КОД безопасности

Аппаратно-программный комплекс шифрования

Континент

Версия 3.9

Руководство администратора

Аудит

RU.88338853.501430.022 90 6



© Компания "Код Безопасности", 2024. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

Почтовый адрес:	**115127, Россия, Москва, а/я 66 ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Список сокращений ... **4**

Введение ... **5**

Общие сведения ... **6**

Задачи аудита ... 6
Журналы ... 6
Журналы регистрации событий ... 6
Системный журнал ... 7
Журнал НСД ... 8
Журнал сетевого трафика ... 9
Журнал приложения ... 10
Журнал сервера доступа ... 11
Интерфейс программы управления ЦУС ... 11
Конфигуратор ... 12
Агент и единый ключевой носитель ... 15
Программа просмотра журналов ... 16
Программа просмотра отчетов ... 17

Эксплуатация ... **19**

Настройка системы ... 19
Подключение конфигуратора к серверу БД ... 19
Подключение агента ЦУС и СД ... 21
Подключение программы просмотра журналов ... 22
Работа с программой просмотра журналов ... 23
Загрузка записей журналов ... 23
Фильтрация записей ... 24
Поиск записей ... 27
Сохранение записей ... 27
Очистка журналов ... 28
Статистика атак ... 28
Отображение времени регистрации событий в часовом поясе сетевого устройства ... 29
Включение и отключение отображения элементов интерфейса ... 30
Обновление отображаемой информации ... 30
Очистка иерархического списка от удаленных сетевых устройств ... 30
Работа с программой просмотра отчетов ... 30
Отчеты ЦУС ... 30
Запуск программы просмотра отчетов ... 32
Настройка параметров соединения с ЦУС ... 32
Формирование отчета ... 33
Сохранение отчета ... 33
Дополнительные настройки ... 33
Управление единым ключевым носителем ... 33
Просмотр содержимого единого ключевого носителя ... 34
Управление агентом с помощью программы управления ЦУС ... 34
Локальное управление агентом ... 41
Настройка параметров хранения и передачи журналов ... 44
Сбор данных для SIEM-систем ... 47

Приложение ... **50**

Перечень регистрируемых событий ... 50

Документация ... **55**

Список сокращений

БД	База данных
ДА	Детектор атак
ЕКН	Единый ключевой носитель
КК	Криптографический коммутатор (криптокоммутатор)
КШ	Криптографический шлюз (криптошлюз)
НСД	Несанкционированный доступ
ОС	Операционная система
ППЖ	Программа просмотра журналов
ППО	Программа просмотра отчетов
ПУ	Программа управления
РМ	Рабочее место
СД	Сервер доступа
СОВ	Система обнаружения вторжений
СУ	Сетевые устройства
СУБД	Система управления базами данных
ЦУС	Центр управления сетью

Введение

Документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования "Континент". Версия 3.9" (далее — комплекс, АПКШ "Континент"). В нем содержатся сведения, необходимые для управления системой мониторинга и аудита.

Дополнительные сведения, необходимые администратору комплекса, содержатся в документах [**1**] и [**2**] .

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Список учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru. Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Версия — 3.9.3 от 06.06.2024.

Глава 1
Общие сведения

Задачи аудита

Под аудитом подразумевается контроль состояния защищенности и работоспособности комплекса. Оценка функционирования комплекса осуществляется посредством анализа произошедших событий, зарегистрированных в журналах сетевых устройств. Аудит проводится ответственными лицами из числа сотрудников службы информационной безопасности.

В задачи аудита входит:

- регулярный просмотр содержимого журналов регистрации;
- оптимальная настройка параметров хранения журналов;
- управление содержимым журналов (записями о событиях).

Возможностью просмотра содержимого журналов обладают администраторы, которым назначена одна из следующих ролей:

- главный администратор;
- аудитор;
- администратор сети;
- администратор ключей.

Главный администратор и аудитор обладают всеми правами, которые необходимы для работы с записями журналов. Для данных учетных записей доступны все возможности управления записями о событиях и настройки параметров хранения журналов. Права администратора сети и администратора ключей ограничены — пользователь не может настраивать параметры, влияющие на сохранность записей.

Для проведения аудита установите программы:

- конфигуратор БД журналов ЦУС и СД (далее — конфигуратор) (см. стр. **12**);
- агент ЦУС и СД (далее — агент);
- программа просмотра журналов;
- программа просмотра отчетов;
- программа управления сервером доступа.

Журналы

Журналы регистрации событий

Список регистрационных журналов комплекса представлен в Табл.1.

Табл.1 Регистрационные журналы комплекса

Объекты	Журналы
ЦУС	Системный журнал. Журнал несанкционированного доступа
КШ (в том числе КШ с ЦУС)	Системный журнал. Журнал несанкционированного доступа. Журнал сетевого трафика
Детектор атак	Системный журнал. Журнал несанкционированного доступа
Криптокоммутатор	Системный журнал. Журнал несанкционированного доступа. Журнал сетевого трафика
Сервер доступа	Журнал сервера доступа
Агент ЦУС и СД	Журнал приложения

Примечание.
На КШ с ЦУС формируются журналы криптографического шлюза и журналы ЦУС.

Далее в настоящем руководстве, если это не оговорено особо, под терминами "системный журнал" и "журнал НСД" подразумеваются соответствующие журналы всех сетевых устройств.

Содержимое журналов с указанных объектов перемещается агентом ЦУС на хранение в базу данных. События, связанные с работой агента ЦУС, регистрируются в отдельном журнале базы данных — журнале приложения.

Для просмотра аудитором записи журналов загружаются в программе просмотра журналов комплекса.

Очистка журналов выполняется в следующих режимах:

- автоматический;
- ручной.

Автоматическая очистка выполняется по расписанию, сформированному для агента ЦУС средствами программы управления комплексом. Ручная очистка выполняется администратором с помощью программы просмотра журналов.

События, происходящие на сетевых устройствах, регистрируются в их локальных журналах. Для централизованного доступа к записям содержимое локальных журналов перемещается через ЦУС на хранение в базу данных.

Порядок перемещения журналов реализован следующим образом. Каждое сетевое устройство локально хранит записи журналов до момента их передачи центру управления сетью криптографических шлюзов. При наличии связи с ЦУС отправка содержимого журналов осуществляется по мере регистрации событий. После передачи записи удаляются из локальных журналов сетевых устройств. Если связь с ЦУС отсутствует, записи накапливаются в локальных журналах.

На ЦУС выделен специальный буфер для временного хранения принятых записей журналов. Аналогично локальным журналам сетевых устройств записи хранятся в буфере до момента их передачи в базу данных ЦУС. Передача журналов из буфера ЦУС в базу данных осуществляется агентом ЦУС и СД по заданному расписанию или по команде аудитора.

Для обеспечения сохранности записей журналов и их своевременного получения настраиваются следующие параметры:

- локальных журналов сетевых устройств (см. стр. **45**);
- расписания передачи журналов в базу данных (см. стр. **38**);
- очистки базы данных от устаревших записей журналов (см. стр. **39**).

События, зарегистрированные сервером доступа, временно хранятся в его буфере. Срок хранения событий определяется расписанием автоматической передачи журналов в базу данных. Расписание настраивается в свойствах агента. С момента регистрации и до передачи журналов в базу данных события доступны для просмотра в программе управления сервером доступа.

Системный журнал

В системном журнале регистрируются события, связанные с работой подсистем сетевых устройств. Для каждого зарегистрированного события сохраняются время регистрации, название события, категория и ряд дополнительных параметров.

В Табл.2 и Табл.3 представлены описания категорий регистрируемых событий и список полей системных журналов сетевых устройств.

Табл.2 Категории событий, регистрируемых в системных журналах

Категория события	Журнал	Описание
Управляющая команда	ЦУС, КШ, ДА, КК	Команды управления комплексом
Задача	КШ, ДА, КК	Задания на синхронизацию
Статус выполнения задачи	КШ, ДА, КК	Успешное/неуспешное завершение выполнения задачи
Конфликт версий	КШ, ДА, КК	Конфликт адресов IP
Сеть "Континент"	ЦУС, КШ, ДА, КК	События, связанные с работой сети
Журнал ключевой системы	ЦУС, КШ, ДА, КК	События, связанные с изменением ключевой информации на СУ
Безопасность виртуального коммутатора	КК	События, связанные с работой криптокоммутатора в режиме безопасности

Табл.3 Список полей системного журнала

Поле	Описание
Дата/Время	Дата и время регистрации события в часовом поясе пользователя программы просмотра журналов. Часовой пояс определяется региональными настройками компьютера, на котором запущена программа просмотра журналов
Дата/Время на СУ	Дата и время регистрации события в часовом поясе сетевого устройства
Категория события	Наименование категории события
Событие	Наименование события
Описание	Детальное описание события

Журнал НСД

В журнале НСД хранятся записи о зарегистрированных событиях возможных угроз безопасности.

В Табл.4 представлен список полей журнала НСД, в Табл.5 представлено описание подсистем — источников событий НСД.

Табл.4 Список полей журнала НСД

Поле	Описание
Дата/Время	Дата и время регистрации события в часовом поясе пользователя программы просмотра журналов. Часовой пояс определяется региональными настройками компьютера, на котором запущена программа просмотра журналов
Дата/Время на СУ	Дата и время регистрации события в часовом поясе СУ
Название подсистемы	Название подсистемы, зарегистрировавшей событие
Количество событий	Количество зафиксированных событий НСД этого типа в течение 1 мин.
Описание	Детальное описание произошедшего события

Табл.5 Подсистемы, регистрирующие события НСД

Подсистема		Журнал	Название события	Описание
	ЦУС	ЦУС	Неверная имитовставка от КШ	IP-адрес или диапазон адресов источника
			Администратор заблокирован согласно политике аутентификации	IP-адрес или диапазон адресов источника
			Неудачная попытка соединения с ЦУС. Возможно, неверный ключ или пароль администратора	Адрес источника: имя учетной записи, под которой было выполнено обращение к ЦУС
			Неверный номер входящего пакета	IP-адрес или диапазон адресов источника
	Управление КШ	КШ	Неверная имитовставка	IP-адрес или диапазон адресов источника
			Неверный номер входящего пакета	IP-адрес или диапазон адресов источника
	Шифратор	КШ, ДА, КК	Неправильный номер пакета	IP-адрес источника
			Неверная имитовставка	IP-адрес источника
	Контроль целостности	КШ, ДА, КК	Ошибка контроля целостности	Полное имя файла
	Аутентификация	КШ	Неуспешная аутентификация	IP-адрес хоста, дата, логин
	Пакетный фильтр	КШ	Направление пакета	Диапазон адресов отброшенных пакетов
	Сигнатурный/эвристический анализатор	ДА	Сигнатурный/эвристический анализатор	Описание атаки
	Безопасность виртуального коммутатора	КК	Неизвестный хост	MAC-адрес, имя интерфейса
			Подмена MAC-адреса	MAC-адрес, имя интерфейса, виртуальный коммутатор
			Переполнение таблицы MAC-адресов	MAC-адрес последнего пакета за минуту

Журнал сетевого трафика

В журнале сетевого трафика сохраняются сведения о работе фильтра IP-пакетов криптошлюза и криптокоммутатора. В зависимости от заданных параметров в журнале регистрируются IP-пакеты, отброшенные фильтром или не соответствующие ни одному правилу фильтрации. Регистрация IP-пакетов, отброшенных фильтром или не соответствующих ни одному правилу, осуществляется также и в журнале НСД.

Примечание.

При интенсивном трафике журнал периодически переполняется с последующей автоматической очисткой, и часть информации теряется. Переполнение журналов происходит как на КШ/КК, так и на ЦУС. Рекомендуется использовать режим регистрации всех пакетов в журнале сетевого трафика только при вводе комплекса в эксплуатацию. Анализ трафика на наличие атак в процессе эксплуатации рекомендуется проводить с помощью специальных средств, подключенных к SPAN-порту КШ/КК.

Описание используемых графических обозначений и список полей журнала сетевого трафика представлены в Табл.6, Табл.7, Табл.8.

Табл.6 Пиктографические обозначения IP-пакетов

Пиктографическое обозначение	Описание
	Входящий IP-пакет
	Исходящий IP-пакет
	IP-пакет, отброшенный по блокирующему правилу в мягком режиме работы фильтра
	Включен мягкий режим работы фильтра

Табл.7 Цвет обозначения IP-пакетов

Цвет	Описание
Зеленый	IP-пакет пропущен в соответствии с правилом фильтрации
Красный	IP-пакет отброшен в соответствии с правилом фильтрации
Синий	IP-пакет отброшен как не соответствующий ни одному правилу фильтрации

Табл.8 Список полей журнала сетевого трафика

Поле	Описание
Дата/Время	Дата и время регистрации IP-пакета в часовом поясе пользователя программы просмотра журналов. Часовой пояс определяется региональными настройками компьютера, на котором запущена программа просмотра
Дата/Время на СУ	Дата и время регистрации IP-пакета в часовом поясе криптошлюза, криптокоммутатора
Протокол	Название протокола
Источник	IP-адрес отправителя IP-пакета
Приемник	IP-адрес получателя IP-пакета
Интерфейс	Наименование интерфейса
Длина пакета	Размер IP-пакета (байт)
ПФ/ПТ	Наименование правила фильтрации или правила трансляции, примененного к IP-пакету

Журнал приложения

В журнале приложения фиксируются события, связанные с работой агента ЦУС. В журнале сохраняются сведения о:

- загрузке журналов;
- очистке журналов;
- командах на немедленную очистку журналов, поступающих из ППЖ;
- возникающих при работе агента проблемах (потеря соединения с СУБД, потеря соединения с ЦУС и т. п.).

В Табл.9 приведен список полей журнала приложения.

Табл.9 Список полей журнала приложения

Поле	Описание
Дата/Время	Дата и время регистрации события
Подсистема	Название компонента, выполнившего действие (агент или программа просмотра журналов)

Поле	Описание
Имя компьютера	Сетевое имя компьютера, с которого поступила команда на выполнение действия. Регистрируется для событий, инициированных программой просмотра журналов и агентом
Пользователь	Для событий, инициированных программой просмотра журналов — имя пользователя, открывшего сеанс работы на указанном компьютере. Для событий, инициированных агентом под учетной записью Windows — имя пользователя, открывшего сеанс работы на указанном компьютере. Для событий, инициированных агентом под учетной записью СУБД — имя компьютера
Описание	Детальное описание произошедшего события

Журнал сервера доступа

В журнале сервера доступа фиксируются события, произошедшие на серверах доступа сети "Континент". В Табл.10 представлен список полей журнала сервера доступа.

