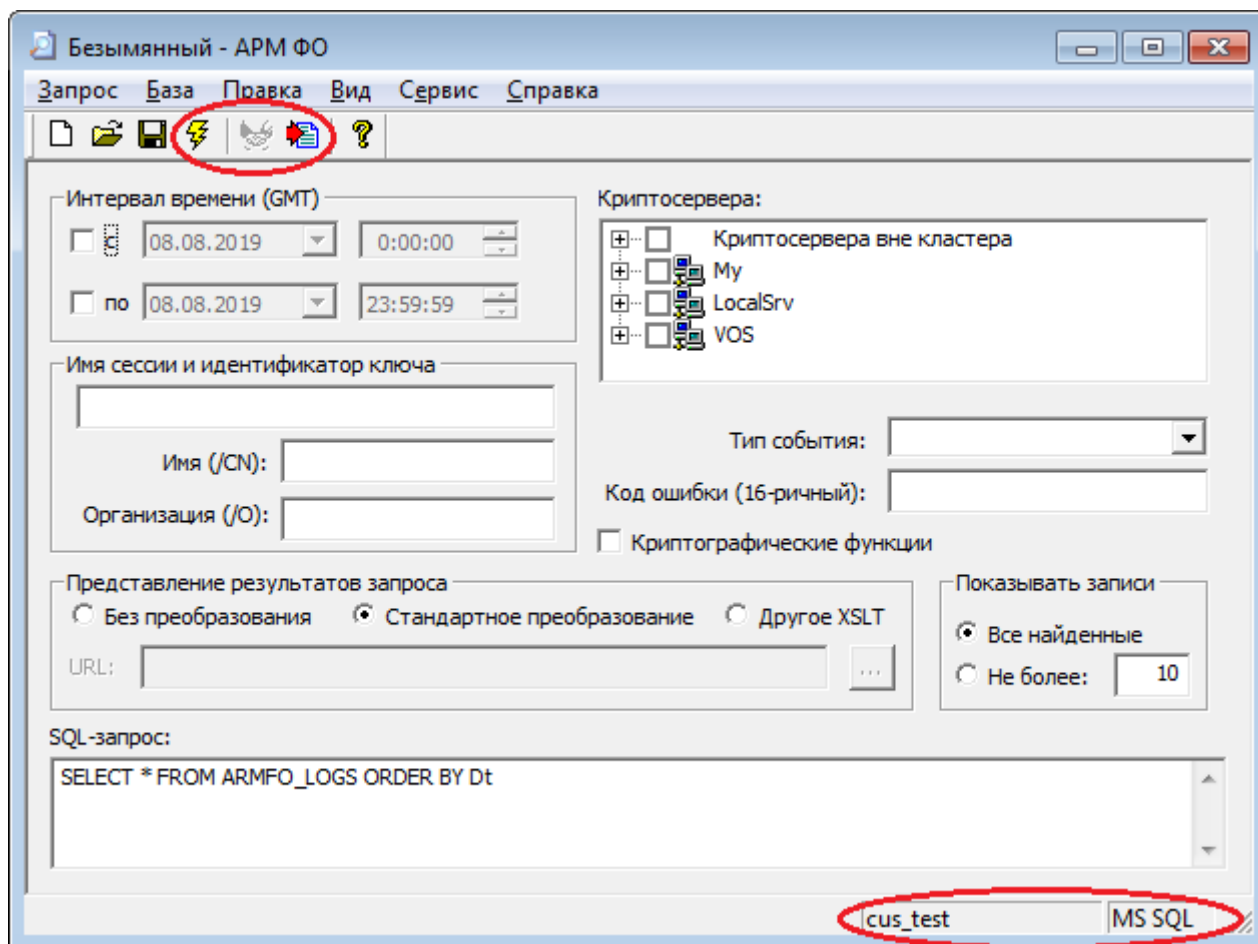



Рисунок 44 – Главное окно АРМ ФО после подключения к БД

Чтобы отсоединиться от базы данных, выберите пункт меню «**База**» – «**Отключиться**» или завершите работу программы.

11.3 Импорт протоколов в базу

Импорт протоколов в базу осуществляется из источников, заданных в настройках АРМ УКС. Сформируйте списки КС и кластеров в программе АРМ УКС прежде, чем запускать программу АРМ ФО.

Предупреждение - Введённые в конфигурации АРМ УКС имена КС должны совпадать со значениями, записанными во второй колонке соответствующих файлов протоколов.

Для импорта протоколов в базу выберите пункт меню: «**База**» – «**Импортировать протоколы**» или нажмите кнопку  на панели инструментов. На экране появится окно импорта протоколов (Рисунок 45).

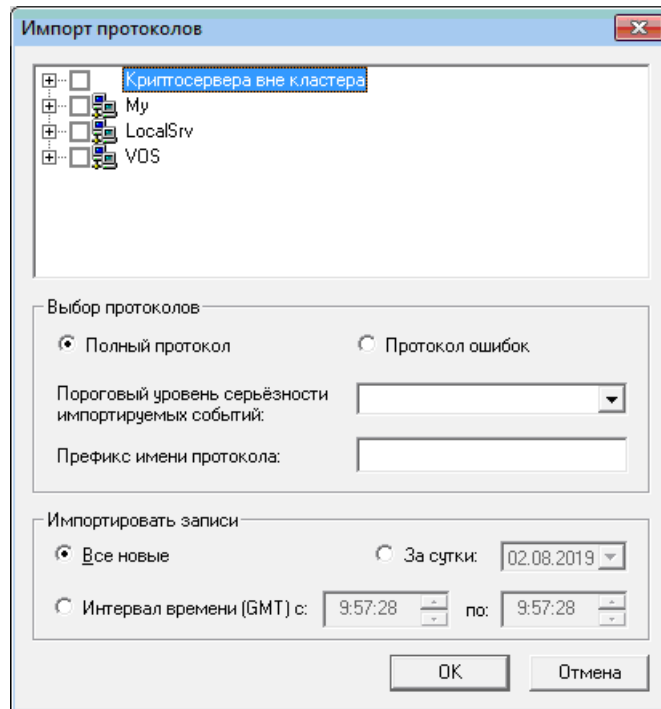


Рисунок 45 – Окно импорта протоколов

Выберите в списке кластеры или отдельные серверы, с которых нужно произвести импорт протоколов.

КС ведёт параллельно два протокола: полный протокол и протокол ошибок, поэтому с помощью переключателя «**Выбор протоколов**» необходимо выбрать, из какого протокола импортировать данные в АРМ ФО. При выборе опции «**Протокол ошибок**» изменяются ещё два параметра: «Пороговый уровень серьёзности импортируемых событий» и «Префикс имени протокола» (Рисунок 46).

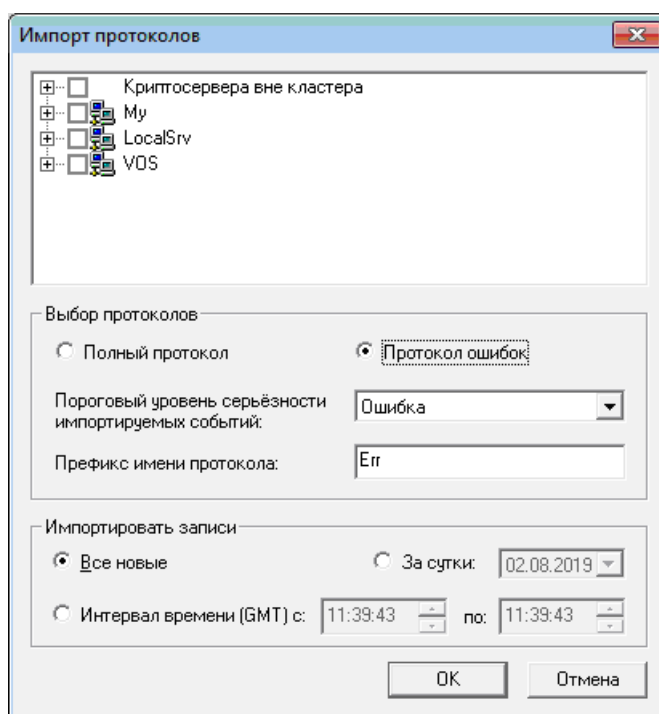


Рисунок 46 – Диалог импорта протоколов в режиме «Протокол ошибок»

Параметр **«Пороговый уровень серьёзности импортируемых событий»** позволяет отказаться от импорта наименее серьёзных (и наиболее многочисленных) событий. Он может использоваться и в режиме **«Полный протокол»** для уменьшения объёма базы и ускорения работы.

Полные протоколы КС записываются в файлы с именем YYYYMMDD.csv, где YYYY - год, MM - месяц, DD - день, то есть без префикса, а протоколы ошибок - с именем ErrYYYYMMDD.csv, то есть с префиксом Err. Кроме того, параметр **«Префикс имени протокола»** может использоваться для импорта протоколов других программ с совместимым форматом файла протокола.

Если выбрать режим **«Все новые»**, в базе осуществляется поиск последней по времени записи и импортируются записи протоколов, начиная с этого времени. Если необходимо импортировать все протоколы, предварительно очистите базу (см. подраздел 11.4).

Для импорта протоколов за одни сутки выберите режим **«За сутки»** и укажите требуемую дату. При этом в базе будет найдена последняя по времени запись, относящаяся к указанной дате, и импортированы записи протоколов за выбранную дату, начиная с этого времени. Если необходимо импортировать действительно все протоколы за сутки, предварительно требуется очистить базу (см. подраздел 11.4).