Табл.10 Список полей журнала сервера доступа

Поле	Описание
Дата/Время	Дата и время регистрации события
Дата/Время на КШ	Дата и время регистрации события с учетом часового пояса КШ
Пользователь	Имя пользователя абонентского пункта — источника события
Событие	Название зарегистрированного события
IP-адрес	IP-адрес абонентского пункта — источника события
Описание	Детальное описание произошедшего события

Интерфейс программы управления ЦУС

Централизованное управление сетевыми устройствами осуществляется с помощью специальной программы управления, устанавливаемой на одном или нескольких компьютерах, находящихся в защищенном сегменте сети (РМ администратора). Программа управления устанавливает защищенное соединение с ЦУС и позволяет в диалоговом режиме контролировать все сетевые устройства, а также редактировать данные, содержащиеся в базе данных ЦУС.

При запуске ПУ ЦУС осуществляется аутентификация администратора. Аутентификация выполняется в соответствии с политикой, заданной по умолчанию или измененной главным администратором комплекса.

Для запуска программы управления:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите "Программа управления ЦУС (ПУ ЦУС)".

   На экране появится запрос идентификатора администратора.

2. Предъявите идентификатор администратора.

   На экране появится запрос пароля для расшифровки ключей администратора.

3. Введите пароль и нажмите кнопку "ОК".

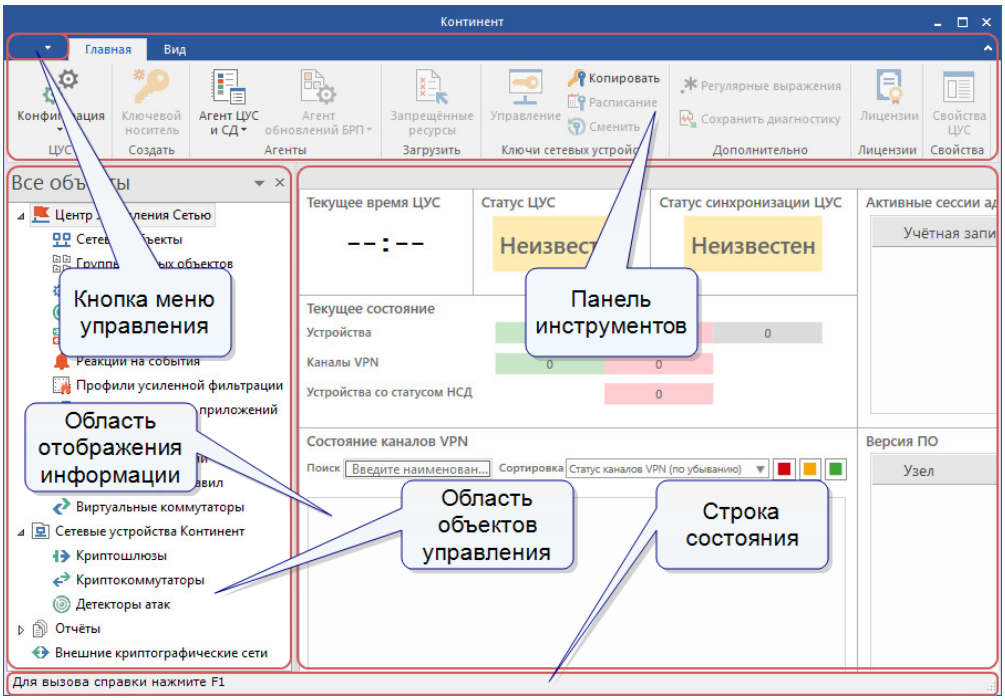
   При успешном чтении служебной информации с идентификатора программа управления установит защищенное соединение с ЦУС и агентом, загрузит данные, необходимые для ее работы, и отобразит на экране главное окно.

Если носитель поврежден или не содержит административного ключа, соединение с ЦУС установлено не будет и на экране появится сообщение об ошибке. В этом случае закройте окно сообщения и повторите процедуру запуска с надлежащим носителем.

Совет.

Если при установлении соединения произошел сбой и на экран выведено сообщение о невозможности соединения с ЦУС, проверьте работоспособность ЦУС и повторите попытку соединения с ним еще раз. Сообщение об ошибке может содержать техническую информацию для разработчиков. При обращении в службу технической поддержки необходимо представить снимок экрана с сообщением или полный текст сообщения, включая техническую информацию.

После запуска ПУ ЦУС и успешной аутентификации на экране отображается главное окно приложения.



Окно ПУ ЦУС содержит следующие элементы интерфейса:

Элемент интерфейса	Описание
Панель инструментов	Содержит набор инструментов на вкладках: • "Главная" — основные инструменты; • "Вид" — настройка отображения элементов интерфейса и ряда объектов ПУ ЦУС. На вкладках расположены функциональные кнопки, предназначенные для запуска часто используемых команд. Состав кнопок зависит от выбора объекта на панели навигации, а их доступность определяется текущей ситуацией. При наведении курсора мыши на кнопку появляется всплывающая подсказка с дополнительной информацией
Кнопка меню управления	Кнопка предназначена для доступа к меню управления и меню настройки параметров ПУ ЦУС
Область объектов управления	Содержит список объектов комплекса
Область отображения информации	Содержит информацию выбранного раздела или пункта из списка объектов
Строка состояния	Отображает в реальном времени данные мониторинга

Конфигуратор

Конфигуратор предназначен для решения следующих задач:

- настройка параметров подключения агента к СУБД;
- обеспечение доступа администраторов комплекса к БД журналов.

Конфигуратор предоставляет администратору СУБД следующие возможности:

- дистанционно подключиться к серверу СУБД;
- сконфигурировать базу данных для хранения журналов;
- записать сведения, необходимые агенту для подключения к БД, в реестр компьютера.

Интерфейс конфигуратора

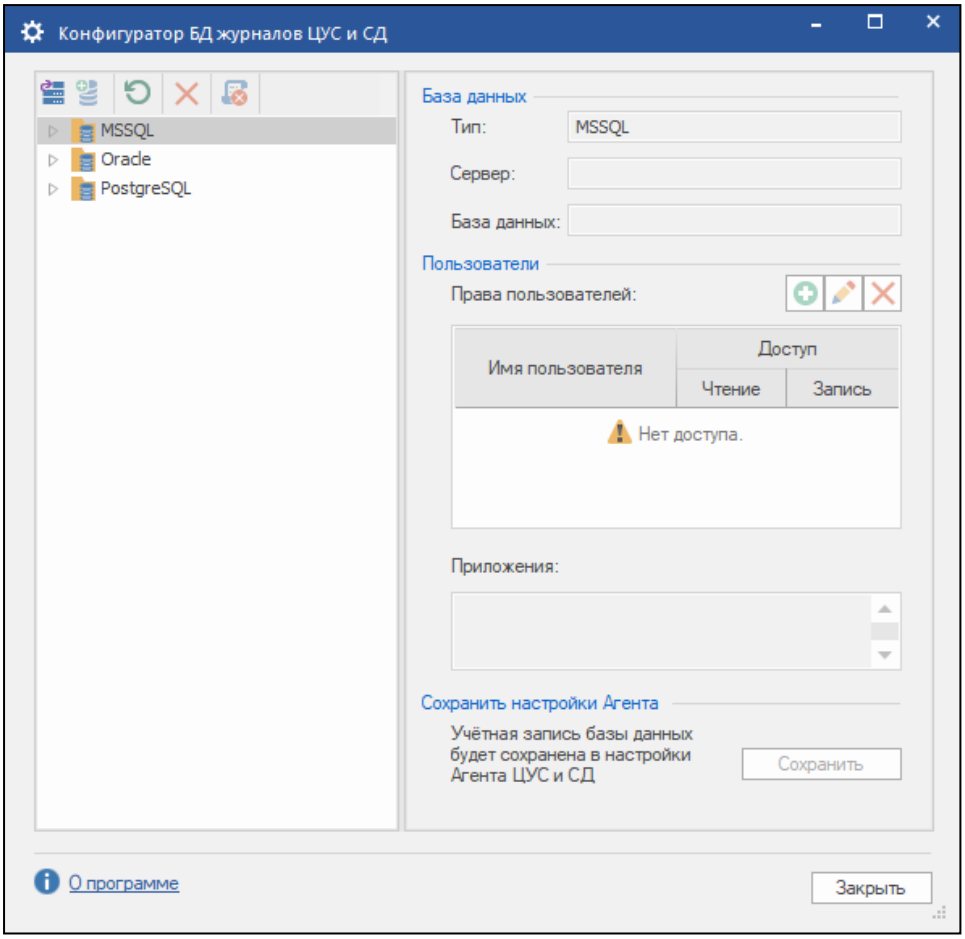


Рис.1 Интерфейс конфигуратора

В левой части окна отображается иерархический список объектов. В правой верхней части окна — настройки агента для подключения к СУБД. В правой нижней части окна — список учетных записей администраторов комплекса для доступа к БД журналов.

Управление объектами осуществляют с помощью команд контекстного меню и кнопок на панели инструментов в Табл.11.

Табл.11 Команды управления объектами

	Команда	Описание
	Подключиться к серверу	Запускает процедуру подключения конфигуратора к серверу БД с правами администратора
	Создать базу	Запускает процедуру создания базы данных
	Обновить	Обновляет в иерархическом списке отображаемые сведения о выбранном объекте
	Удалить базу	Удаляет выбранную базу данных
	Очистить логи	Выполняет очистку журналов выбранной базы данных

Внимание! Перед удалением подключенной БД PostgreSQL необходимо завершить все сессии с ее сервером.

Интерфейс конфигуратора

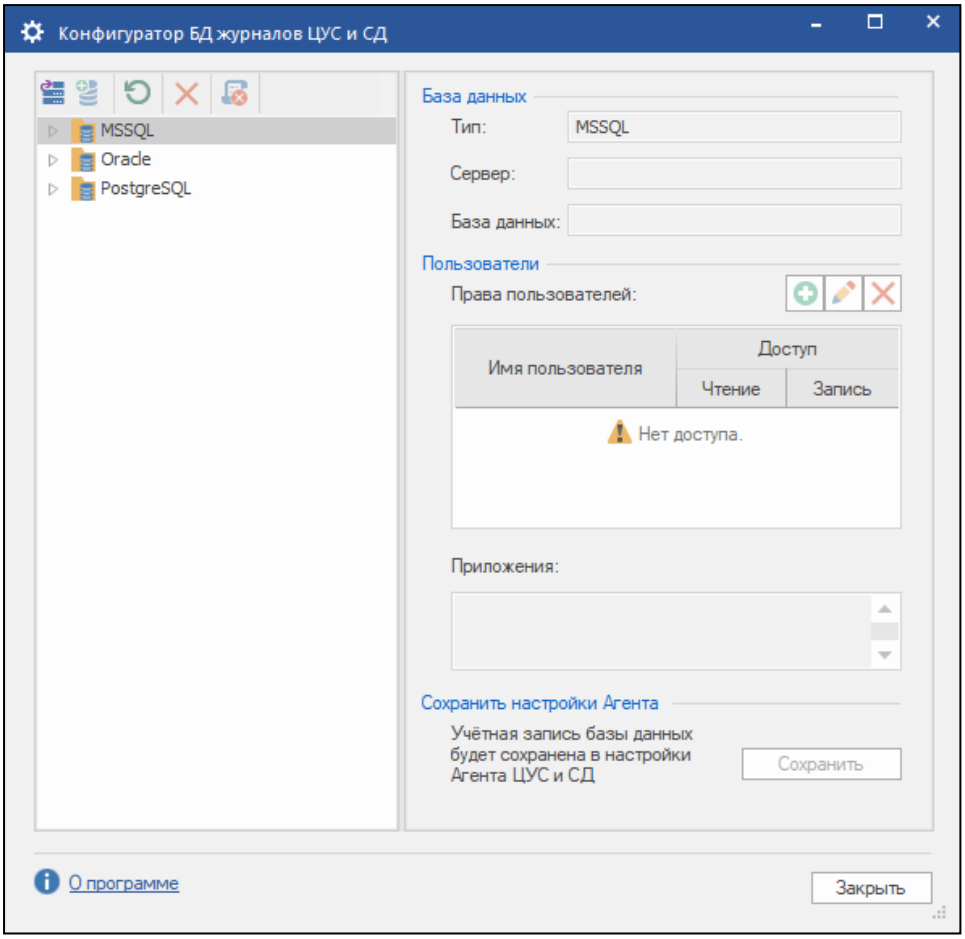


Рис.2 Интерфейс конфигуратора

В левой части окна отображается иерархический список объектов. В правой верхней части окна — настройки агента для подключения к СУБД. В правой нижней части окна — список учетных записей администраторов комплекса для доступа к БД журналов.

Управление объектами осуществляют с помощью команд контекстного меню и кнопок на панели инструментов в Табл.12.

Табл.12 Команды управления объектами

	Команда	Описание
	Подключиться к серверу	Запускает процедуру подключения конфигуратора к серверу БД с правами администратора
	Создать базу	Запускает процедуру создания базы данных
	Обновить	Обновляет в иерархическом списке отображаемые сведения о выбранном объекте
	Удалить базу	Удаляет выбранную базу данных
	Очистить логи	Выполняет очистку журналов выбранной базы данных

Внимание! Перед удалением подключенной БД PostgreSQL необходимо завершить все сессии с ее сервером.

Агент и единый ключевой носитель

Агент ЦУС и СД обеспечивает:

- установление защищенного соединения с ЦУС для получения содержимого журналов регистрации в соответствии с установленным расписанием;
- установление защищенного соединения с СД для получения содержимого журналов регистрации в соответствии с установленным расписанием;
- очистку журналов регистрации в соответствии с установленным расписанием;
- автоматическое сохранение в зашифрованном виде резервной копии конфигурации ЦУС в соответствии с установленным расписанием.

При настройке агента определяют следующие параметры:

- расписание получения журналов от ЦУС;
- расписание очистки журналов;
- пароль для зашифрования резервной копии конфигурации ЦУС;
- расписание сохранения резервной копии конфигурации ЦУС и папку для архивных копий.

Для подключения агента к ЦУС и СД создайте единый ключевой носитель (ЕКН) .

Внимание!
Для корректной работы с ключевыми носителями eToken и Рутокен в настройках Windows необходимо запустить системную службу "Смарт-карты", предварительно установив тип запуска – "Авто".

Интерфейс агента

После запуска программы управления агентом в правом углу панели задач появляется пиктограмма "Программа управления агентом ЦУС и СД". Пиктограмма отображает текущее состояние агента, а также наличие события НСД на каком-либо СУ. Используемые для этой цели пиктографические изображения, а также сведения о командах контекстного меню данной пиктограммы представлены в Табл.13 и Табл.14.

Оповещение об ошибках в работе агента осуществляется с помощью всплывающих сообщений в правой нижней части экрана. Более подробные сведения об ошибках фиксируются в регистрационном журнале ОС "Просмотр событий| Приложение".