Для импорта протоколов за интервал времени, который меньше суток выберите режим **«Интервал времени (GMT)»** и укажите требуемую дату и интервал времени. При этом сначала будут автоматически удалены все записи в базе за указанный период (если они там были), а затем соответствующие записи будут импортированы.

Нажмите кнопку "OK". На экране появится индикатор выполнения операции (Рисунок 47).

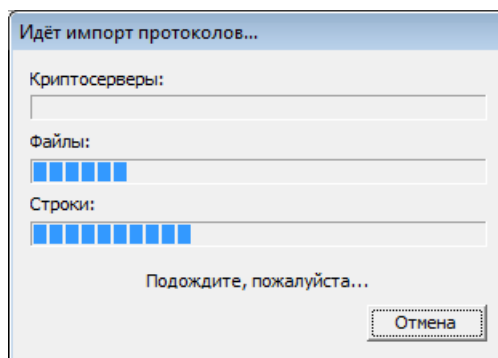


Рисунок 47 – Индикатор выполнения операции импорта протоколов

Для остановки импорта нажмите кнопку «**Отмена**» или клавишу «**Esc**».

11.4 Очистка базы

Из базы данных можно удалить записи за любое количество суток. Для этого выберите пункт меню: «**База**» – «**Очистить**». На экране появится диалоговое окно (Рисунок 48).

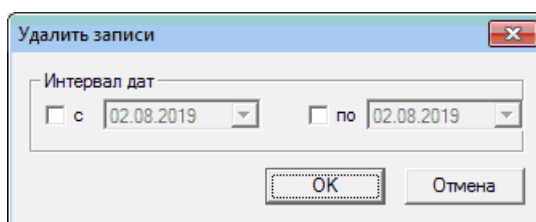


Рисунок 48 – Диалог очистки базы данных

Задайте интервал дат (выбраны обе даты), период с заданной даты до текущей (задана только первая дата), период до указанной даты (задана только вторая дата) или полную очистку базы (не задана ни одна дата). Нажмите кнопку «**ОК**» (Рисунок 49).

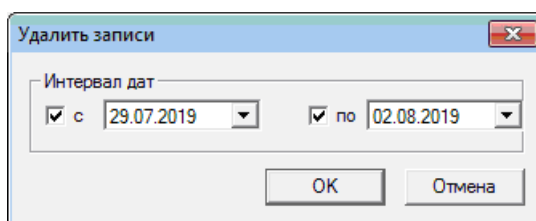


Рисунок 49 – Диалог очистки базы данных за интервал времени

Подтвердите очистку базы данных в появившемся окне подтверждения (Рисунок 50).

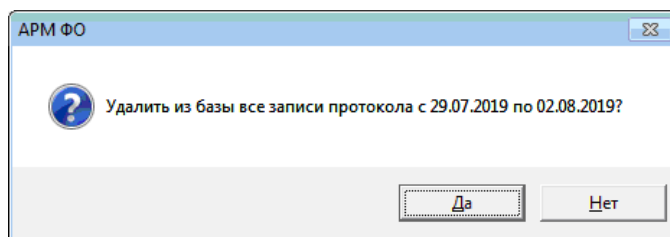


Рисунок 50 – Диалог подтверждения очистки базы данных

Программа вычислит количество записей, подлежащих удалению и запросит второе подтверждение (Рисунок 51).

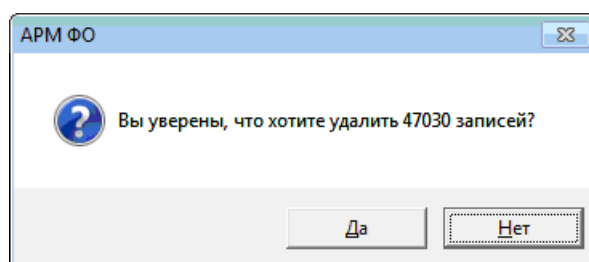


Рисунок 51 – Диалог повторного подтверждения очистки базы данных

Нажмите кнопку «Да».

11.5 Структура базы данных

Вся информация, импортируемая в базу данных, размещается в одной таблице - ARMFO_LOGS (Таблица 1).

Таблица 1 – Структура таблицы ARMFO_LOGS

Наименование поля	Тип	Описание
N	Целочисленный	Внутренний счётчик, в запросах не используется
Dt	Дата/время	Дата/время события
Server	Строка (32)	Имя компьютера, сделавшего запись
Pid	Целочисленный	Идентификатор процесса, сделавшего запись
Tid	Целочисленный	Идентификатор потока, сделавшего запись
Facility	Целочисленный	Модуль, сделавший запись. Допустимы следующие значения: 0x0 - System 0x7 - Win32 0x10 - Kernel 0x20 - Security

Наименование поля	Тип	Описание
		0x30 - Logging 0x40 - Service 0x50 - Application 0x60 - User 0x70 - KC 0x71 - Config 0x72 - Управление 0x73 - Local3 0x80 - OpenSSL 0xAA - KC (монитор) 0xBB - Монитор
Severity	Целочисленный	Тип события. Допустимы следующие значения: 0x0 - Фатальная ошибка 0x10 - Сигнал тревоги 0x20 - Критическая ошибка 0x30 - Ошибка 0x40 - Предупреждение 0x50 - Уведомление 0x60 - Информация 0x66 - Неуспешная аутентификация 0x67 - Успешная аутентификация 0x70 - Отладочное сообщение 0x80 - Трассировка
Func	Целочисленный	Код функции. Получение текстового значения имени функции осуществляется программным путём при формировании отчёта
Code	Целочисленный	Код завершения (ошибки). Получение текстового значения описания ошибки осуществляется программным путём при формировании отчёта
Address	Строка (64)	Сетевой адрес клиента
UserId	Строка (255)	Номер ключа и (или) идентификатор сертификата
CN	Строка (64)	Имя владельца сертификата, если UserId его содержит
Org	Строка (64)	Наименование организации владельца сертификата, если UserId его содержит
Description	Текст (длина не ограничена)	Дополнительное описание

По умолчанию индексированными являются поля N (первичный индекс), Dt, Server, Severity и CN.

11.6 Выполнение запросов к базе данных и просмотр отчётов

11.6.1 Создание, сохранение и открытие запросов

Новый запрос создаётся при запуске программы, кроме того, можно создать новый запрос, выбрав пункт меню «Запрос» – «Новый» или нажав кнопку «Новый» на панели инструментов. Новый запрос имеет следующее SQL-представление:

SELECT * FROM ARMFO_LOGS ORDER BY Dt

что означает – отбор всех записей базы данных и упорядочение их по дате/времени событий. В большинстве случаев не следует выполнять этот запрос, так как он малоинформативен, а его выполнение может занять очень много времени.

Для сохранения созданного запроса нужно выбрать пункт меню «Запрос» – «Сохранить» или «Запрос» – «Сохранить как», или нажать стандартную кнопку «Сохранить» на панели инструментов и указать имя для файла запроса в стандартном диалоге сохранения файла.

Для открытия ранее созданного запроса нужно выбрать пункт меню «Запрос» – «Открыть» или нажать кнопку «Открыть» на панели инструментов и выбрать файл, содержащий запрос (с расширением *.lq) в стандартном диалоге открытия файла. Также можно выбрать ранее открытый запрос в списке последних открытых файлов.

Поскольку реализации языка SQL для БД Oracle и MS SQL существенно различаются, запрос, созданный для одного типа БД, не может быть открыт, если в настройках установлен другой тип (Рисунок 52).

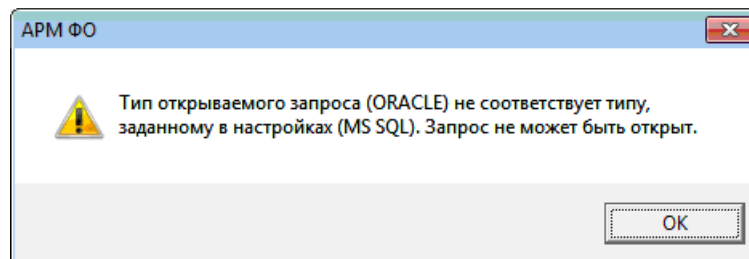


Рисунок 52 – Сообщение о несовпадении типов БД в запросе и в настройке

11.6.2 Редактирование запросов

Все запросы АРМ ФО к базе данных являются SQL-запросами, следовательно, их редактирование производится в поле «SQL-запрос». Кроме того, для упрощения ввода наиболее часто используемых условий отбора в главном окне предусмотрены несколько визуальных элементов управления, позволяющих выбрать:

- интервал времени событий с точностью до секунды;
- имена КС;
- имя сессии и идентификатор ключа;

- имя пользователя (/CN);
- наименование организации (/O);
- тип события;
- код завершения операции (код ошибки);
- принадлежность события к криптографическим функциям.

Для ограничения количества записей, возвращаемых запросом, необходимо перевести переключатель «**Показывать записи**» в положение «**Не более**» и ввести ограничение на количество записей.

При изменении условий отбора с помощью перечисленных элементов управления программа автоматически изменяет текст SQL-запроса. Кроме того, при изменении SQL-запроса вручную программа пытается отобразить условия отбора, введенные в поле «**SQL-запрос**», с помощью тех же элементов управления. Если это невозможно, все эти элементы управления становятся недоступными, после чего редактировать запрос можно только в поле «**SQL-запрос**» (Рисунок 53).