Табл.13 Пиктографические обозначения состояний агента

Пиктограмма	Описание
	Связь между агентом и ЦУС установлена
	Связь между агентом и ЦУС отсутствует
	Агент остановлен
	На одном из устройств зафиксировано событие несанкционированного доступа

Табл.14 Команды контекстного меню программы управления агентом

Название команды	Описание
Запустить агент	Осуществляет запуск агента
Остановить агент	Осуществляет остановку агента
Параметры агента...	Открывает окно программы управления агентом, предназначенное для просмотра и настройки параметров агента
Журнал приложений системы	Вызывает на экран журнал приложений Windows
О программе...	Открывает окно, содержащее сведения о номере версии программы управления агентом, а также сведения об авторских правах на программный продукт
Выход	Осуществляет выход из программы управления агентом и удаляет пиктограмму с панели задач

Примечание.
Полный набор команд доступен при запуске агента от имени администратора.

Агент собирает журналы с ЦУС и всех СД комплекса. Для подключения к каждому объекту агенту требуется:

- указать сетевой адрес объекта;
- предъявить специальный ключ, индивидуальный для каждого объекта.

Ключи создаются при инициализации объекта и записываются в файле contkey.str на отдельный отчуждаемый носитель — идентификатор администратора.

Единый ключевой носитель содержит ключевую информацию и адреса всех объектов также в файле contkey.str. Для создания и обновления ЕКН используют программу "Менеджер ключей".

IP-адреса и ключи записываются в специальное хранилище (контейнер) на носитель.

Программа просмотра журналов

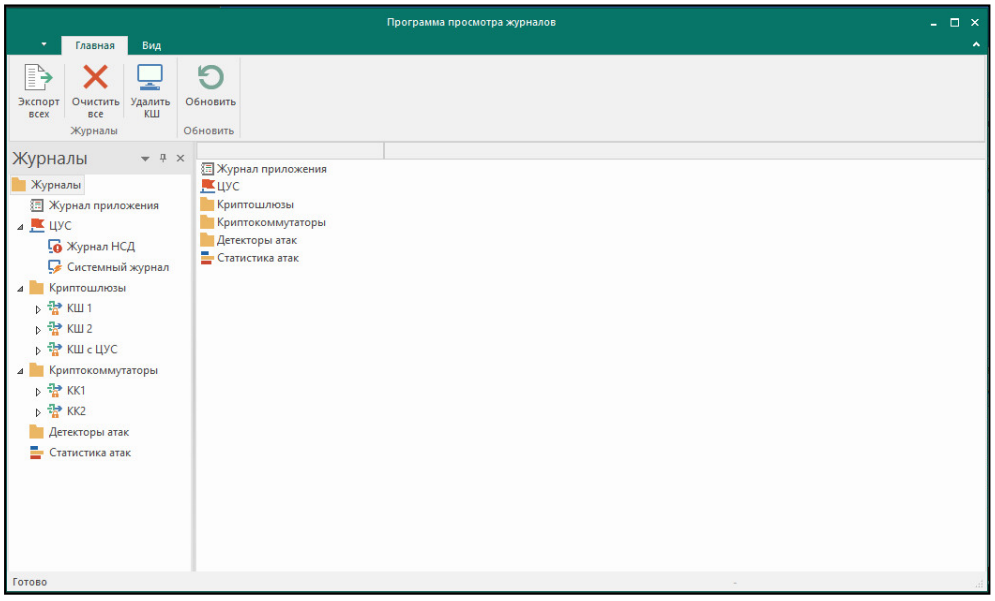
Программа просмотра журналов комплекса устанавливается на РМ администратора по умолчанию вместе с ПУ ЦУС.

Программа предоставляет следующие возможности:

- загрузка записей журналов регистрации из базы данных ЦУС;
- управление отображением записей;
- сохранение записей в файлы;
- очистка содержимого журналов в базе данных (только для главного администратора и аудитора).

Для работы с программой предъявите ключ и укажите пароль администратора комплекса.

При заданной по умолчанию настройке интерфейса основное окно программы просмотра журналов имеет вид:



Для удобства работы с программой элементы интерфейса обладают рядом возможностей по настройке. Пользователь может изменять состав отображаемых элементов и их расположение на экране. Внешний вид основного окна программы сохраняется в системном реестре компьютера и используется в следующих сеансах работы пользователя с программой.

Табл.15 Элементы интерфейса основного окна программы просмотра журналов

Элемент	Описание
Меню	Содержит команды управления программой
Панель инструментов	Содержит кнопки быстрого вызова команд управления и программных средств

Элемент	Описание
Окно структуры журналов	Окно предназначено для выбора журналов в иерархическом списке объектов. В структуре представлены журналы, хранящиеся в базе данных: журнал приложения, журналы ЦУС, журналы КШ, журналы ДА, журналы КК
Область отображения записей	Предназначена для просмотра записей выбранного журнала (при выборе любого другого объекта структуры отображается список объектов следующего уровня подчинения). Список записей выводится в табличной форме. Колонки таблицы соответствуют полям записей журнала. Для вывода компактного списка основных сведений о зарегистрированном событии наведите указатель мыши на нужную строку таблицы. Через 1–2 секунды появится всплывающее окно, которое содержит информацию о событии
Строка сообщений	Отображает служебные сообщения программы, а также краткие подсказки к командам и кнопкам панели инструментов. В правой части строки отображаются номер страницы и количество загруженных записей

Программа просмотра отчетов

Для формирования и получения отчетов используется программа просмотра отчетов. Программа устанавливается на любой компьютер защищенного сегмента сети, к которой подключен один из интерфейсов КШ с установленным ЦУС.

Формирование отчета осуществляется на основании запроса, отправляемого из ППО в ЦУС. Для соединения с ЦУС укажите параметры соединения и предъявите ключ администратора комплекса. Список доступных отчетов зависит от роли администратора. Сформированный отчет отображается в формате Crystal Reports и может быть распечатан и сохранен в файл.

Окно программы состоит из трех панелей и области отображения отчета.

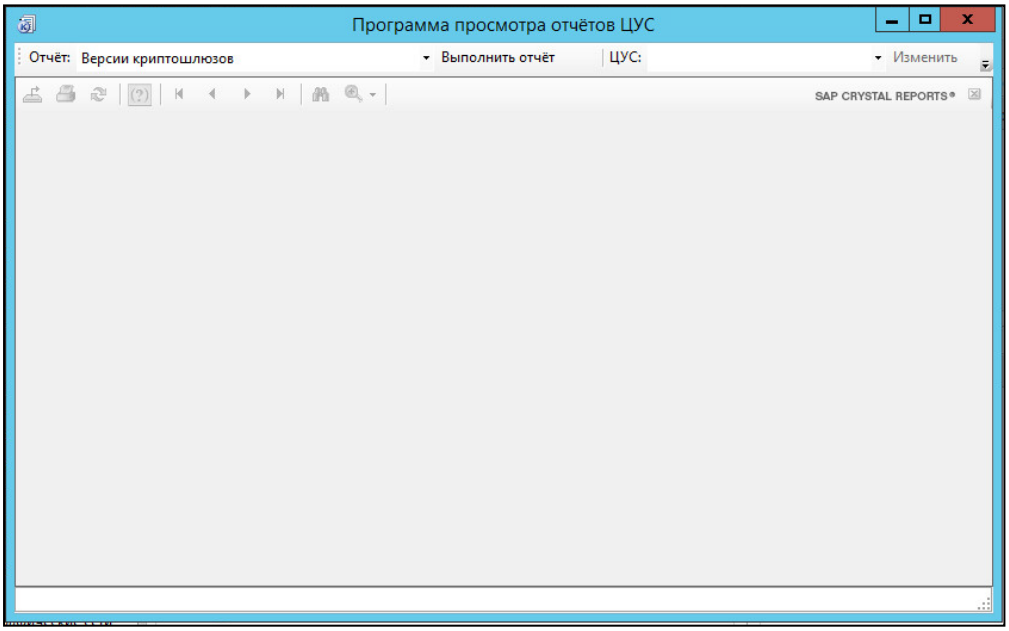


Рис.3 Окно программы просмотра отчетов

Верхняя панель предназначена для выбора вида отчета и настройки соединения с ЦУС. На панели расположены:

- раскрывающийся список выбора вида отчета;
- кнопка "Выполнить отчет" для отправки запроса ЦУС на формирование отчета;
- раскрывающийся список выбора ЦУС (список соединений);
- кнопка "Изменить" для настройки параметров соединения с ЦУС, выбранным в раскрывающемся списке;
- кнопка "Удалить" для удаления выбранного в раскрывающемся списке ЦУС.

На средней панели расположены кнопки, предназначенные для навигации по содержимому отчета и выполнения операций печати и экспорта:

-  — экспортировать отчет;
-  — распечатать отчет;
-  — обновить на сервере;
-  — копировать отчеты;
-  — показать или скрыть панель параметров;
-  — перелистывание по страницам отчета;
-  — поиск по тексту отчета;
-  — изменение масштаба просматриваемого отчета.

На нижней панели отображается название сформированного отчета.

Примечание.
Нижняя панель появляется только после формирования отчета.

Отчет "Правила фильтрации по КШ" состоит из разделов по количеству КШ комплекса. При открытии отчета отображается список разделов. Для просмотра раздела необходимо выбрать его в списке. При открытии каждого из разделов их заголовки отображаются на панели после названия отчета. Для удаления открытого раздела из области просмотра используется кнопка отмены отображения раздела.

Глава 2
Эксплуатация

Настройка системы

Перед настройкой АПКШ "Континент" для выполнения задачи аудита установите СУБД, например, PostgreSQL. На текущий момент в качестве БД для хранения журналов может использоваться PostgreSQL 14 из состава ОС Astra Linux 1.7 (сертификат соответствия № 2557 от 27.01.2012). После установки СУБД запустите конфигуратор.

Для запуска конфигуратора:

- В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите программу "Конфигуратор БД журналов ЦУС и СД".

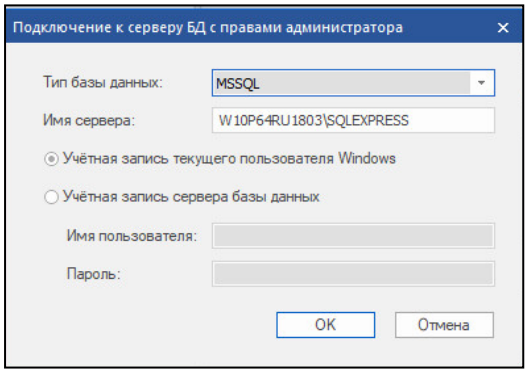
  На экране появится окно конфигуратора (см. Рис.2).

Подключение конфигуратора к серверу БД

Для подключения к серверу БД:

1. Вызовите на экран окно конфигуратора.
2. Нажмите кнопку "Подключиться к серверу".

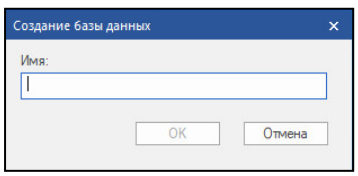
   На экране появится окно "Подключение к серверу БД с правами администратора".



3. Заполните поля диалога и нажмите кнопку "OK".

Тип базы данных	Тип базы данных (поле не редактируется)
Имя сервера	Сетевое имя сервера БД
Учетная запись текущего пользователя Windows	При наличии отметки подключение к СУБД выполняется под текущей учетной записью Windows
Учетная запись сервера базы данных	При наличии отметки подключение к СУБД выполняется под учетной записью, указанной ниже
Имя пользователя	Имя пользователя, зарегистрированного в СУБД
Пароль	Пароль пользователя, зарегистрированного в СУБД

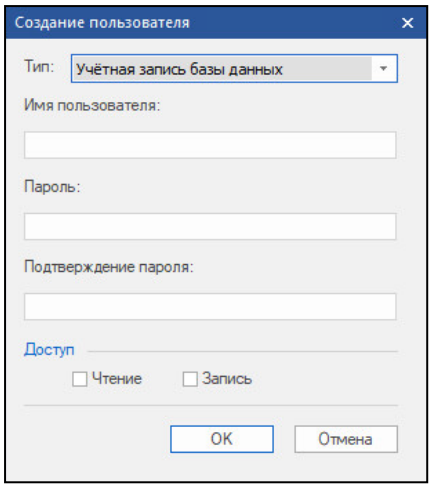
4. Нажмите кнопку "Создать базу данных" и в появившемся окне введите имя базы.



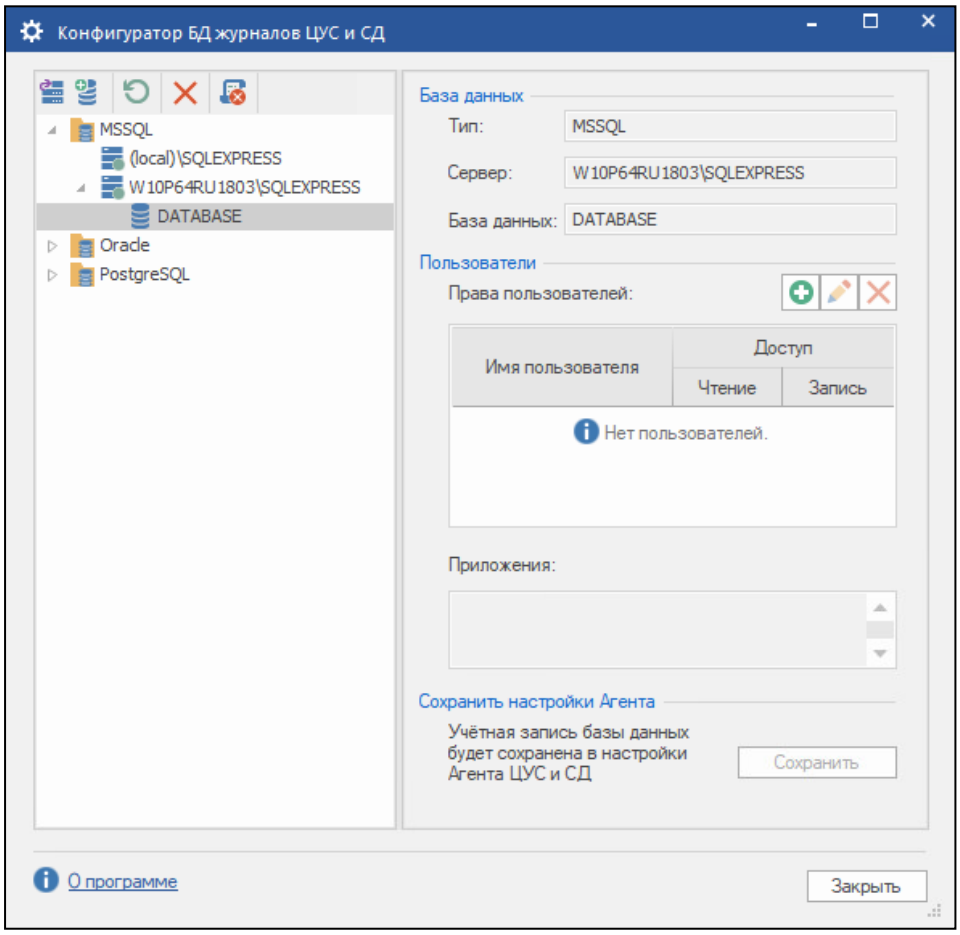
   Новая база данных появится в списке.