The screenshot shows a software window titled "Запрос_1.lq - АРМ ФО" with a menu bar (Запрос, База, Правка, Вид, Сервис, Справка) and a toolbar. The main area contains several sections:

- Интервал времени (GMT):** Two date-time pickers. The first is set to "с 08.08.2019 0:00:00" and the second to "по 08.08.2019 23:59:59".
- Имя сессии и идентификатор ключа:** Two empty text input fields.
- Имя (/CN):** An empty text input field.
- Организация (/O):** An empty text input field.
- Криптосервера:** A tree view showing "Криптосервера вне кластера", "My", "LocalSrv", and "VOS".
- Тип события:** A dropdown menu.
- Код ошибки (16-ричный):** An empty text input field.
- Криптографические функции:** An unchecked checkbox.
- Представление результатов запроса:** Three radio buttons: "Без преобразования" (unchecked), "Стандартное преобразование" (checked), and "Другое XSLT" (unchecked). Below is a "URL:" label and an empty text input field.
- Показывать записи:** Two radio buttons: "Все найденные" (checked) and "Не более:" (unchecked). Next to "Не более:" is a text input field containing the number "10".
- SQL-запрос:** A large text area containing the SQL query: `SELECT * FROM ARMFO_LOGS WHERE Dt>='2019-08-08T00:00:00' AND Dt<='2019-08-08T23:59:59' AND Severity>=20 ORDER BY Dt`

At the bottom right, there are two labels: "cus_test" and "MS SQL".

Рисунок 53 – Окно программы с SQL-запросом, непредставляемым через визуальные элементы управления

11.6.3 Выполнение запросов к базе данных

Для выполнения запроса к базе данных (соединение с которой должно быть уже установлено) выберите пункт меню «**Запрос**» – «**Выполнить**». На экране появится диалоговое окно (Рисунок 54), которое автоматически закрывается после выполнения запроса.

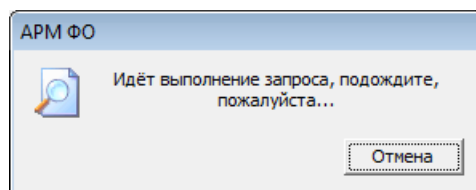


Рисунок 54 – Сообщение о выполнении запроса

Для прерывания выполнения запроса нажмите кнопку «**Отмена**» или клавишу «**Esc**».

11.6.4 Просмотр отчётов

После выполнения запроса его результат загружается в браузер HTML и отображается на экране (Рисунок 55).

Дата/Время (GMT)	Сервер/Модуль	Тип события/код сообщения	Функция	Описание
2019-08-01 10:51:08.154	W2008R2CRSRV3 Криптосервер	Ошибка 0xE070000F	Проверка ЭП данных	Ошибка выполнения ASN.1-распаковки сообщения в формате PKCS#7
2019-08-01 10:51:42.006	W2008R2CRSRV3 Криптосервер	Ошибка 0xE0700042	Проверка ЭП данных	Подпись недостоверна ЭП №1 [всего ЭП: 1] : Время создания ЭП Aug 01 13:51:40 2019"; Издатель: "CN=rootca,CN=Users,DC=skad35,DC=ru" Серийный номер: "40:50:14:C0:84:D8:A0:E5:74:DF:4C:F5:5D:X509v3 идентификатор ключа владельца
2019-08-01 10:51:42.006	W2008R2CRSRV3 Криптосервер	Ошибка 0xE0700019	Проверка ЭП данных	Ошибка проверки ЭП
2019-08-01 10:51:42.006	W2008R2CRSRV3 Криптосервер	Ошибка 0xE070000F	Проверка ЭП данных	Ошибка выполнения ASN.1-распаковки сообщения в формате PKCS#7
2019-08-01 10:51:47.091	W2008R2CRSRV3 Криптосервер	Ошибка 0xE0700042	Проверка ЭП данных	Подпись недостоверна ЭП №1 [всего ЭП: 1] : Время создания ЭП Aug 01 13:51:46 2019"; Издатель:

Рисунок 55 – Отображение результатов запроса

Пользуясь стандартными возможностями HTML-браузера, можно просматривать, печатать и сохранять в файл результаты запроса.

Результат, подобный показанному на примере (Рисунок 55), будет получен при условии, что переключатель «**Представление результатов запроса**» (Рисунок 53) стоит в положении по умолчанию - «**Стандартное преобразование**». Реально программа АРМ ФО выдаёт результаты запроса в виде XML-файла, а затем может преобразовывать его в HTML с помощью XSLT-преобразования. Чтобы посмотреть результаты запроса в формате XML (Рисунок 56), переведите переключатель «**Представление результатов запроса**» в положение «**Без преобразования**» (Рисунок 53).

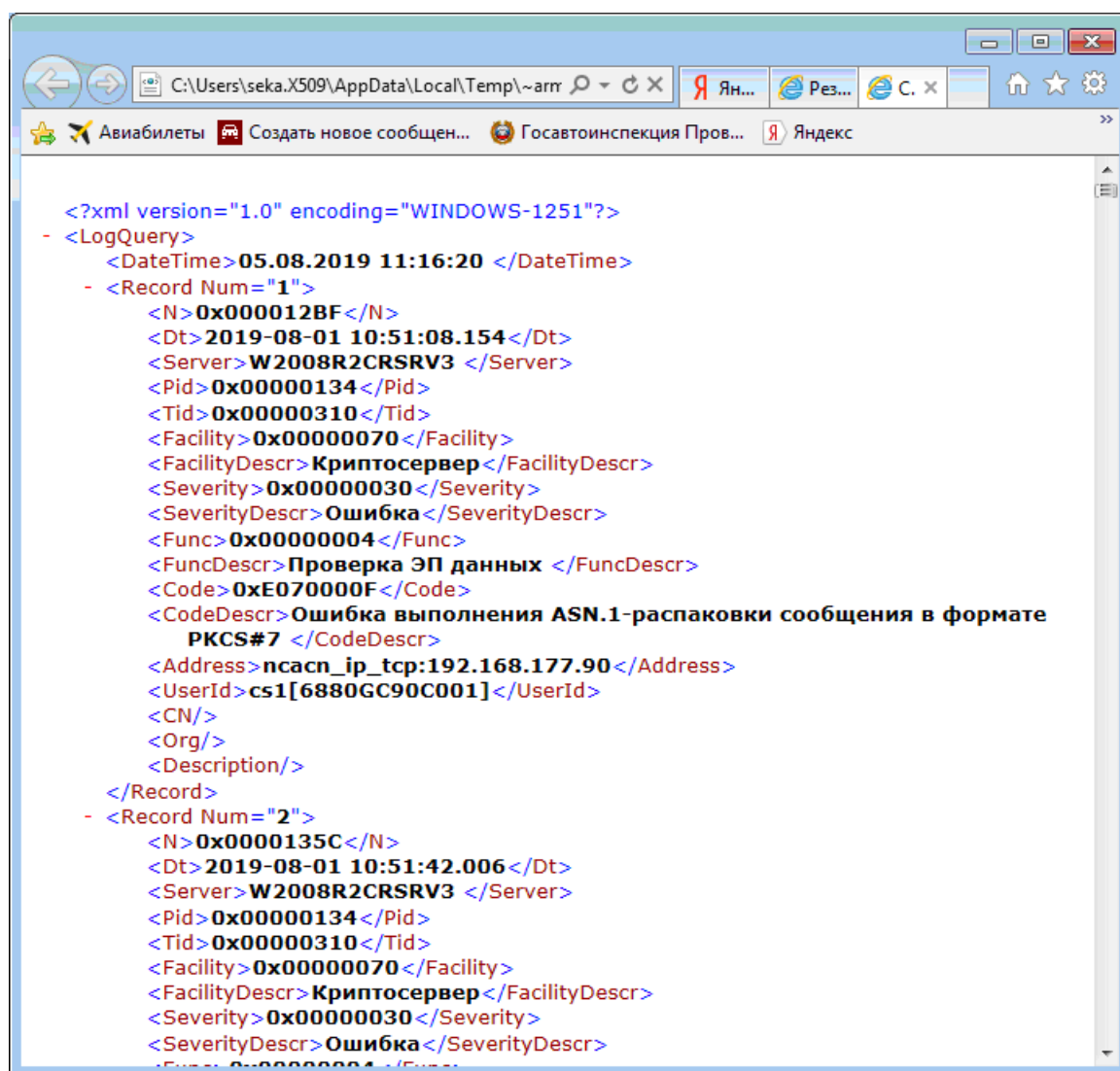


Рисунок 56 – Отображение результатов запроса в формате XML

Если переключатель «**Представление результатов запроса**» (Рисунок 53) стоит в положении «**Стандартное преобразование**», в заголовок XML-файла добавляется ссылка на файл, производящий стандартное XSLT-преобразование - ~armfo_.xsl, который программа АРМ ФО помещает во временную директорию (туда же, куда и временный файл с результатами запроса).

Не рекомендуется изменять содержимое этого файла без серьезной необходимости. Если необходимо изменить представление результатов запроса (набор полей, отображаемых на экране, шрифт, оформление), следует создать своё XSLT-преобразование в соответствии со стандартом <http://www.w3.org/TR/1999/REC-xslt-19991116>, записать его в файл с расширением .xsl, переключатель «**Представление результатов запроса**» поставить в положение «**Другое XSLT**» и указать в поле URL главного окна программы путь к этому файлу в формате URL. В простейшем случае, если файл доступен через файловую систему, можно воспользоваться стандартным диалогом выбора файла, нажав кнопку справа от поля ввода «**URL:**» (Рисунок 57).