5. В правой области окна в разделе "Пользователи" нажмите кнопку .

На экране появится окно создания пользователя.



6. Заполните поля и нажмите кнопку "ОК".
   Созданный пользователь появится в таблице.



7. Нажмите кнопку "Сохранить".
   На экране появится окно с параметрами созданной учетной записи.
8. Нажмите кнопку "ОК",чтобы сохранить учетную запись.
9. Для выхода из конфигуратора нажмите кнопку "Закрыть".

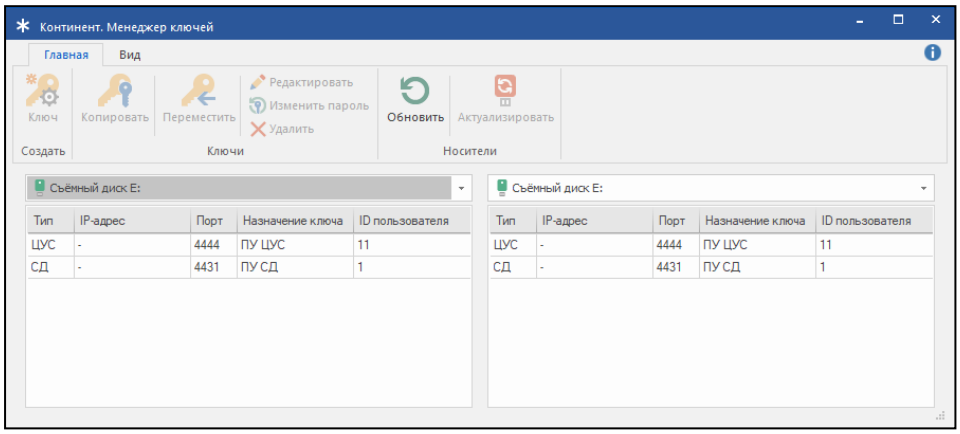
Подключение агента ЦУС и СД

Для подключения агента к ЦУС и СД создайте единый ключевой носитель с помощью программы "Менеджер ключей".

Для запуска программы выполните одно из следующих действий:

- В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите пункт "Менеджер ключей".
- В программе управления ЦУС на панели инструментов нажмите кнопку "Ключевой носитель".

  На экране появится главное окно программы.



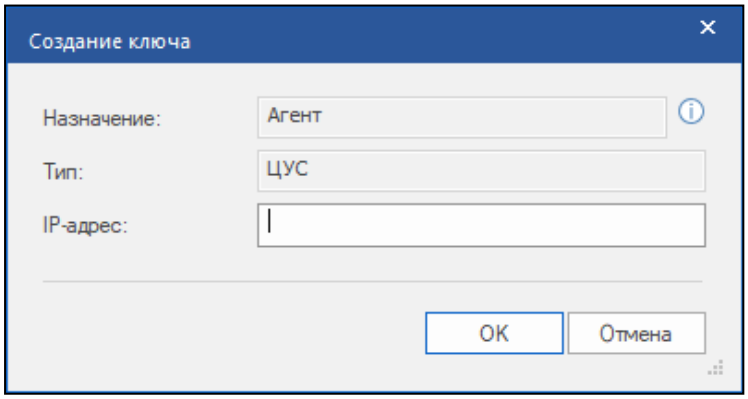
Для создания ЕКН:

1. Подключите исходный ключевой носитель и ЕКН к считывателю.
2. Выберите в левой части Менеджера ключей в раскрывающемся списке исходный ключевой носитель.

   В списке ключевых контейнеров отобразятся все контейнеры на носителе.
3. Выберите в списке необходимый ключевой контейнер и на панели инструментов Менеджера ключей нажмите кнопку "Ключ".

   Откроется окно для ввода пароля.
4. Введите текущий пароль.

   Откроется окно "Создание ключа".



5. Укажите IP-адрес объекта и нажмите кнопку "ОК".

   Появится сообщение об успешном создании ключа.
6. Нажмите кнопку "ОК".

   Созданный ключ отобразится в списке ключевых контейнеров исходного носителя.
7. Выберите в правой части Менеджера ключей в раскрывающемся списке ЕКН.
8. Выберите созданный ключ и на панели инструментов Менеджера ключей нажмите кнопку "Копировать".

   Откроется окно для ввода пароля.
9. Введите текущий пароль.

   Ключевой контейнер будет скопирован.

10. Выполните пп. 2–9 для каждого объекта.

Агент запускается двумя способами:

- автоматически;
- вручную.

Для автоматического запуска агента:

- Перезагрузите компьютер, на котором установлен агент, и предъявите ЕКН до окончания загрузки операционной системы.

  При успешном чтении ключевой информации агент будет запущен, а в правом углу панели задач появится пиктограмма "Программы управления агентом", отображающая состояние связи между агентом и ЦУС.

Для запуска агента вручную:

1. Предъявите ЕКН.
2. Вызовите контекстное меню программы управления агентом и активируйте команду "Запустить агент".

   При успешном чтении ключевой информации агент будет запущен.

Примечание.
Если носитель испорчен или не содержит административного ключа, на экране появится всплывающее сообщение об ошибке. Предъявите надлежащий носитель и запустите агент вручную.

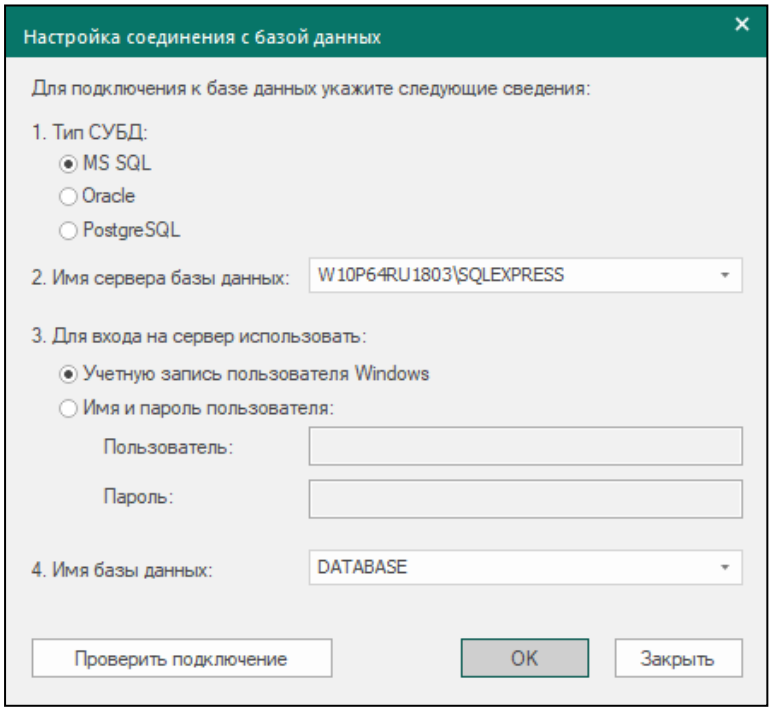
Подключение программы просмотра журналов

Запустите программу просмотра журналов. Для подключения программы просмотра журналов к базе данных настройте параметры соединения. Если при установке ППЖ эти параметры не были определены, то при первом запуске программы просмотра журналов на экране автоматически появляется окно настройки.

Для настройки параметров соединения с базой данных:

1. Нажмите кнопку управления и выберите пункт "Параметры соединения с БД".

   На экране появится окно настройки параметров соединения.



2. Установите отметку в поле с названием типа базы данных — MS SQL, Oracle или PostgreSQL.
3. В поле "Имя сервера базы данных" выберите сетевое имя.

Примечание.
БД Oracle. Если раскрывающийся список значений пуст, проверьте правильность настройки клиента Oracle.
БД MS SQL. Выберите сетевое имя компьютера, на котором установлен сервер БД. В случае использования локального сервера введите с клавиатуры значение "(local)".

4. Укажите режим идентификации пользователя программы просмотра журналов:
   - чтобы идентификация при обращении к базе данных осуществлялась от имени пользователя, открывшего сеанс работы в ОС Windows (с учетными данными, указанными при входе в систему), — установите отметку в поле "Учетную запись пользователя Windows";
   - чтобы идентификация осуществлялась от имени пользователя СУБД, установите отметку в поле "Имя и пароль пользователя" и введите имя и пароль этого пользователя.

   Примечание.
   Для обращения к базе данных пользователю должны быть предоставлены права доступа (см. стр. 12).
5. В раскрывающемся списке "Имя базы данных" выберите имя используемой схемы (базы данных).
6. Нажмите кнопку "ОК".

   Примечание.
   Для проверки возможности подключения к базе данных с заданными параметрами используйте кнопку "Проверить подключение".

Для отключения соединения:

- Нажмите кнопку управления и выберите пункт "Отключение" (команда доступна, если установлено соединение с базой данных).

Для подключения к базе данных:

- Нажмите кнопку управления и выберите пункт "Соединение с БД" (команда доступна, если соединение с базой данных не установлено).

Предусмотрено несколько способов запуска программы просмотра журналов.

Примечание.
Если при установке ППЖ не были определены параметры соединения с ЦУС, то при первом запуске программы просмотра журналов на экране автоматически появляется диалог настройки параметров:
- IP-адрес интерфейса ЦУС, который подключен к сегменту сети, содержащему данный компьютер;
- время ожидания соединения в секундах (от 10 до 600 сек.);
- устройство для считывания ключа администратора.

Для запуска из главного меню Windows:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите пункт "Программа просмотра журналов ЦУС".

   На экране появится окно ввода пароля администратора.
2. Введите пароль администратора комплекса и нажмите кнопку "ОК".

   На экране появится окно программы просмотра журналов.

Для запуска из программы управления ЦУС:

1. Выполните запуск программы управления ЦУС (см. стр. 11).
2. В программе управления ЦУС в меню кнопки управления выберите пункт "Просмотр журналов".

   На экране появится окно ввода пароля администратора.
3. Введите пароль администратора комплекса и нажмите кнопку "ОК".

   На экране появится окно программы просмотра журналов.

Для запуска из программы управления ЦУС с выбором КШ:

1. Запустите программу управления ЦУС (см. стр. 11).
2. В программе управления ЦУС в иерархическом списке объектов выберите КШ.
3. В контекстном меню КШ выберите пункт "Просмотр журналов".

   На экране появится окно программы просмотра журналов. В иерархическом списке журналов автоматически будет выполнен переход к выбранному КШ.

Работа с программой просмотра журналов

Загрузка записей журналов

Для работы с записями журналов осуществите их загрузку в программу просмотра, выбрав нужный журнал. Загрузка записей выполняется из базы данных.

Выбор журнала

- Используя стандартные операции просмотра иерархических структур, перейдите к соответствующему объекту и выберите нужный журнал.

  Начнется процесс загрузки записей в программу просмотра. По окончании процесса записи журнала появятся в области отображения записей.

Ограничение количества записей

Максимальное количество одновременно загружаемых записей в ППЖ можно регулировать по желанию пользователя (по умолчанию 500).

Для ограничения количества загружаемых записей:

- Выберите значение в раскрывающемся списке поля "Количество одновременно загружаемых записей".

Обновление записей

Процедура обновления записей позволяет загрузить из базы данных новые записи выбранного журнала.

Для обновления записей:

- Выберите журнал, записи которого уже были загружены в программу, и нажмите кнопку "Обновить" (Обновить).

Фильтрация записей

При фильтрации осуществляется отбор для отображения тех записей, которые соответствуют некоторым критериям. За счет этого уменьшается количество отображаемых записей и облегчается поиск сведений.

Программа позволяет выполнять фильтрацию записей следующих журналов:

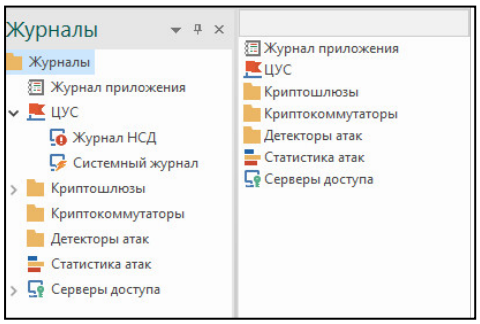
- системный журнал;
- журнал НСД;
- журнал сервера доступа;
- журнал сетевого трафика.

Фильтрация записей системного журнала и журнала НСД

Настройку и применение параметров фильтрации системного журнала выполняют после выбора журнала.

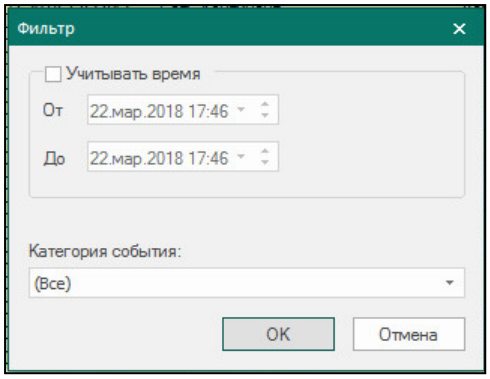
Для настройки параметров фильтрации:

1. Выберите журнал.



2. После загрузки записей нажмите кнопку "Фильтр" ( ).

   На экране появится диалог настройки параметров фильтрации.



3. Для фильтрации записей по времени задайте границы интервала. Установите отметку в поле "Учитывать время" и измените содержимое полей даты и времени.
4. В раскрывающемся списке поля "Категория события" выберите категорию (для системного журнала) или название подсистемы (для журнала НСД).
5. Нажмите кнопку "ОК".

   В области отображения записей останутся записи, удовлетворяющие заданным условиям отбора.

Фильтрация записей журнала сетевого трафика

Параметры фильтрации записей для журнала сетевого трафика могут быть заданы:

- вручную — пользователь осуществляет настройку параметров фильтрации самостоятельно;
- автоматически — параметры фильтрации задаются программой и обеспечивают вывод сведений, относящихся к выбранной записи журнала НСД. Данный способ фильтрации применяется в тех случаях, когда требуется отобразить сведения об IP-пакетах, вызвавших регистрацию события НСД в журнале НСД (регистрация события НСД осуществляется подсистемой "Пакетный фильтр").

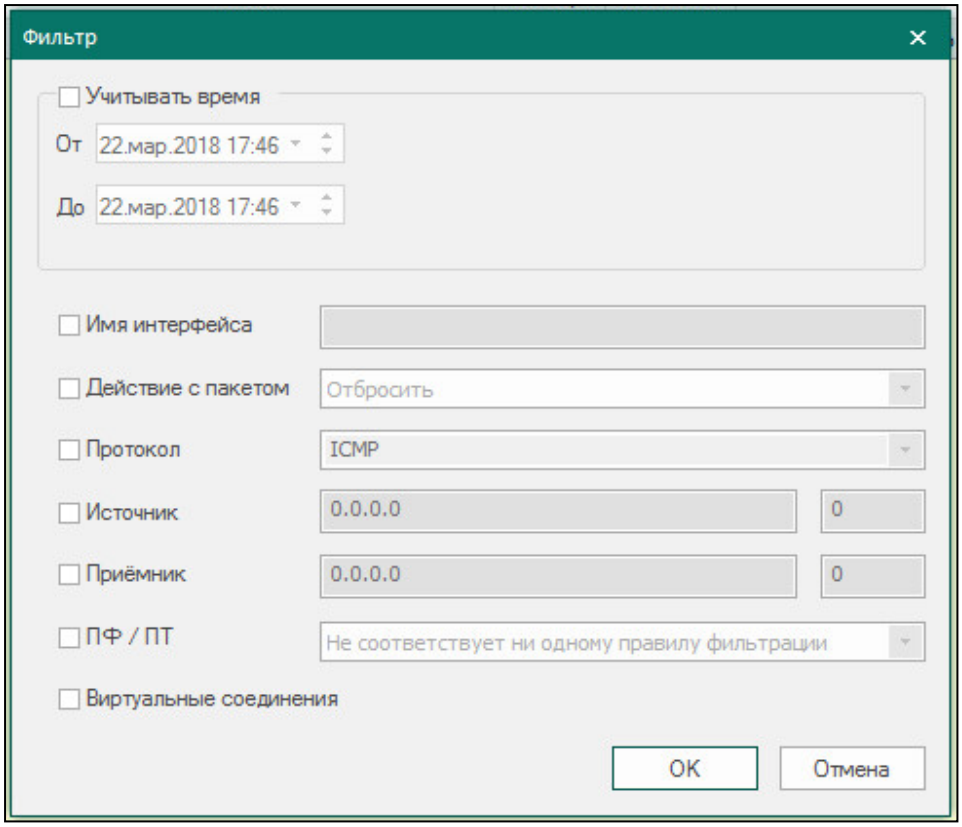
Для настройки параметров фильтрации вручную:

1. Выберите журнал.

   Примечание.

   Если фильтрация журнала была выполнена ранее, для выполнения фильтрации с другими параметрами нажмите кнопку "Фильтр" ( ).

   На экране появится окно настройки параметров фильтрации.



Примечание.
Опция "Просмотр пакетов" доступна только для журналов НСД.

Фильтрация записей осуществляется по заданным значениям параметров.

2. Отметьте параметры и укажите значения.

Учитывать время	Определяет границы интервала времени регистрации событий. Фильтру будут удовлетворять записи, которые были зарегистрированы в указанном интервале времени
Имя интерфейса	Определяет содержимое поля "Интерфейс" в записях журнала. Фильтру будут удовлетворять записи, содержащие заданное имя интерфейса (без учета регистра)
Действие с пакетом	Определяет выполненное действие с пакетом. Фильтру будут удовлетворять записи о регистрации IP-пакетов, над которыми было выполнено указанное действие (в программе просмотра журналов выполненные действия обозначаются пиктограммами — см. стр. **9**)
Протокол	Определяет содержимое поля "Протокол" в записях журнала. Фильтру будут удовлетворять записи, содержащие указанное имя протокола
Источник	Определяет содержимое поля "Источник" в записях журнала. Фильтру будут удовлетворять записи, содержащие указанный IP-адрес
Приемник	Определяет содержимое поля "Приемник" в записях журнала. Фильтру будут удовлетворять записи, содержащие указанный IP-адрес
ПФ/ПТ	Определяет содержимое поля "ПФ/ПТ" в записях журнала. Фильтру будут удовлетворять записи, содержащие указанное правило фильтрации или трансляции адресов
Виртуальные соединения	Отображаются записи, зарегистрированные при установлении виртуальных соединений

3. Нажмите кнопку "ОК".

В области отображения записей останутся записи, удовлетворяющие заданным условиям отбора.

Для автоматической настройки параметров фильтрации:

1. Выберите журнал НСД (см.стр. **24**).
2. Выберите запись о событии.

Примечание.
Событие должно быть зарегистрировано подсистемой "Пакетный фильтр".

3. В контекстном меню записи выберите пункт "Просмотр пакетов".

   Программа выполнит переход к журналу сетевого трафика текущего КШ. В области отображения записей отобразятся сведения об IP-пакетах, вызвавших регистрацию события НСД.

Отключение режима фильтрации журнала

При включенном режиме фильтрации записей выбранного журнала кнопка "Фильтр" ( ) отображается в "нажатом" состоянии. Чтобы вывести все записи, хранящиеся в журнале, необходимо отключить режим фильтрации для данного журнала.

Для отключения режима фильтрации записей:

- Нажмите кнопку "Очистить" ( ).

  Кнопка активна, если для данного журнала была выполнена фильтрация записей.

Фильтрация записей журнала будет отключена.

Поиск записей

Имеется возможность быстрого поиска всех вхождений указанного текста.

Для поиска записей:

1. Выберите журнал.
2. В поле "Поиск" на панели инструментов введите текст, который требуется найти.
3. Нажмите одну из следующих кнопок:
   - кнопку "Поиск" — для поиска очередного вхождения указанного текста;
   - кнопку "Поиск и выделение всех записей"— для поиска всех вхождений указанного текста.

Сохранение записей

Программа позволяет сохранять записи журналов в файлы формата XML. Операция сохранения может применяться для следующих журналов:

- системный журнал;
- журнал НСД;
- журнал сервера доступа;
- журнал сетевого трафика.

Для сохранения записей:

1. Вызовите на экран диалог "Экспорт журналов". Для этого выполните одно из следующих действий:
   - в иерархическом списке вызовите контекстное меню корневого элемента "Журналы" и активируйте команду "Экспорт журналов всех СУ";
   - в иерархическом списке вызовите контекстное меню нужного устройства или ЦУС и активируйте команду "Экспорт журналов";
   - вызовите контекстное меню в любом месте области отображения записей и активируйте команду "Экспорт журнала".
2. Заполните поля диалога и нажмите кнопку "ОК".

Тип журнала	Журналы, записи которых требуется сохранить
Учитывать время	Интервал времени регистрации событий для выборочного сохранения записей. Установите отметку и укажите дату и время границ интервала
Имя файла	Полное имя файла для сохранения записей. Для выбора файла в стандартном диалоге Windows используйте кнопку "..."

Записи выбранных журналов будут сохранены в указанный файл.

Очистка журналов

В соответствии с заданным расписанием выполняется автоматическая очистка журналов в базе данных (описание процедуры см. стр. **39**).

Программа позволяет выполнить внеочередную очистку содержимого журналов, хранящихся в базе данных. Перед выполнением очистки пользователю предоставляется возможность сохранить записи в файл.

Для очистки журналов всех СУ:

1. Выполните одно из следующих действий:
   - В иерархическом списке, в контекстном меню корневого элемента "Журналы" выберите пункт "Очистка всех журналов".
   - В контекстном меню выбранного устройства или ЦУС выберите пункт "Очистка журналов".

   На экране появится запрос на сохранение записей.
2. Нажмите одну из следующих кнопок:

Да	Вызывает на экран диалог "Экспорт журналов" для настройки параметров сохранения записей (см. стр. **27**)
Нет	Удаляет записи без сохранения
Отмена	Очистка журналов не выполняется

Сведения о выполнении очистки регистрируются в журнале приложения.

Статистика атак

В программе просмотра журналов предусмотрено формирование настраиваемых графических отчетов об атаках, зарегистрированных системой обнаружения вторжений.

Отчеты формируются для каждого детектора атак или для всех ДА комплекса на основании сведений, содержащихся в журналах НСД.

Настраиваемый состав отчета включает в себя следующие компоненты:

- статистика по IP-адресам объектов атаки;
- статистика по портам объектов атаки;
- статистика по IP-адресам источников атаки;
- распределение количества атак по классам;
- интенсивность атак;
- распределение общего количества атак по детекторам (только в отчете для всех ДА комплекса).

Отчет составляется за определенный период времени, который может принимать следующие значения:

- час;
- день;
- неделя;
- месяц;
- настраиваемый временной интервал.

При настройке отчета указывается количество самых активных объектов, отображаемых в диаграммах.

Предусмотрено автоматическое обновление сформированного отчета с указанием периода обновления.

Сформированный отчет может быть экспортирован в буфер обмена или в файл формата bmp или png.

Для формирования отчета детектора атак:

1. Раскройте в иерархическом списке объектов узел "Детекторы атак" и выберите объект "Статистика атак" требуемого ДА.

   В области отображения записей появится форма для настройки отчета.

   Примечание.
   Если отчет для данного ДА уже был сформирован ранее, он появится в области отображения записей.

2. Выполните настройку отчета.

Компоненты отчета	Установите отметку нужного компонента, чтобы включить его в отчет. Для исключения компонента из отчета удалите отметку
Параметры для сбора статистики	Укажите временной интервал отчета. Для этого выберите фиксированное значение из списка или укажите пределы "От" и "До" вручную, используя специальную форму. Введите количество самых активных объектов, отображаемых в отчете
Автообновление	Если необходимо, чтобы отчет обновлялся, установите отметку и задайте периодичность обновления (в минутах)

3. После настройки отчета нажмите кнопку "Построить отчет".

   В области отображения записей появится сформированный отчет.

4. Для копирования отчета в буфер обмена или сохранения в файл нажмите кнопку "Экспорт".

   На экране появится меню выбора варианта сохранения отчета.

5. Выберите нужный вариант и сохраните отчет.
   - Если было выбрано "в файл", на экране появится стандартный диалог сохранения файла.

     Сохраните отчет в формате bmp или png.
   - Если было выбрано "в буфер", далее отчет может быть вставлен в какой-либо графический редактор или документ MS Word.

Для формирования отчета для всех ДА комплекса:

1. Выберите в иерархическом списке объектов узел "Детекторы атак".

   В области отображения записей появится список детекторов атак и объект "Статистика атак".

2. Активируйте объект "Статистика атак".

   В области отображения записей появится форма для настройки отчета.

3. Настройте и сформируйте отчет в соответствии с описанием процедуры формирования отчета для отдельного ДА (см. выше).

   Внимание!
   Отчет отличается дополнительной настройкой, позволяющей отображать распределение атак по детекторам.

Отображение времени регистрации событий в часовом поясе сетевого устройства

По умолчанию таблицы с записями журналов (кроме таблицы журнала приложения) содержат колонку "Дата/Время на СУ". Колонка предназначена для вывода даты и времени регистрации событий в часовом поясе устройства. При необходимости можно скрыть отображение колонки.

Для включения или отключения отображения колонки:

- В меню "Вид" активируйте команду "Показывать время на СУ" (установленная отметка рядом с командой означает, что колонка "Дата/Время на СУ" отображается).

Включение и отключение отображения элементов интерфейса

Отображение элементов интерфейса в основном окне программы настраивается стандартными способами, принятыми в большинстве приложений Windows.

При необходимости можно отключить отображение панели инструментов, строки сообщений или дополнительного окна структуры журналов.

Для включения или отключения строки сообщений:

- На вкладке "Вид" нажмите кнопку "Строка состояния".

Для включения или отключения окна структуры журналов:

- На вкладке "Вид" нажмите кнопку "Область папок".

Примечание.
Кроме перечисленных способов отключить отображение дополнительного окна можно стандартной кнопкой ✕, которая расположена в правом углу заголовка окна.

Обновление отображаемой информации

Для обновления отображаемой информации:

- В контекстном меню корневого элемента иерархического списка выберите пункт "Обновить" или нажмите клавишу <F5>.

Очистка иерархического списка от удаленных сетевых устройств

Удаленные СУ отображаются в иерархическом списке программы до тех пор, пока не будет выполнена процедура очистки удаленных устройств.

Для очистки иерархического списка:

1. В иерархическом списке объектов выберите корневой элемент "Журналы".
2. В контекстном меню элемента выберите пункт "Очистка несуществующих СУ".

   На экране появится окно запроса на продолжение операции.
3. Нажмите кнопку "Да".

   Сведения об удаленных СУ, включая записи журналов этих сетевых устройств, будут удалены из базы данных.

Работа с программой просмотра отчетов

Отчеты ЦУС

Предусмотрена возможность получения отчетов, содержащих сведения о СУ комплекса. Список доступных отчетов зависит от роли администратора.

Табл.16 Отчеты ЦУС

Наименование отчета	Содержание	Доступ
Версии криптошлюзов	Список всех КШ комплекса и их версии	Все администраторы
Версии детекторов атак	Список всех ДА комплекса и их версии	Все администраторы
Версии криптокоммутаторов	Список всех КК комплекса и их версии	Все администраторы

Наименование отчета	Содержание	Доступ
Состояние криптошлюзов	Для каждого КШ отображаются: • Имя; • Описание; • Время смены ключей КШ; • Мягкий режим; • Введен в эксплуатацию; • Сервер доступа; • Кластер; • Наличие НСД; • Расположение; • Multi-WAN	Все администраторы
Состояние детекторов атак	Для каждого ДА отображаются: • имя; • описание; • признак ввода в эксплуатацию; • режим работы; • наличие НСД; • время загрузки главного ключа; • время смены ключа связи с ЦУС	Все администраторы
Состояние криптокоммутаторов	Для каждого КК отображаются: • имя; • описание; • время смены ключей КК; • мягкий режим; • введен в эксплуатацию; • наличие НСД; • кластер; • расположение; • Multi-WAN	Все администраторы
Конфигурации криптошлюзов	Для каждого КШ указываются: • имя КШ; • версия КШ; • аппаратная конфигурация КШ (платформа, процессор, память, устройство хранения данных, список сетевых интерфейсов с MAC-адресами)	Кроме администратора ключей
Конфигурации детекторов атак	Для каждого ДА указываются: • имя ДА; • версия ДА; • аппаратная конфигурация ДА (платформа, процессор, память, устройство хранения данных, список сетевых интерфейсов с MAC-адресами)	Кроме администратора ключей
Конфигурации крип-токоммутаторов	Для каждого КК указываются: • имя КК; • версия КК; • аппаратная конфигурация КК (платформа, процессор, память, устройство хранения данных, список сетевых интерфейсов с MAC-адресами)	Кроме администратора ключей
Наличие связей между КШ	Список криптографических шлюзов, которые должны устанавливать защищенные соединения, и характеристики этих соединений	Все администраторы
Наличие связей между КК	Список КК, которые должны устанавливать защищенные соединения, и характеристики этих соединений	Все администраторы
Правила трансляции по КШ	Для каждого КШ/адреса интерфейса/направления правила указываются: • отправитель; • получатель; • IP-адрес; • маска подсети для подстановки; • используемый сетевой сервис для входящих правил	Кроме администратора ключей
Правила маршрутизации по КШ	Для каждого КШ указываются маршруты статической маршрутизации. Маршрут представляется в виде IP-адреса/маски назначения и IP-адреса следующего узла	Кроме администратора ключей

Наименование отчета	Содержание	Доступ
Правила маршрутизации по ДА	Для каждого ДА указываются маршруты статической маршрутизации. Маршрут представляется в виде IP–адреса/маски назначения и IP-адреса следующего узла	Кроме администратора ключей
Правила фильтрации по КШ	Для каждого КШ из общего списка правил фильтрации на ЦУС формируется свой список правил фильтрации, включающий в себя те правила, в которых участвуют сетевые объекты КШ в качестве отправителя или получателя. Объекты могут быть указаны явно или через группы. Сведения о каждом КШ оформляются в виде отдельного раздела отчета	Кроме администратора ключей
Правила фильтрации на ЦУС	Список правил фильтрации ЦУС с выделением отключенных правил. Правила приводятся в порядке обработки	Кроме администратора ключей
Даты смены ключей КШ парной связи	Список дат смены ключей КШ парной связи. Даты приводятся по возрастанию времени смены ключей	Все администраторы
Даты смены ключей КК парной связи	Список дат смены ключей КК парной связи. Даты приводятся по возрастанию времени смены ключей	Все администраторы

Запуск программы просмотра отчетов

Для запуска программы:

- В меню "Пуск"ОС Windows в группе "Код Безопасности" выберите пункт "Программа просмотра отчетов ЦУС".