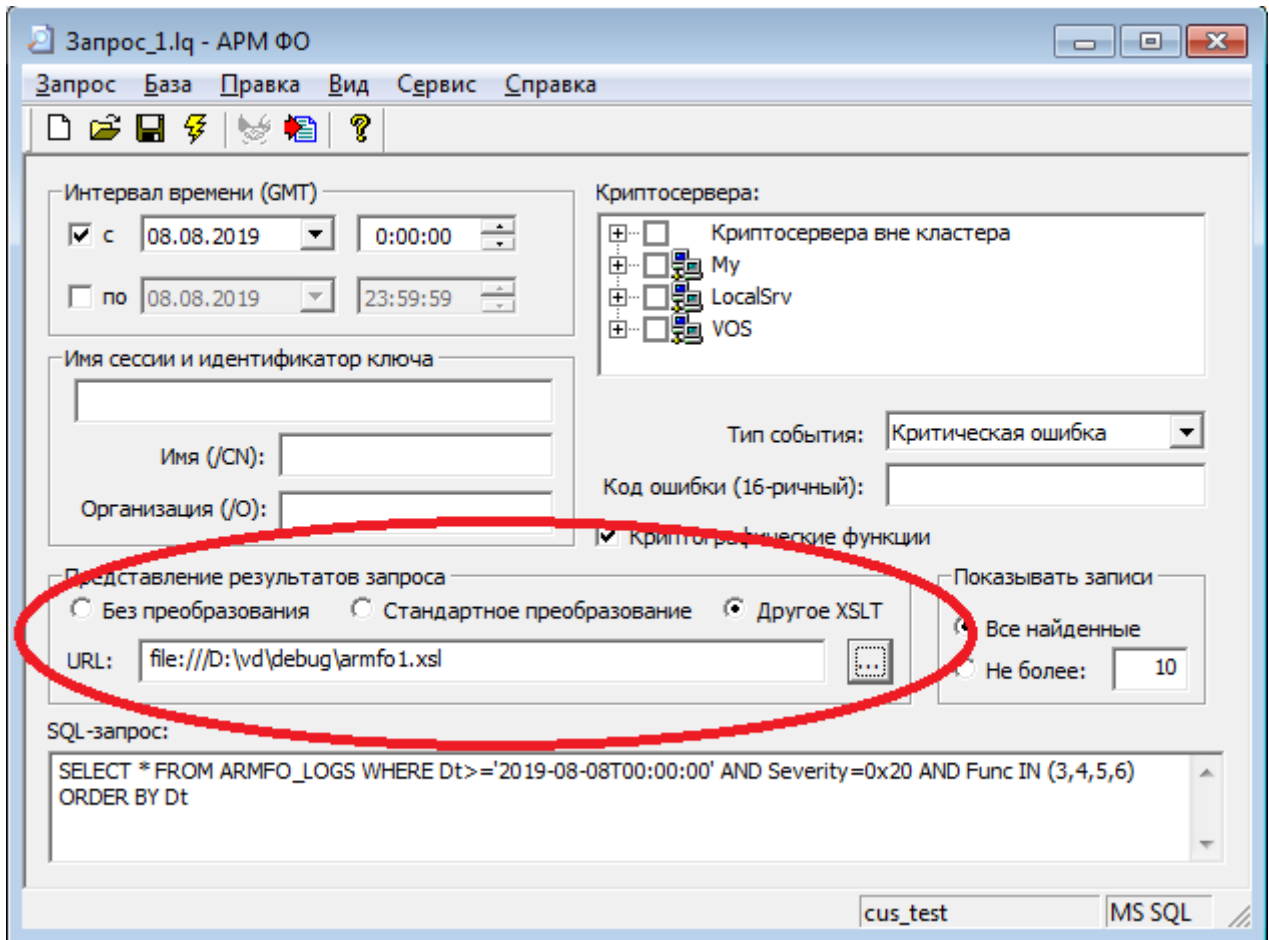


Рисунок 57 - Диалог выбора XSLT-преобразования

Результаты того же запроса в этом случае могут выглядеть иначе (Рисунок 58).

Результаты запроса

Дата/Время	Сервер/ Модуль	Тип события/ Код сообщения/ Функция	Пользователь	Описание
2019-08-01 10:51:08.154	W2008R2CRSRV3 Криптосервер	Ошибка 0xE070000F Проверка ЭП данных	cs1 [6880GC90C001]	Ошибка выполнения ASN.1-распаковки сообщения в формате PKCS#7
2019-08-01 10:51:42.006	W2008R2CRSRV3 Криптосервер	Ошибка 0xE0700042 Проверка ЭП данных	cs2 [2254MFPPQA01]	Подпись недостоверна ЭП №1 [всего ЭП: 1] : Время создания ЭП: "Thu Aug 01 13:51:40 2019"; Издатель: "CN=rootca,CN=Users,DC=skad35,DC=ru"; Серийный номер: "40:50:14:C0:84:D8:A0:E5:74:DF:4C:F5:5D:0A:82:1C"; X509v3 идентификатор ключа владельца: "";
2019-08-01 10:51:42.006	W2008R2CRSRV3 Криптосервер	Ошибка 0xE0700019 Проверка ЭП данных	cs2 [2254MFPPQA01]	Ошибка проверки ЭП
2019-08-01 10:51:42.006	W2008R2CRSRV3 Криптосервер	Ошибка 0xE070000F Проверка ЭП данных	cs2 [2254MFPPQA01]	Ошибка выполнения ASN.1-распаковки сообщения в формате PKCS#7
2019-08-01 10:51:47.091	W2008R2CRSRV3 Криптосервер	Ошибка 0xE0700042 Проверка ЭП данных	cs2 [2254MFPPQA01]	Подпись недостоверна ЭП №1 [всего ЭП: 1] : Время создания ЭП: "Thu Aug 01 13:51:46 2019"; Издатель: "CN=rootca,CN=Users,DC=skad35,DC=ru"; Серийный номер: "40:50:14:C0:84:D8:A0:E5:74:DF:4C:F5:5D:0A:82:1C"; X509v3 идентификатор ключа владельца: "";

Рисунок 58 – Отображение результатов запроса с пользовательским XSLT-преобразованием

В состав АРМ ФО входят два дополнительных файла XSLT-преобразования - arm-fo1.xsl и crypto.xsl. Их можно использовать, соответственно, для создания более подробного отчёта и для создания отчёта о выполнении криптографических операций по всем пользователям ключевых документов.

11.7 Протокол работы АРМ ФО

Программа АРМ ФО протоколирует в системный журнал свои ошибки, а также события запуска программы и выхода из неё. Для просмотра системного журнала следует выбрать пункт меню «Сервис» – «Журнал событий» или воспользоваться стандартным способом просмотра Журнала Windows. На экране появится стандартная программа просмотра событий. Выберите раздел «Журнал приложений» для просмотра событий, у которых поле «Источник» имеет значение *armfo* (Рисунок 59).