  На экране появится главное окно программы (см. Рис.3).

Настройка параметров соединения с ЦУС

Для отправки запроса ЦУС на формирование и получение отчета необходимо указать параметры соединения:

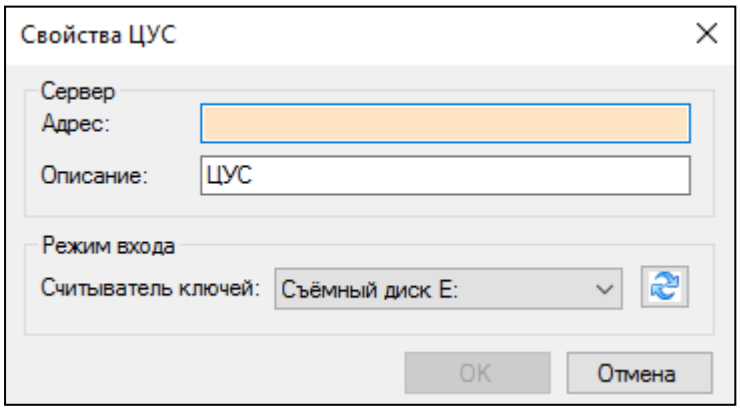
- IP-адрес ЦУС;
- тип ключевого носителя пользователя, используемого для связи с ЦУС.

Настройка выполняется в тех случаях, когда требуется добавить в список выбора новый ЦУС или изменить параметры уже имеющегося в списке соединения.

Для добавления в список нового ЦУС:

1. В раскрывающемся списке "ЦУС" выберите пункт "Новое соединение".

   Появится диалог настройки соединения.



2. Введите IP-адрес ЦУС, краткое описание (название соединения, отображаемое в списке выбора) и выберите тип ключевого носителя.

   Примечание.
   Кнопка "Обновить" обновляет список в поле "Тип ключевого носителя".

3. Нажмите кнопку "OK".

   В списке выбора появится название нового соединения.

Для изменения параметров соединения:

1. Выберите соединение на панели инструментов в раскрывающемся списке ЦУС.
2. Нажмите кнопку "Изменить", расположенную справа от раскрывающегося списка.
   Появится окно настройки соединения.
3. Введите изменения и нажмите кнопку "ОК".

Для удаления соединения из списка:

1. Выберите соединение на панели инструментов в раскрывающемся списке ЦУС.
2. Нажмите кнопку "Удалить", расположенную справа от раскрывающегося списка.

Формирование отчета

Для получения отчета:

1. Предъявите ключевой носитель.
2. Выберите вид отчета.
3. Выберите ЦУС.
4. Нажмите кнопку "Выполнить отчет".
   На экране появится запрос на ввод пароля администратора.
5. Введите пароль и нажмите кнопку "ОК".
   ППО направит запрос в ЦУС и из полученных данных сформирует отчет. Отчет отображается в окне программы в формате Crystal Reports.

Для просмотра отчета используйте кнопки, расположенные на средней панели.

Сохранение отчета

В программе предусмотрены печать отчета и сохранение его в одном из следующих форматов:

- Crystal Reports;
- PDF;
- CSV;
- Microsoft Excel;
- Microsoft Excel Data Only;
- Microsoft Word;
- Rich Text Format;
- XML.

Для вывода отчета на печать и сохранения используйте соответственно кнопки "Печать отчета" и "Экспорт отчета", расположенные на средней панели окна программы.

Примечание.
В программах построения отчетов параметры печати документа могут зависеть от свойств принтера, установленного по умолчанию. Для корректной печати необходимо настроить свойства принтера (например, установить требуемую ширину отступов).

Дополнительные настройки

Управление единым ключевым носителем

Обновление единого ключевого носителя

Обновление выполняют в следующих случаях:

- ввод в эксплуатацию новых ЦУС и КШ с СД;
- переинициализация ЦУС и КШ с СД;
- изменение адреса КШ с СД.

Для обновления ЕКН:

1. Вызовите на экран окно программы создания ключевого носителя (см. стр. 21).

2. Подключите ЕКН к считывателю.
3. Удалите устаревшие ключи.

   Для удаления выбранных ключей используйте кнопку "Удалить".

   Для очистки всего списка — кнопку "Очистить".
4. Добавьте новые ключи.

   Для каждого объекта выполните следующие действия:
   - Подключите носитель с ключами к считывателю.
   - В поле "Ключевой носитель-источник" укажите нужный считыватель и нажмите кнопку "Прочесть ключи".
   - В появившемся диалоге "Ключи" укажите IP-адрес объекта, пароль для расшифровки ключей и нажмите кнопку "ОК".

   В поле "Ключи в хранилище" отобразится новая запись.

Просмотр содержимого единого ключевого носителя

Для просмотра содержимого ЕКН:

1. Вызовите на экран окно программы создания ключевого носителя (см. стр. **21**).
2. Вставьте носитель с ЕКН.
3. В поле "Ключевой носитель хранилища" выберите ключевой носитель и нажмите кнопку "Загрузить ключи".

   В поле "Ключи в хранилище" отобразится содержимое ЕКН в виде списка ключей и IP-адресов ЦУС и СД.

Управление агентом с помощью программы управления ЦУС

Настройка параметров соединения с агентом

Для настройки параметров соединения с агентом:

1. В меню "ЦУС" выберите пункт "Параметры соединения с агентом…".

   На экране появится одноименное окно.
2. Заполните поля окна:

IP-адрес	IP-адрес компьютера, на котором установлен агент. Если агент и программа управления установлены на одном и том же компьютере — IP-адрес данного компьютера или 127.0.0.1
Время ожидания соединения, сек.	Время ожидания соединения в секундах (от 10 до 1800 сек.)

3. Нажмите кнопку "ОК".

Программа управления устанавливает соединение с агентом автоматически каждый раз, когда это необходимо, поэтому никакие дополнительные действия после изменения параметров соединения не требуются.

Определение параметров работы агента выполняют в окне настройки.

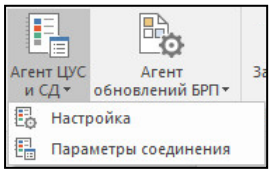
Примечание. Перед настройкой свойств агента из программы управления убедитесь, что служба "Агент ЦУС и СД" работает. При остановленной службе "Агент ЦУС и СД" настройка агента из программы управления невозможна.

Для вызова окна настройки агента:

1. Нажмите на панели инструментов кнопку "Агент ЦУС и СД" — 

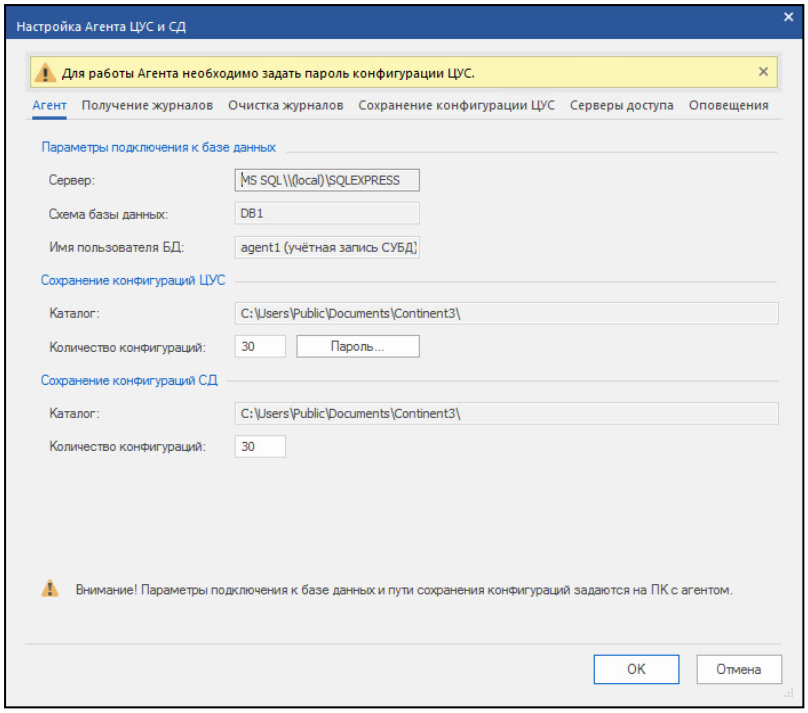
.

   На экране появится раскрывающийся список.



2. Выберите пункт "Настройка".

   На экране появится окно "Настройка Агента ЦУС и СД".



Предусмотрена возможность сохранения конфигураций ЦУС и СД в файл. Резервная копия позволяет быстро восстановить работу сети при выходе из строя штатного УБ. Агент сохраняет резервную копию конфигурации ЦУС и СД в соответствии с заданным расписанием в папку, которую можно указать средствами локального управления агентом (см. стр. **43**).

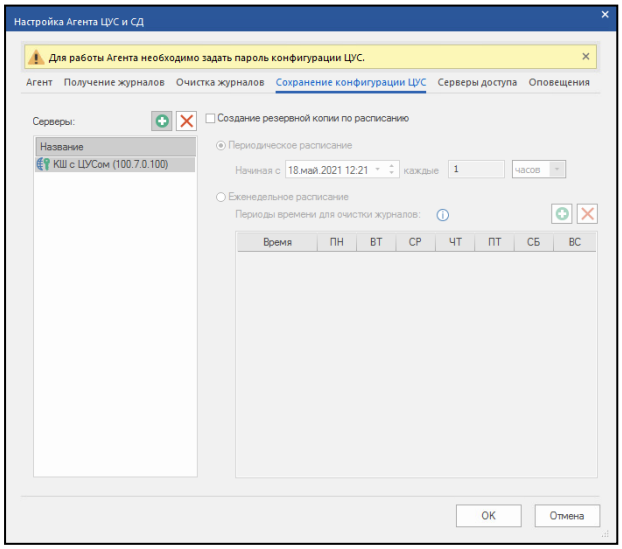
Внимание!

Если произошли изменения с уже назначенным ЕКН в Агенте ЦУС и СД, необходимо заново выполнить привязку ЕКН в настройках подключения агента (стр. **43**).

Для настройки расписания автоматического сохранения конфигурации ЦУС:

1. Вызовите на экран окно "Настройка Агента ЦУС и СД" (см. стр. **34**).
2. Выберите вкладку "Сохранение конфигурации ЦУС".
3. Нажмите кнопку  и в появившемся списке выберите ЦУС.

   На вкладке "Сохранение конфигурации ЦУС" отобразятся параметры расписания.



4. Установите отметку в поле "Создание резервной копии по расписанию".

   Параметры расписания станут доступными для редактирования.
5. Выберите тип расписания и определите его параметры:

Периодическое расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется через равные промежутки времени. Продолжительность промежутка задается количеством минут или часов. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент начала действия режима, активируйте ссылку с текущим значением даты и времени и в появившемся на экране диалоге введите нужные значения. Способы выбора и редактирования значений в этом диалоге аналогичны стандартным способам, принятым в ОС Windows для установки даты и времени
Еженедельное расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется в моменты времени, заданные специальным расписанием. Расписание представлено в виде таблицы, разделенной, для оптимального отображения, на две части. В столбцах таблицы перечислены дни недели, а в строках — часы и минуты с шагом 30 минут. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы. Для установки отметки поместите указатель в ячейку и нажмите левую кнопку мыши. Повторное нажатие кнопки приводит к удалению отметки. Действие расписания повторяется еженедельно

6. Нажмите кнопку "ОК".

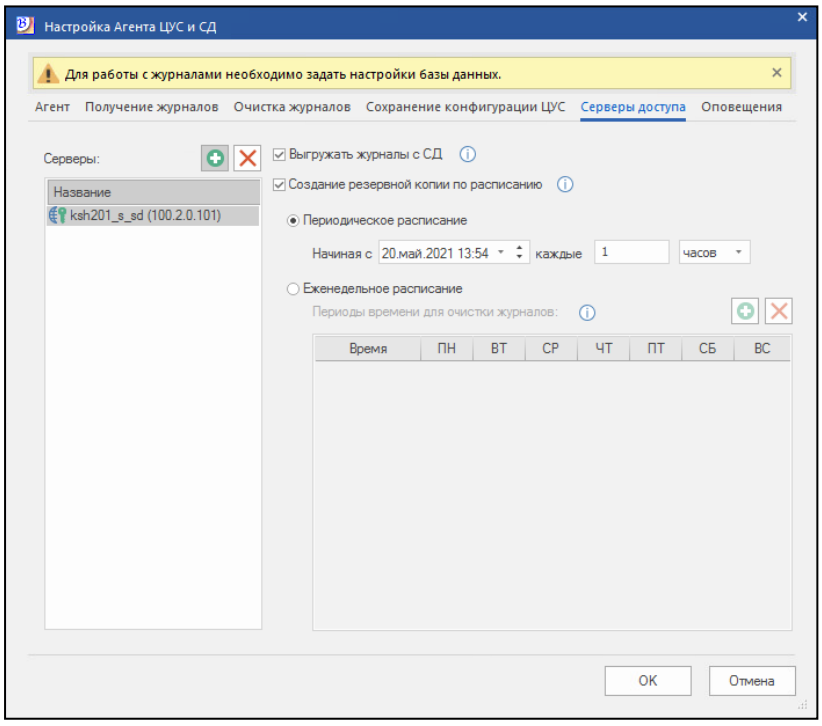
Агент будет автоматически создавать резервную копию конфигурации ЦУС в соответствии с заданным расписанием.

Для настройки расписания автоматического сохранения конфигурации СД:

1. Вызовите на экран окно "Настройка Агента ЦУС и СД" (см. стр. **34**).
2. Выберите вкладку "Серверы доступа".
3. Нажмите кнопку и в появившемся списке выберите СД.

   На вкладке "Серверы доступа" отобразятся параметры расписания.
4. Установите отметку в поле "Создание резервной копии по расписанию".

   Параметры расписания станут доступными для редактирования.



5. Выберите тип расписания и определите его параметры:

Периодическое расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется через равные промежутки времени. Продолжительность промежутка задается количеством минут или часов. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент начала действия режима, активируйте ссылку с текущим значением даты и времени и в появившемся на экране диалоге введите нужные значения. Способы выбора и редактирования значений в этом диалоге аналогичны стандартным способам, принятым в ОС Windows для установки даты и времени

Еженедельное расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется в моменты времени, заданные специальным расписанием. Расписание представлено в виде таблицы, разделенной, для оптимального отображения, на две части. В столбцах таблицы перечислены дни недели, а в строках — часы и минуты с шагом 30 минут. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы. Для установки отметки поместите указатель в ячейку и нажмите левую кнопку мыши. Повторное нажатие кнопки приводит к удалению отметки. Действие расписания повторяется еженедельно

6. Нажмите кнопку "ОК".
7. Агент будет автоматически создавать резервную копию конфигурации СД в соответствии с заданным расписанием.

Количество сохраняемых резервных копий ЦУС и СД устанавливается в разделе "Настройка Агента ЦУС и СД".

Чтобы установить количество сохраняемых конфигураций:

1. Вызовите на экран окно "Настройка Агента ЦУС и СД" (см. стр. **34**).
2. Выберите вкладку "Агент".
3. В группе параметров "Сохранение конфигурации ЦУС" установите значения для следующих параметров:

Количество конфигураций	Максимальное количество хранимых резервных копий ЦУС
Пароль	Назначение пароля для зашифрования резервной копии конфигурации ЦУС. Пароль не должен быть простым и его длина должна составлять не менее 8 символов. Этот пароль потребуется для загрузки сохраненных БД **Внимание!** Пароль должен содержать буквы верхнего и нижнего регистра, специальные символы: !"#$%&')(*+,\-./:;<=>?@[]!_`{|}~.Не допускается использование более двух одинаковых символов.

4. В группе параметров "Сохранение конфигурации СД", в поле "Количество конфигураций" установите максимальное количество хранимых резервных копий СД.
5. Нажмите кнопку "ОК".

Управление журналами с помощью агента

Для настройки параметров соединения агента и ЦУС:

1. Активируйте в меню "ЦУС" команду "Параметры соединения с агентом…". На экране появится одноименное диалоговое окно.
2. Заполните поля данного окна и нажмите кнопку "ОК":

IP-адрес	IP-адрес компьютера, на котором установлен агент. Если агент и программа управления установлены на одном и том же компьютере — IP-адрес данного компьютера или 127.0.0.1
Время ожидания соединения, сек.	Время ожидания соединения в секундах (от 10 до 1800 сек.)

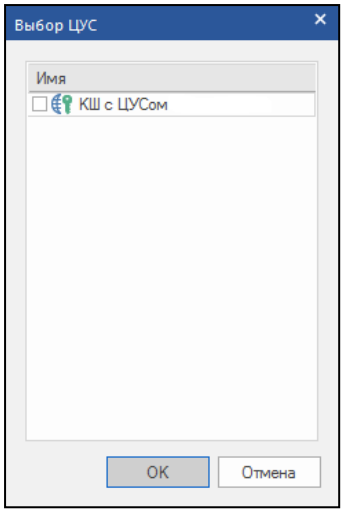
Примечание.
Программа управления устанавливает соединение с агентом автоматически каждый раз, когда это необходимо, поэтому никакие дополнительные действия после изменения параметров соединения не требуются.

Для передачи журналов необходимо указать, для каких КШ (ЦУС и СД) выполняется передача журналов.

Чтобы добавить ЦУС для передачи журналов:

1. Вызовите на экран окно "Настройка Агента ЦУС и СД" (см. стр. **34**).
2. Выберите вкладку "Сохранение конфигурации ЦУС".
3. Нажмите кнопку .

   Откроется окно выбора ЦУС.



4. Установите отметки в строках с выбранными ЦУС и нажмите кнопку "ОК".
   Выбранные ЦУС отобразятся в списке "Серверы".

Чтобы добавить СД для передачи журналов:

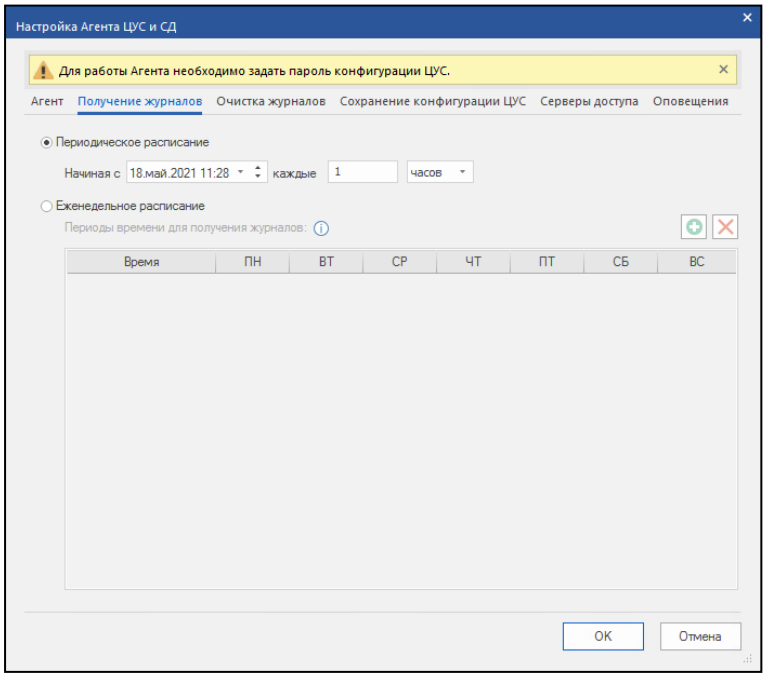
1. Вызовите на экран окно "Настройка Агента ЦУС и СД" (см. стр. **34**).
2. Выберите вкладку "Серверы доступа".
3. Нажмите кнопку .
   Откроется окно выбора СД.
4. Установите отметки в строках с выбранными СД и нажмите кнопку "ОК".
   Выбранные СД отобразятся в списке "Серверы".
5. В списке "Серверы" выберите СД и установите отметку в поле "Выгружать журналы с СД".
6. Повторите п. **5** для СД в списке, для которых необходимо включить передачу журналов.

Передача журналов из буфера ЦУС и буфера СД в базу данных осуществляется агентом одновременно по заданному расписанию.

Примечание.
По команде аудитора может осуществляться внеочередная передача журналов криптографических шлюзов (см. стр. **40**).

Для настройки расписания передачи журналов:

1. Вызовите на экран окно "Настройка Агента ЦУС и СД" (см. стр. **34**).
2. Выберите вкладку "Получение журналов".



3. Во вкладке "Получение журналов" выберите тип расписания и определите его параметры:

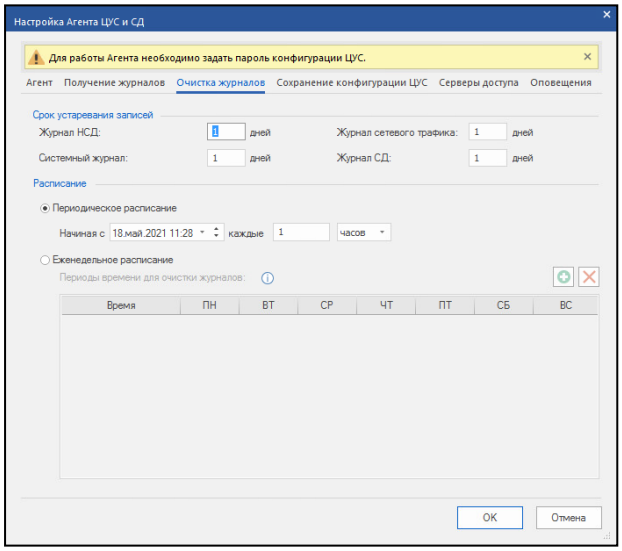
Периодическое расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется через равные промежутки времени. Продолжительность промежутка задается количеством минут или часов. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент начала действия режима, активируйте ссылку с текущим значением даты и времени и в появившемся на экране диалоге введите нужные значения. Способы выбора и редактирования значений в этом диалоге аналогичны стандартным способам, принятым в ОС Windows для установки даты и времени
Еженедельное расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется в моменты времени, заданные специальным расписанием. Расписание представлено в виде таблицы, разделенной, для оптимального отображения, на две части. В столбцах таблицы перечислены дни недели, а в строках — часы и минуты с шагом 30 минут. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы. Для установки отметки поместите указатель в ячейку и нажмите левую кнопку мыши. Повторное нажатие кнопки приводит к удалению отметки. Действие расписания повторяется еженедельно

4. Нажмите кнопку "ОК".

В базе данных записи журналов хранятся определенное время до установленного срока устаревания записей. Очистка журналов от устаревших записей осуществляется агентом по заданному расписанию.

Для настройки параметров очистки журналов:

1. Вызовите на экран окно "Настройка Агента ЦУС и СД" (см. стр. **34**).
2. Перейдите к вкладке "Очистка журналов".



3. В группе полей "Срок устаревания записей" для каждого журнала укажите срок хранения записей. При автоматической очистке журналов записи, которые хранятся в базе данных менее указанного срока, удалены не будут.
4. Выберите тип расписания и определите его параметры:

Периодическое расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется через равные промежутки времени. Продолжительность промежутка задается количеством минут или часов. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент начала действия режима, активируйте ссылку с текущим значением даты и времени и в появившемся на экране диалоге введите нужные значения. Способы выбора и редактирования значений в этом диалоге аналогичны стандартным способам, принятым в ОС Windows для установки даты и времени
Еженедельное расписание	Включает режим передачи журналов, при котором запуск процесса осуществляется в моменты времени, заданные специальным расписанием. Расписание представлено в виде таблицы, разделенной, для оптимального отображения, на две части. В столбцах таблицы перечислены дни недели, а в строках — часы и минуты с шагом 30 минут. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы. Для установки отметки поместите указатель в ячейку и нажмите левую кнопку мыши. Повторное нажатие кнопки приводит к удалению отметки. Действие расписания повторяется еженедельно

5. Нажмите кнопку "ОК".

Автоматическая передача регистрационных журналов в базу данных осуществляется агентом в соответствии с заданным расписанием (описание процедуры настройки расписания см. стр. **37**). При необходимости аудитор может выполнить внеочередной запуск процесса передачи журналов. Запуск осуществляется в программе управления ЦУС.

Для запуска передачи журналов:

- Активируйте кнопку управления и выберите "Сбор журналов".

  На экране появится сообщение об отправке команды на исполнение. После передачи журналов в базу данных записи могут быть загружены в программу просмотра журналов.

Настройка рассылки уведомлений по электронной почте

В комплексе предусмотрена возможность рассылки уведомлений о событиях по заданным адресам электронной почты.

Агент автоматически рассылает уведомления по указанным адресам электронной почты о заданных событиях из следующего списка:

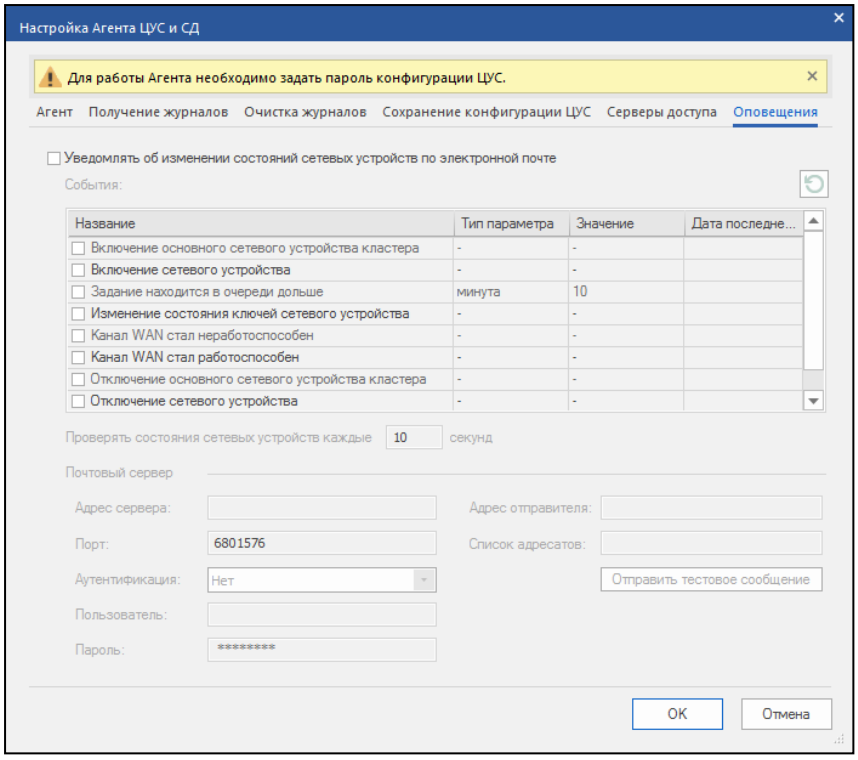
- включение сетевого устройства;
- выключение сетевого устройства;
- канал WAN стал неработоспособен;
- канал WAN стал работоспособен;
- появление НСД;
- отключение основного сетевого устройства кластера;
- включение основного сетевого устройства кластера;
- изменение состояния ключей сетевого устройства;
- задание находится в очереди дольше.

Примечание.
На почтовом сервере, через который будут рассылаться уведомления, должен быть включен один из следующих типов аутентификации:
- Anonymous access;
- Basic authentication.

Для настройки рассылки:

1. Нажмите на панели инструментов кнопку "Агент ЦУС и СД" и в раскрывающемся списке выберите пункт "Настройка".

  На экране появится окно параметров агента.



2. Выберите вкладку "Оповещения".
3. Установите отметку в поле "Уведомлять об изменении состояний сетевых устройств по электронной почте".