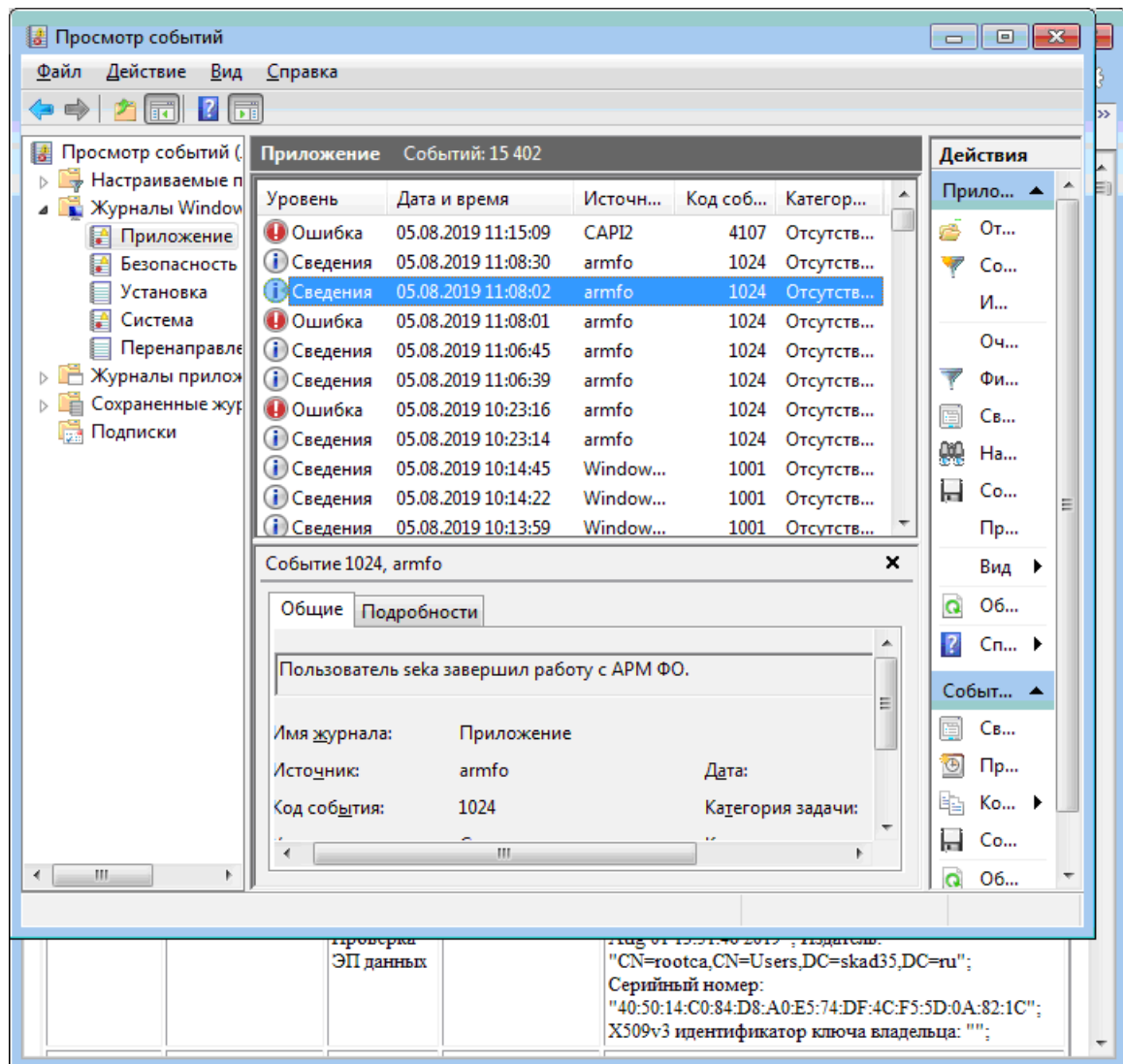


Рисунок 59 – Просмотр журнала событий АРМ ФО

12 ОПИСАНИЕ ОШИБОЧНЫХ СИТУАЦИЙ

Ниже (Таблица 2) приведено описание возможных ошибочных ситуаций. В левой колонке указано символьное имя ошибки и шестнадцатеричное значение ее кода, в правой колонке приведено детальное описание и причина возникновения ошибки.

Таблица 2 – Описание ошибочных ситуаций

Имя и код ошибки	Описание и причина возникновения ошибки
VCERT_OK (0x00000000)	Успешное завершение функции
VCERT_E_GENERIC (0xE0700001)	Общая (внутренняя) ошибка библиотеки. Указывает на возможную ошибку в самой библиотеке или на искажения в ее настройках
VCERT_E_INVALID_PARAMETER (0xE0700002)	В функцию был передан неверный параметр. Возникает в случае передачи нулевого указателя, неверно заполненной структуры объекта системы управления сертификатами (СУС) или параметров или при неверном размере блока памяти
VCERT_E_INVALID_CONTEXT (0xE0700003)	Неверный контекст библиотеки, потоковой или другой операции. Вероятно, искажены настройки профиля пользователя или обнаружена ошибка в синтаксисе конфигурационного файла pkil.conf
VCERT_E_OPERATION_NOT_SUPPORTED (0xE0700004)	Операция (или функция) не поддерживается. Выполнен вызов функции или операции, не поддерживаемой библиотекой или не разрешенной для контекста библиотеки
VCERT_E_INVALID_FLAG (0xE0700005)	В функцию был передан неверный флаг. В параметре или в структуре параметров функции указана неверная маска (битовое ИЛИ) флагов
VCERT_E_NO_MEMORY (0xE0700006)	Недостаточно оперативной памяти. Вероятно, произведен вызов блочной функции над слишком большим блоком памяти или файлом
VCERT_E_DIGEST (0xE0700007)	Ошибка вычисления хэш-значения. Вероятно, неверен объектный идентификатор (OID) алгоритма хэширования
VCERT_E_CERT_USAGE (0xE0700008)	Неверное использование сертификата. В рабочем сертификате отсутствует требуемое разрешенное использование ключа проверки ЭП/открытого ключа шифрования, регламент или расширенное использование ключа проверки ЭП/открытого ключа шифрования
VCERT_E_CERT_FIND_PRIVATE_KEY (0xE0700009)	Не найден ключ ЭП, соответствующий данному сертификату. Отсутствует ключевой носитель с требуемым ключом ЭП, неверен ПИН-код устройства типа смарт-карта или неверен пароль ключа ЭП
VCERT_E_CMS_ADD_SIGNATURE (0xE070000C)	Ошибка добавления ЭП к сообщению в формате CMS/PKCS#7. Вероятно, что недостаточно ресурсов для выполнения операции, произошел сбой аппаратного датчика случайных чисел (ДСЧ) или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_CMS_ASN1_DECODE (0xE070000F)	Ошибка выполнения ASN.1-распаковки сообщения в формате CMS/PKCS#7. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_CMS_ASN1_ENCODE (0xE0700010)	Ошибка выполнения ASN.1-упаковки сообщения в формате CMS/PKCS#7. Вероятно, возникла нехватка ресурсов для выполнения операции
VCERT_E_SIGN_HASH (0xE0700012)	Ошибка вычисления ЭП хэш-значения. Вероятно, неверна длина хэш-значения, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_VERIFY_POLICY (0xE0700013)	Ошибка добавления регламента в контекст проверки сертификата. Вероятно, объектный идентификатор (OID) регламента неверен
VCERT_E_VERIFY_EXTKEYUSAGE (0xE0700014)	Ошибка добавления расширенного использования ключа в контекст проверки сертификата. Вероятно, объектный идентификатор (OID) расширенного использования ключа проверки ЭП/открытого ключа шифрования неверен
VCERT_E_OVERFLOW (0xE0700016)	Ошибка переполнения - либо данные слишком велики, либо буфер слишком мал. Вероятно, произведен вызов блочной функции над слишком большим блоком памяти или файлом
VCERT_E_PKCS10_DAMAGED (0xE0700017)	PKCS#10 запрос на сертификат поврежден или искажен
VCERT_E_REVREQ_DAMAGED (0xE0700018)	Запрос на аннулирование сертификата поврежден или искажен
VCERT_E_VERIFY (0xE0700019)	Общая ошибка проверки ЭП CMS/PKCS#7 сообщения. Возникла ошибка при проверке хотя бы одной ЭП CMS-сообщения
VCERT_E_CMS_INVALID_TYPE (0xE0700022)	Неверный тип содержимого сообщения в формате CMS/PKCS#7. Вероятно, в функцию проверки ЭП передано зашифрованное CMS-сообщение или наоборот

Имя и код ошибки	Описание и причина возникновения ошибки
VCERT_E CMS_NO_RECIPIENTS (0xE0700024)	Отсутствуют или неверны данные сертификатов получателей зашифрованного сообщения в формате CMS/PKCS#7. CMS-сообщение повреждено или искажено
VCERT_E CMS_NOT_RECIPIENT (0xE0700026)	Владелец сертификата не является получателем зашифрованного сообщения в формате CMS/PKCS#7. Идентификатор рабочего сертификата отсутствует в списке получателей зашифрованного CMS-сообщения
VCERT_E CMS_KEY_DECRYPT (0xE0700027)	Ошибка расшифрования сеансового ключа зашифрованного CMS/PKCS#7 сообщения. Вероятно, CMS-сообщение повреждено или искажено, или нет доступа к ФКН vdToken с неизвлекаемым закрытым ключом шифрования
VCERT_E DATA_DECRYPT (0xE0700028)	Ошибка расшифрования блока данных. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_RANDOM (0xE0700029)	Ошибка генерации случайного числа. Вероятно, произошел сбой аппаратного ДСЧ
VCERT_E_OPEN_CONFIG (0xE071002A)	Ошибка доступа к конфигурационному файлу pkil.conf . В текущем рабочем каталоге процесса не найден конфигурационный файл pkil.conf
VCERT_E_READ_CONFIG (0xE071002B)	Ошибка разбора конфигурационного файла pkil.conf . Обнаружена ошибка в формате конфигурационного файла pkil.conf
VCERT_E_NO_DEFAULT_CONFIG (0xE071002C)	Профиль по умолчанию не указан в конфигурационном файле pkil.conf . Вероятно, была произведена попытка инициализации контекста библиотеки с профилем по умолчанию
VCERT_E_OPEN_PSTORE (0xE070002D)	Ошибка доступа к ПСП или к подписанному справочнику. Вероятно, путь (URI) к ПСП или подписанному справочнику неверен
VCERT_E_OPEN_LOCALSTORE (0xE070002E)	Ошибка доступа к ЛСП. Вероятно, путь (URI) к ЛСП неверен
VCERT_E_VERIFY_STORE_USAGE (0xE070002F)	Подписанный справочник имеет неверный идентификатор использования. Вероятно, произведена попытка использовать подписанное обновление от Центра сертификации (ЦС) или Центра регистрации (ЦР) вместо ПСП или наоборот
VCERT_E_VERIFY_STORE (0xE0700030)	Ошибка проверки целостности ПСП или подписанного справочника. Вероятно, произошла ошибка построения или проверки цепочки сертификата подписанта или подписанный справочник поврежден или искажен
VCERT_E_OPEN_LDAPSTORE (0xE0700031)	Ошибка доступа к ССС. Вероятно, путь (URI) к ССС неверен, отсутствует сетевое подключение к ССС или доступ к ССС запрещен из-за отсутствия билета Kerberos
VCERT_E_VERIFY_CERT (0xE0700034)	Ошибка построения и проверки цепочки сертификата. Вероятно, срок действия рабочего сертификата или ключа ЭП истек, не найдены сертификат ЦС или САС, необходимые для построения цепочки, или срок действия САС истек
VCERT_E_CERT_MISSING (0xE0700035)	Сертификат издателя не был найден в доступных справочниках. В доступных справочниках отсутствует сертификат ЦС, необходимый для построения цепочки, при этом не разрешен или отсутствует доступ к точкам AIA
VCERT_E_CERT_EXPIRED (0xE0700036)	Срок действия сертификата уже истек
VCERT_E_CERT_DAMAGED (0xE0700037)	Сертификат поврежден или искажен
VCERT_E_CERT_BROKEN - CONSTRAINT (0xE0700038)	Нарушены базовые ограничения цепочки сертификата
VCERT_E_CERT_REVOKED (0xE0700039)	Сертификат был аннулирован издателем
VCERT_E_CERT_UNTRUSTED (0xE070003A)	Цепочка сертификации не оканчивается доверенным сертификатом. В ПСП отсутствует необходимый сертификат корневого ЦС
VCERT_E_CRL_MISSING (0xE070003B)	САС издателя не был найден в доступных справочниках. В доступных справочниках отсутствует САС, необходимый для построения цепочки, при этом не разрешен или отсутствует доступ к точкам CDP
VCERT_E_CRL_EXPIRED (0xE070003C)	Срок действия САС уже истек
VCERT_E_CRL_DAMAGED (0xE070003D)	САС поврежден или искажен
VCERT_E_CERT_BROKEN - HIERARCHY (0xE070003E)	Нарушено ограничение иерархии цепочки сертификата
VCERT_E_CHAIN_ERROR (0xE070003F)	Общая ошибка построения и проверки цепочки сертификата. Вероятно, цепочка слишком длинная
VCERT_E_INVALID_USAGE (0xE0700041)	Ошибка использования сертификата не по назначению. В проверяемом сертификате отсутствует требуемое разрешенное использование ключа проверки ЭП/открытого ключа шифрования, регламент или расширенное использование ключа проверки ЭП/открытого ключа шифрования

BAMБ.00096-06 95 01

Имя и код ошибки	Описание и причина возникновения ошибки
VCERT_E_INVALID_SIGNATURE (0xE0700042)	ЭП недостоверна. Проверяемые данные повреждены или искажены, или неверен ключ проверки ЭП, который был использован для проверки ЭП
VCERT_E_PUBKEY_NOT_FOUND (0xE0700043)	У сертификата неизвестный ключ проверки ЭП/открытый ключ шифрования. Вероятно, неверен алгоритм ключа проверки ЭП/открытого ключа шифрования сертификата
VCERT_E_UPDATECRL (0xE0700045)	Общая ошибка обновления САС. Вероятно, при критичном обновлении одного из САС, находящихся в ЛСП, произошла ошибка
VCERT_E_CERT_NOT_FOUND (0xE0700046)	Сертификат не был найден в доступных справочниках. При поиске в доступных справочниках не был найден ни один сертификат, удовлетворяющий заданному шаблону
VCERT_E_CERT_NOT_YET_VALID (0xE0700047)	Срок действия сертификата еще не наступил
VCERT_E_NO_ATTACHED_SIGNER (0xE070004A)	Сертификат подписанта отсутствует в сообщении в формате CMS/PKCS#7. Вероятно, был установлен флаг проверки ЭП FLAG_CMS_VERIFY_REQUIREATTACHEDSIGNER
VCERT_E_KERBEROS_FAILURE (0xE070004B)	Ошибка получения или обновления билета Kerberos. Вероятно, нет доступа к Центру распределения ключей (Key Distribution Center, KDC) или имя пользователя и пароль неверны
VCERT_E_KEY_EXPIRED (0xE070004C)	Ключ ЭП/закрытый ключ шифрования уже истек
VCERT_E_KEY_NOT_YET_VALID (0xE070004D)	Ключ ЭП/закрытый ключ шифрования еще недействителен
VCERT_E_CRL_NOT_YET_VALID (0xE070004E)	Срок действия САС еще не наступил
VCERT_E_INIT_CSP (0xE070004F)	Ошибка выполнения инициализации Средства КЗИ. Вероятно, Средство КЗИ не установлено, или его конфигурация искажена
VCERT_E_ENUM_OBJECTS (0xE0700050)	Ошибка доступа к справочнику при переборе объектов. Вероятно, путь (URI) к справочнику неверен, или отсутствует подключение к справочнику по сети
VCERT_E_ENUM_NO_MORE (0xE0700051)	В справочнике больше нет объектов для перебора. Перебор справочника завершен, все объекты были успешно считаны
VCERT_E_INVALID_X500_NAME (0xE0700052)	Текстовая строка, содержащая X.500-имя, имеет неверное представление. Вероятно, строка с X.500-именем искажена или содержит неверный RDN
VCERT_E_INVALID_HEX_STRING (0xE0700053)	Текстовая строка, содержащая шестнадцатеричное число, имеет неверное представление. Текстовая строка с шестнадцатеричным числом должна иметь вид 00:01:0E:0F
VCERT_E_CMS_STREAM_MISMATCH (0xE0700054)	Обнаружено несоответствие между потоковым признаком обрабатываемых данных и вызванной функцией. Вероятно, произошла попытка вызова блочной функции для обработки CMS-сообщения, имеющего ASN.1 кодировку неопределенной длины, или наоборот
VCERT_E_CMS_DETACH_MISMATCH (0xE0700055)	Обнаружено несоответствие между признаком отсоединенной ЭП обрабатываемых данных и вызванной функцией. Вероятно, произошла попытка вызова функции, предназначенной для обработки CMS-сообщений с присоединенными ЭП, для обработки CMS-сообщения с отсоединенными ЭП, или наоборот
VCERT_E_CMS_INVALID_DIGESTS (0xE0700056)	Отсутствуют или неверны данные алгоритмов хэширования подписанного сообщения в формате CMS/PKCS#7. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_CMS_INVALID_SIGNERS (0xE0700057)	Отсутствуют или неверны данные сертификатов подписантов подписанного сообщения в формате CMS/PKCS#7. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_CMS_INVALID_CIPHER (0xE0700058)	Зашифрованное сообщение в формате CMS/PKCS#7 содержит неизвестный или неверный алгоритм шифрования. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_CMS_DATA_SIGNING (0xE0700059)	Ошибка вычисления ЭП подписанного сообщения в формате CMS/PKCS#7. Вероятно, что недостаточно ресурсов для выполнения операции, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_CMS_OMAC_MISMATCH (0xE070005A)	Имитовставка зашифрованного сообщения в формате CMS/PKCS#7 не совпадает с вычисленной. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_FIND_SESSION (0xE0700081)	Требуемая сессия криптосервера не была найдена. В функцию библиотеки был передан идентификатор несуществующей сессии КС
VCERT_E_CMS_NOT_ENCRYPTED (0xE0700083)	CMS/PKCS#7-сообщение не зашифровано или формат сообщения поврежден или искажен. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_ADD_OBJECT (0xE0700087)	Ошибка добавления объекта в справочник сертификатов. Вероятно, такой объект уже существует или добавление объекта в ССС запрещено

ВАНБ.00096-06 95 01

Имя и код ошибки	Описание и причина возникновения ошибки
VCERT_E_TOO_MANY_CERTS_FOUND (0xE0720089)	Слишком много сертификатов найдено по уникальному критерию поиска. Вероятно, несколько сертификатов содержат один и тот же идентификатор ключа ЭП
VCERT_E_USER_CANCEL (0xE072008A)	Операция была отменена пользователем
VCERT_E_OPEN_INFILE (0xE070008B)	Ошибка открытия входного файла. Вероятно, путь или имя файла неверны или доступ к файлу запрещен
VCERT_E_OPEN_OUTFILE (0xE070008C)	Ошибка открытия выходного файла. Вероятно, путь или имя файла неверны или доступ к файлу запрещен
VCERT_E_READ_FILE (0xE070008D)	Ошибка чтения из входного файла. Вероятно, произошло искажение файловой системы
VCERT_E_WRITE_FILE (0xE070008E)	Ошибка записи в выходной файл. Вероятно, на файловой системе закончилось свободное пространство
VCERT_E_FILE_LENGTH (0xE070008F)	Неверный размер файла (нулевой или более 2Гб)
VCERT_E_DELETE_OBJECT (0xE0700091)	Ошибка удаления объекта из справочника сертификатов. Указанный объект не был удален из кэша контекста библиотеки или сессии КС или из ЛСП сессии КС по команде с АРМ УКС
VCERT_E_TOO_FEW_SIGNATURES (0xE0700092)	Подписанный документ содержит недостаточное количество ЭП. Вероятно, были установлены флаги проверки ЭП FLAG_CMS_VERIFY_DELETESIGNATURES или FLAG_CMS_VERIFY_MINIMUMSIGNATURES , или индекс ЭП для операции со штампом времени слишком велик
VCERT_E_GET_PUBKEY (0xE0700094)	Ошибка получения ключа проверки ЭП/открытого ключа шифрования сертификата. Вероятно, возникла нехватка ресурсов или неверен алгоритм ключа проверки ЭП/открытого ключа шифрования сертификата
VCERT_E_PKCS10_CREATE (0xE0700098)	Ошибка создания нового PKCS#10 запроса. Вероятно, произошла ошибка при генерации или записи ключа ЭП на ключевой носитель или XML шаблон имеет неверный формат
VCERT_E_PKCS10_SIGN (0xE070009A)	Ошибка вычисления ЭП PKCS#10 запроса. Вероятно, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_REVREQ_CREATE (0xE070009B)	Ошибка создания нового запроса на аннулирование. Вероятно, возникла нехватка ресурсов
VCERT_E_REVREQ_SIGN (0xE070009C)	Ошибка вычисления ЭП запроса на аннулирование. Вероятно, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_LOAD_PRIVATE_KEY (0xE070009D)	Ошибка загрузки ключа ЭП/закрытого ключа шифрования. Отсутствует ключевой носитель с требуемым ключом ЭП/закрытым ключом шифрования, неверен ПИН-код устройства типа смарт-карта или неверен пароль ключа ЭП/закрытого ключа шифрования
VCERT_E_ADD_SIGNER (0xE070009E)	Ошибка добавления ЭП к ЛСП или к подписанному справочнику. Вероятно, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_OPEN_IDP (0xE07000A1)	Ошибка доступа к точке распространения САС. Вероятно, к точке CDP запрещен доступ или в точке CDP отсутствует требуемый САС
VCERT_E_READ_IDP (0xE07000A2)	Ошибка чтения из точки распространения САС. Вероятно, возникла проблема с сетевым подключением или в точке CDP отсутствует требуемый САС
VCERT_E_INVALID_CREDENTIALS (0xE02000A8)	Ошибочные данные аутентификации при доступе к сессии криптосервера. Вероятно, длина данных аутентификации равна 0
VCERT_E_ACCESS_DENIED (0xE02000A9)	Доступ к сессии криптосервера запрещен. Вероятно, данные аутентификации неверны
VCERT_E_SESSION_BLOCKED (0xA02000AA)	Сессия криптосервера заблокирована
VCERT_E_CLIENT_INFO (0xE02000AB)	Ошибка получения информации о клиенте из протокола DCE-RPC. Вероятно, произошла системная ошибка библиотеки DCE-RPC при получении сетевого адреса клиента
VCERT_E_UNSECURE_CREDENTIALS (0xE02000AC)	Небезопасные (слишком короткие) данные аутентификации сессии криптосервера. Длина данных аутентификации должна быть не менее 8 символов
VCERT_E_SESSION_TIMEOUT (0xA07000AE)	Истек интервал ожидания доступа к сессии КС из-за того, что данная сессия КС в настоящий момент заблокирована и не готова обрабатывать поступающие запросы. Данная ошибка может возникнуть, только если для данной сессии КС настроен ненулевой интервал ожидания доступа

Имя и код ошибки	Описание и причина возникновения ошибки
VCERT_E_TSP_HASH_LENGTH (0xE0700100)	Неверная длина хэш-значения при создании запроса на штамп времени. Длина хэш-значения не соответствует указанному алгоритму хэширования
VCERT_E_TSP_HASH_ALGORITHM (0xE0700101)	Неверный алгоритм хэширования при создании запроса на штамп времени. Объектный идентификатор (OID) алгоритма хэширования неверен
VCERT_E_TSP_CERT_PURPOSE (0xE0700102)	Сертификат не может быть использован для подписи штампов времени. Сертификат не удовлетворяет условиям использования на сервере штампов времени
VCERT_E_TSP_SIGN_FAILED (0xE0700103)	Ошибка вычисления ЭП штампа времени. Вероятно, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_TSP_NO_DIGEST (0xE0700104)	В списке атрибутов отсутствует хэш-значение ЭП и/или данных. Вероятно, штамп времени поврежден или искажен
VCERT_E_TSP_INVALID_SIGNER_NUM (0xE0700105)	Штамп времени содержит неверное количество ЭП. Вероятно, штамп времени поврежден или искажен
VCERT_E_TSP_NO_TST_INFO (0xE0700106)	Ошибка при получении информационного блока штампа времени. Вероятно, штамп времени поврежден или искажен
VCERT_E_TSP_RESP_ASN1_DECODE (0xE0700107)	Ошибка выполнения ASN.1-распаковки подписанного штампа времени. Вероятно, штамп времени поврежден или искажен
VCERT_E_TSP_RESP_NOT_ISSUED (0xE0700108)	Штамп времени не был выдан авторитетным источником. Вероятно, произошла внутренняя ошибка сервера штампов времени
VCERT_E_TSP_DIGEST_MISMATCH (0xE0700109)	Штамп времени содержит хэш-значение, отличное от хэш-значения ЭП CMS/PKCS#7 сообщения. Вероятно, штамп времени поврежден или искажен
VCERT_E_OCSP_CERT_PURPOSE (0xE0700140)	Сертификат не может быть использован для вычисления ЭП ответов сетевого ответчика. Сертификат не удовлетворяет условиям использования на сервере OCSP ответчика
VCERT_E_OCSP_SIGN_FAILED (0xE0700141)	Ошибка вычисления ЭП ответа сетевого ответчика. Вероятно, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_OCSP_RESP_ASN1_DECODE (0xE0700142)	Ошибка выполнения ASN.1-распаковки подписанного ответа сетевого ответчика. Вероятно, ответ сервера OCSP ответчика поврежден или искажен
VCERT_E_OCSP_RESP_NOT_ISSUED (0xE0700143)	Подписанный ответ не был выдан сетевым ответчиком. Вероятно, произошла внутренняя ошибка сервера OCSP ответчика
VCERT_E_OCSP_NOT_BASICRESP (0xE0700144)	Неверный (небазовый) тип подписанного ответа сетевого ответчика. Вероятно, ответ сервера OCSP ответчика содержит статус более чем для одного сертификата
VCERT_E_OCSP_CERTID_MISMATCH (0xE0700145)	Идентификатор сертификата из подписанного ответа сетевого ответчика не соответствует запрашиваемому. Вероятно, ответ сервера OCSP ответчика поврежден или искажен
VCERT_E_OCSP_ISSUER_MISMATCH (0xE0700146)	Издатель сертификата сетевого ответчика не соответствует издателю проверяемого сертификата. Вероятно, ответ сервера OCSP ответчика поврежден или искажен
VCERT_E_TLS_UNSUPPORTED (0xE0700180)	Функции протокола TLS не могут быть использованы с данным контекстом библиотеки. Вероятно, произведена попытка использования функций протокола TLS с минимальным контекстом библиотеки
VCERT_E_TLS_NEW_CONTEXT (0xE0700181)	Ошибка создания контекста нового сеанса связи протокола TLS. Вероятно, возникла нехватка ресурсов, произошел сбой аппаратного ДСЧ или использован контекст проверки библиотеки
VCERT_E_TLS_INVALID_STATE (0xE0700182)	Контекст сеанса связи протокола TLS находится в неверном состоянии. Вероятно, произведена попытка обмена данными между клиентом и сервером, когда защищенный канал еще не сформирован
VCERT_E_TLS_HANDSHAKE (0xE0700183)	Ошибка выполнения переговоров при формировании нового сеанса связи протокола TLS. Клиент и сервер не смогли сформировать защищенный канал, вероятно из-за отсутствия общих наборов криптографических алгоритмов
VCERT_E_TLS_NOT_COMPLETE (0xE0700184)	Переговоры при формировании нового сеанса связи протокола TLS еще не завершены
VCERT_E_TLS_NO_QUERY_DATA (0xE0700185)	Запрашиваемые данные в контексте сеанса связи протокола TLS отсутствуют. Вероятно, на сервере был выполнен запрос на получение сертификата клиента в DER-кодировке при выполнении односторонней аутентификации
VCERT_E_TLS_WRONG_CERT (0xE0700186)	Сертификат противоположной стороны сеанса связи TLS протокола неверен или искажен
VCERT_E_TLS_WRONG_NAME (0xE0700187)	Сертификат противоположной стороны сеанса связи TLS протокола имеет неверное имя. Вероятно, сертификат сервера имеет в дополнении "Альтернативное имя владельца" DNS-имя отличное от того, которое указал клиент

BAMБ.00096-06 95 01

Имя и код ошибки	Описание и причина возникновения ошибки
VCERT_E_TLS_WRITE_ERROR (0xE0700188)	Ошибка при записи данных сеанса связи протокола TLS. Вероятно, возникла нехватка ресурсов или данные TLS протокола искажены
VCERT_E_TLS_READ_ERROR (0xE0700189)	Ошибка при чтении данных сеанса связи протокола TLS. Вероятно, данные TLS протокола искажены
VCERT_E_TLS_READ_MORE (0xE0700190)	Следует продолжить чтение данных сеанса связи протокола TLS. Вероятно, необходимо продолжить переговоры для завершения создания защищенного канала
ERR_PROFILES_BAD_PARAM (0xE0D50001)	При вызове какой-либо функции библиотеки ей передан параметр с недопустимым значением - скорее всего нулевой указатель
ERR_PROFILES_BUFFER_SIZE (0xE0D50002)	При работе со строками (копирование, чтение из реестра и пр.) размер выделенного буфера недостаточен для размещения строки
ERR_PROFILES_NO_MEMORY (0xE0D50003)	Ошибка выделения памяти - либо произошло исчерпание памяти системы, либо при выделении памяти запрошен неадекватный размер
ERR_PROFILES_GET_INSTANCE (0xE0D50004)	Не инициализирована переменная CRYPTO_hinstance, содержащая HINSTANCE исполняемого модуля, содержащего ресурсы
ERR_PROFILES_CREATE_DLG (0xE0D50005)	Ошибка инициализации модального диалога - скорее всего испорчены ресурсы или неправильно инициализирована переменная CRYPTO_hinstance, содержащая HINSTANCE исполняемого модуля, содержащего ресурсы
ERR_PROFILES_GET_DLG_ITEM (0xE0D50006)	Ошибка доступа к элементам управления (кнопка, поле редактирования, список и т.д.) модального диалога - скорее всего испорчены ресурсы
ERR_PROFILES_GET_USER_DIR (0xE0D50007)	Ошибка при вызове функции SHGetFolderPath() библиотеки shell32.dll, возвращающей каталог пользователя по умолчанию - скорее всего проблемы с файловой системой
ERR_PROFILES_GET_WND_RECT (0xE0D50008)	Ошибка функции GetWindowRect() получающей координаты окна. Глобальные проблемы системы
ERR_PROFILES_SET_WND_POS (0xE0D50009)	Ошибка функции SetWindowPos() устанавливающей положение окна. Глобальные проблемы системы
ERR_PROFILES_CLN_TO_SCR (0xE0D5000A)	Ошибка функции ScreenToClient() приводящей экранные координаты окна к клиентским. Глобальные проблемы системы
ERR_PROFILES_USER_CANCEL (0xE0D5000B)	Пользователь нажал кнопку "Отмена" или клавишу ESC
ERR_PROFILES_NO_REG_KEY (0xE0D5000C)	Отсутствует ключ реестра
ERR_PROFILES_DONT_OPEN_- REG_KEY (0xE0D5000D)	Ошибка открытия ключа реестра
ERR_PROFILES_DONT_CREATE_- REG_KEY (0xE0D5000E)	Ошибка создания ключа реестра
ERR_PROFILES_ACCESS_DENY_- REG_KEY (0xE0D5000F)	Недостаточно прав для создания ключа в реестре
ERR_PROFILES_DONT_DEL_- REG_KEY (0xE0D50010)	Ошибка удаления ключа реестра
ERR_PROFILES_AC_DENY_DEL_- REG_KEY (0xE0D50011)	Недостаточно прав для удаления ключа в реестре
ERR_PROFILES_NO_REG_VAL (0xE0D50012)	Отсутствует значение в реестре
ERR_PROFILES_DONT_READ_- REG_VAL (0xE0D50013)	Ошибка чтения значения в реестре
ERR_PROFILES_DONT_WRITE_- REG_VAL (0xE0D50014)	Ошибка записи значения в реестр
ERR_PROFILES_ACCESS_DENY_- REG_VAL (0xE0D50015)	Недостаточно прав для записи значения в реестр
ERR_PROFILES_BAD_TYPE_- REG_VAL (0xE0D50016)	Неправильный тип значения в реестре
ERR_PROFILES_DONT_ENUM_- REG_VAL (0xE0D50017)	Ошибка перечисления значений в ключе реестра

Имя и код ошибки	Описание и причина возникновения ошибки
ERR_PROFILES_NO_PROFILE (0xE0D50018)	При попытке выбора профиля (не в режиме редактирования) в реестре не обнаружено ни одного профиля либо при записи информации о профилях в реестр не было сформировано ни одного профиля
ERR_PROFILES_BAD_CONFIG (0xE0D50019)	Либо в реестре содержится неадекватное (меньше 2) значение параметра "count" обозначающего количество хранилищ для профиля. Либо в конфигурационном файле профиля (cfg.ini) в разделе [ODBC] не задан или задан пустой параметр local.gdbm при параметре local.gdbm_type равном 2
ERR_PROFILES_PROFILE_NOT_FOUND (0xE0D5001A)	Не найден профиль с заданным именем
ERR_PROFILES_PROF_ALREADY_EXISTS (0xE0D5001B)	При попытке добавления нового профиля без флага, разрешающего перезапись, обнаружено, что профиль с таким именем уже есть
ERR_PROFILES_BAD_PROF_INDEX (0xE0D5001C)	Не найден профиль с заданным номером
ERR_PROFILES_FILE_INSTEAD_DIR (0xE0D5001D)	При попытке создания директории (каталога) для хранения профиля обнаружено, что существует файл с таким именем
ERR_PROFILES_AC_DENY_CREATE_DIR (0xE0D5001E)	Недостаточно прав для создания директории (каталога)
ERR_PROFILES_CREATE_DIR_NO_PARENT (0xE0D5001F)	Попытка создать поддиректорию (подкаталог) отсутствующей директории (каталога)
ERR_PROFILES_CREATE_DIR_NO_ROOT (0xE0D50020)	Попытка создать поддиректорию (подкаталог) при отсутствии корня (например, диска)
ERR_PROFILES_DONT_CREATE_DIR (0xE0D50021)	Ошибка создания директории (каталога), не относящаяся к вышеперечисленным
ERR_PROFILES_ODBC (0xE0D50022)	Ошибка вызова функций SQLAllocHandle(), или SQLSetEnvAttr(), или SQLDriverConnect() библиотеки odbc32.dll. Проблемы библиотеки ODBC
ERR_PROFILES_BAD_LDAP_STRING (0xE0D50023)	Ошибка разбора строки LDAP-соединения
ERR_PROFILES_OPEN_MY_STORE (0xE0D50024)	Ошибка функции CertOpenStore() библиотеки Crypt32.dll, открывающей хранилище личных сертификатов
ERR_PROFILES_ENUM_MY_CERTS (0xE0D50025)	Ошибка функции CertEnumCertificatesInStore() библиотеки Crypt32.dll перечисляющей сертификаты из хранилища личных
ERR_PROFILES_GET_CERT_SUBJECT (0xE0D50026)	Ошибка функции CertNameToStr() Crypt32.dll, получающей имя владельца сертификата. Возможно, испорчен сертификат
ERR_PROFILES_NO_MY_CERTS (0xE0D50027)	Не найдено ни одного сертификата в хранилище личных сертификатов
ERR_PROFILES_FILETIME_TO_SYSTIME (0xE0D50028)	Ошибка функции FileTimeToLocalFileTime() или ф-ии FileTimeToSystemTime() библиотеки Kernel32.dll. Возможно, в сертификате указано неадекватное время
ERR_PROFILES_NO_SUBJ_KEY_ID (0xE0D50029)	В сертификате не найдено расширение 'Идентификатор ключа владельца'
ERR_PROFILES_DECODE_OBJECT (0xE0D5002A)	Ошибка функции CryptDecodeObject(), декодирующей объект в ASN1 кодировке. Возможно, испорчен сертификат
ERR_PROFILES_FIND_CERT_BY_KEYID (0xE0D5002B)	Ошибка поиска сертификата ф-ией CertFindCertificateInStore() с параметром CERT_FIND_CERT_ID по идентификатору ключа владельца. Возможно, сертификат отсутствует
ERR_PROFILES_SHOW_CERT (0xE0D5002C)	Ошибка функции CryptUIDlgViewContext(), отображающей сертификат

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ УКС	Автоматизированное рабочее место управления криптографическим сервером
АРМ ФО	Автоматизированное рабочее место формирования отчётов
БД	База данных
КС	Криптографический сервер
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение
САС	Список аннулированных сертификатов
СКЗИ	Средство криптографической защиты информации
ССС	Сетевой справочник сертификатов
ЭВМ	Электронная вычислительная машина
ЭП	Электронная подпись

ПЕРЕЧЕНЬ РИСУНКОВ

1	Загрузка ключа	6
2	Основное окно АРМ УКС	7
3	Добавление криптосервера	8
4	Изменение настроек криптосервера	9
5	Окно просмотра протоколов	11
6	Окно просмотра строки протокола	12
7	Статистика криптосервера	13
8	Окно статистики сессии криптосервера	14
9	Выбор ключа с носителя	15
10	NLB остановлен	16
11	NLB работает	17
12	Файловый диалог выбора сертификата	18
13	Отображение сертификата	19
14	Файловый диалог выбора САС	20
15	Отображение САС	21
16	Выбор каталога для загрузки сертификатов и САС	22
17	Добавление обновления	23
18	Остановка сессии	24
19	Установка фильтрации сертификатов	25
20	Список загруженных сертификатов и САС	26
21	Отсутствующий сертификат на одном из КС	27
22	Просмотр только отсутствующих сертификатов	28
23	Удаление аннулированных/прекративших действие сертификатов	29
24	Удаление сертификатов с истекшими ключами	30
25	Настройка колонок	31
26	Создание отчёта о загруженных объектах	32
27	Установка уровня протоколирования КС	34
28	Уровень протоколирования КС	34
29	Диалоговое окно оповещения о событии	35
30	Протокол работы АРМ УКС	36
31	Окно настройки АРМ УКС	38
32	Настройка оповещения Администратора АРМ УКС	39
33	Большие кнопки панели инструментов	40
34	Ввод кода ошибки для получения описания	41
35	Отображение описания ошибки	41
36	Управление авторизацией сессии	42
37	Добавление записи авторизации	43
38	Изменение записи авторизации	43
39	Главное окно АРМ ФО	45
40	Администратор источников данных ODBC	46
41	Диалог настройки соединения с БД	46
42	Диалог выбора источника данных ODBC	47
43	Сообщение о несовпадении типов БД в источнике данных и в на- стройке	47
44	Главное окно АРМ ФО после подключения к БД	48
45	Окно импорта протоколов	49

46	Диалог импорта протоколов в режиме «Протокол ошибок»	50
47	Индикатор выполнения операции импорта протоколов	51
48	Диалог очистки базы данных	51
49	Диалог очистки базы данных за интервал времени	51
50	Диалог подтверждения очистки базы данных	52
51	Диалог повторного подтверждения очистки базы данных	52
52	Сообщение о несовпадении типов БД в запросе и в настройке	54
53	Окно программы с SQL-запросом, непредставляемым через визуаль- ные элементы управления	55
54	Сообщение о выполнении запроса	56
55	Отображение результатов запроса	57
56	Отображение результатов запроса в формате XML	58
57	Диалог выбора XSLT-преобразования	59
58	Отображение результатов запроса с пользовательским XSLT- преобразованием	60
59	Просмотр журнала событий АРМ ФО	61

ПЕРЕЧЕНЬ ТАБЛИЦ

1	Структура таблицы ARMFO_LOGS	52
2	Описание ошибочных ситуаций	62

[illegible][illegible]