   Параметры рассылки уведомлений станут доступны для редактирования.
4. Укажите значения параметров:

События	Список событий, требующих уведомлений. Для выбора события установите отметку в соответствующей строке
Проверять состояние сетевых устройств	Укажите период проверки состояния сетевых устройств в секундах
Почтовый сервер	Сетевое имя или IP-адрес почтового сервера, через который будут рассылаться уведомления. Укажите имя почтового сервера и, при необходимости, имя и пароль для аутентификации агента на этом сервере
Список адресатов	Список адресов электронной почты получателей уведомлений (через ";")
Адрес отправителя	Произвольный адрес электронной почты для отображения в поле "Отправитель" сообщения с уведомлением

5. Нажмите кнопку "OK".

Примечание.
Для проверки правильности настроек используйте кнопку "Отправить тестовое сообщение". Тестовое сообщение будет отправлено по указанным адресам.

Локальное управление агентом

Агент автоматически сохраняет зашифрованные резервные копии конфигураций ЦУС и СД в соответствии с заданным расписанием. Имя файла резервной копии Save_at_yy_mm_dd_yy-hh_mm.dat. В папках одновременно хранится указанное количество резервных копий. При сохранении очередной копии сверх указанного количества самая старая копия удаляется.

Примечание.
По умолчанию это папка %PUBLIC%\Documents\Continent3\<имя_базы_данных>. Имейте в виду, что в MS Windows имя папки Documents может отображаться как Shared documents.

Для выбора папок архива:

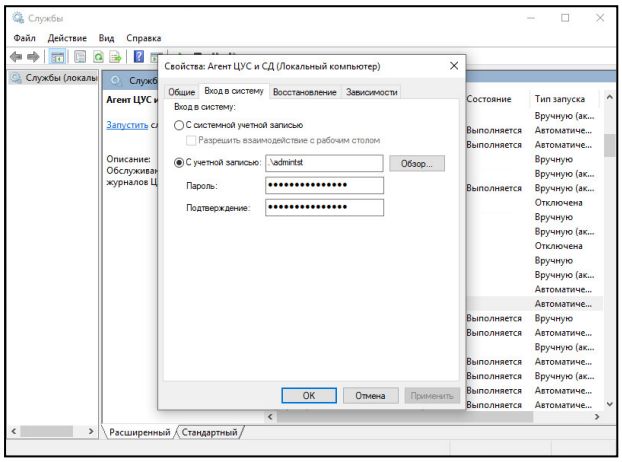
1. В группе полей "Сохранение конфигураций ЦУС" и "Сохранение конфигураций СД", в поле "Каталог" выберите папки с помощью стандартного диалога кнопки "Обзор".
2. Нажмите кнопку "ОК".

Настройка агента

Для корректной работы агента необходимо разрешить администратору доступ к службе агента.

Для предоставления администратору доступа к программе:

1. В консоли "Службы" ОС Windows предоставьте администратору доступ к программе.



2. Для сохранения изменений нажмите кнопку "ОК".
3. Для применения новых настроек остановите агент и заново вручную запустите его (см. стр. **21**).

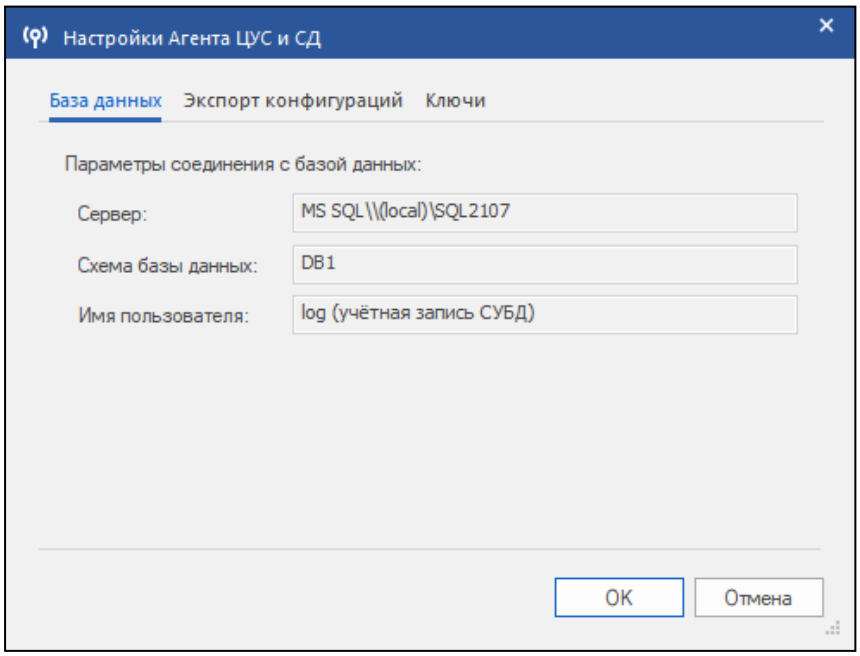
Настройка агента предусматривает:

- просмотр параметров соединения с базой данных для хранения журналов;
- выбор папок архива конфигураций ЦУС и СД;
- выбор ЕКН.

Определение параметров работы агента выполняют в окне настройки.

Для вызова окна настройки агента:

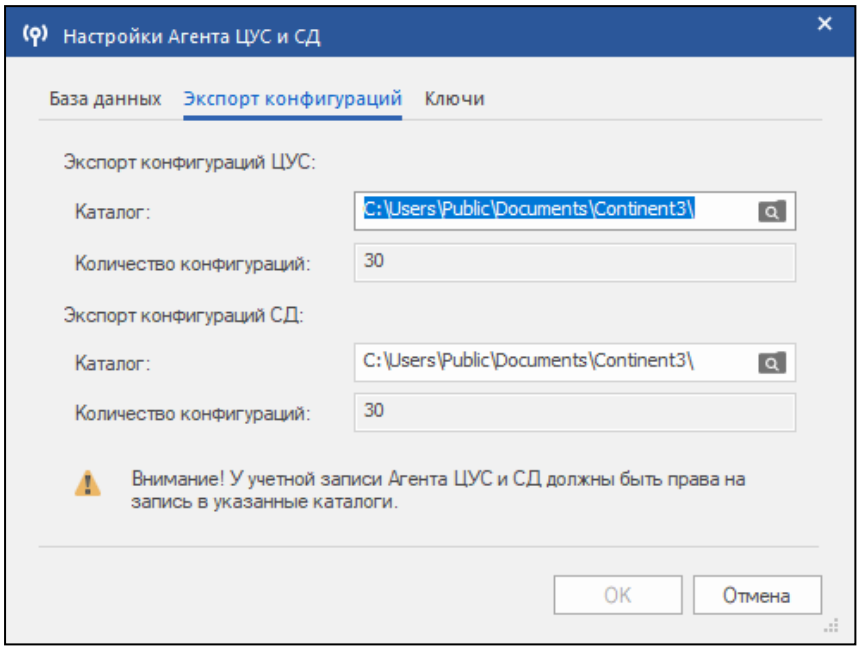
- В контекстном меню агента, расположенного в системной области панели задач, выберите пункт "Параметры агента...". На экране появится следующее окно:



На вкладке "База данных" отображаются параметры соединения с БД, настраиваемые в конфигураторе БД журналов ЦУС и СД. Описание процедуры приведено на стр. **19**.

Для выбора папок архива конфигураций ЦУС и СД:

1. В окне настроек агента выберите вкладку "Экспорт конфигураций".



2. В группе полей "Сохранение конфигураций ЦУС" и "Сохранение конфигураций СД", в поле "Каталог" выберите папки с помощью стандартного диалога кнопки "Обзор".

   Количество сохраняемых резервных копий ЦУС и СД устанавливается в разделе "Настройка Агента ЦУС и СД" ПУ ЦУС (см. стр. **37**).

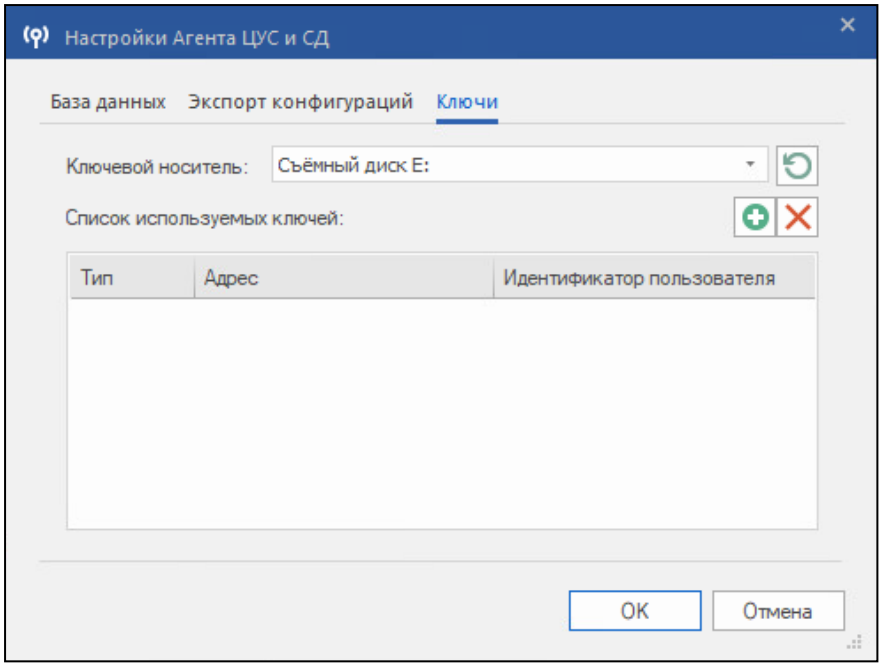
3. Нажмите кнопку "OK".

Агент автоматически сохраняет зашифрованные резервные копии конфигураций ЦУС и СД в соответствии с заданным расписанием. Имя файла резервной копии Save_at_yy_mm_dd_yy-hh_mm.dat. В папках одновременно хранится указанное количество резервных копий. При сохранении очередной копии сверх указанного количества самая старая копия удаляется.

Примечание. По умолчанию это папка %PUBLIC%\Documents\Continent3\<имя_базы_данных>. Имейте в виду, что в MS Windows имя папки Documents может отображаться как Shared documents.

Для выбора типа ЕКН:

1. В окне настроек агента выберите вкладку "Ключи".



2. В раскрывающемся списке "Ключевой носитель" выберите нужное значение и нажмите кнопку "OK".
3. Нажмите кнопку , чтобы добавить ключи ЦУС и СД в список.

   Откроется окно со списком доступных для добавления ключей.
4. Выберите ключ и нажмите кнопку "Добавить".
5. Нажмите кнопку "OK" в основном окне настроек агента, чтобы завершить настройку.

Остановка агента

Остановку агента можно осуществить:

- из программы управления агентом;
- из консоли "Службы".

Для остановки агента из программы управления агентом:

- Вызовите контекстное меню пиктограммы "Программа управления агентом" и активируйте команду "Остановить агент".

  Агент будет остановлен.

Для остановки агента из консоли "Службы":

1. В меню "Пуск" ОС Windows вызовите "Панель управления" и выберите "Администрирование | Службы".
2. Остановите службу "Агент ЦУС и СД". Для остановки службы выберите в списке нужное название, вызовите контекстное меню и выберите команду "Остановить".

   Агент будет остановлен, а его пиктограмма изменит вид.
3. Закройте окно "Службы".

Настройка параметров хранения и передачи журналов

Просмотр журналов удаленных сетевых устройств

После удаления сетевого устройства записи его журналов продолжают храниться в базе данных, пока не будут удалены агентом как устаревшие. По умолчанию в программе просмотра журналов представлены все сетевые устройства, журналы которых можно загрузить в программу. При необходимости можно отключить отображение удаленных устройств.

Для включения или отключения отображения удаленных сетевых устройств:

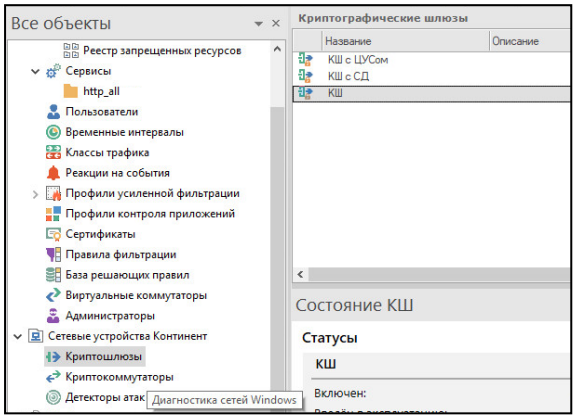
- В меню "Вид" активируйте команду "Скрывать удаленные СУ" (установленная отметка рядом с командой означает, что журналы удаленных сетевых устройств не отображаются в данный момент).

Параметры локальных журналов

При настройке параметров локальных журналов сетевых устройств определяется максимальный размер журналов и осуществляется выбор регистрируемых IP-пакетов.

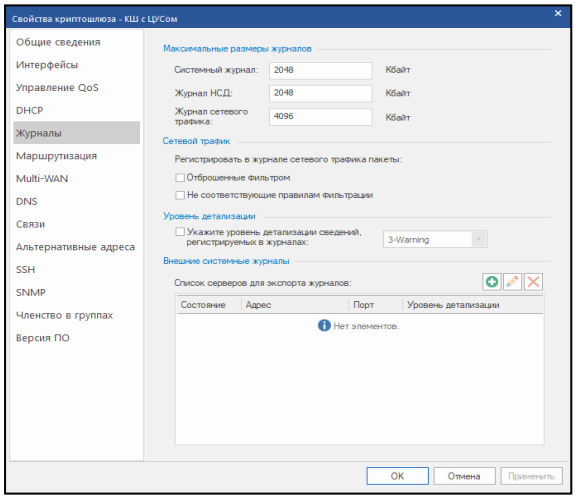
Для настройки параметров хранения журналов:

1. В программе управления ЦУС вызовите контекстное меню сетевого устройства и выберите пункт "Свойства".



   На экране появится диалоговое окно "Свойства".

2. Перейдите в раздел "Журналы".



3. В группе полей "Максимальные размеры журналов" укажите для каждого журнала размер пространства на жестком диске сетевого устройства, которое отводится для хранения записей. Размер пространства указывается в килобайтах.

   Примечание.
   Суммарный размер пространства, отводящегося для хранения журналов, не может превышать 32 МБ. Это конструктивное ограничение введено для поддержки высокого быстродействия системы.
   Если при добавлении новых записей размер журнала превысит указанное значение, произойдет переполнение журнала. В этом случае новые записи заместят записи, помещенные в журнал ранее других (самые старые записи). Сведения об этом будут добавлены в системный журнал сетевого устройства. Журналы хранятся на сетевом устройстве непродолжительное время, а затем передаются на ЦУС. Поэтому переполнение журналов на сетевом устройстве обычно происходит при отсутствии связи сетевого устройства с ЦУС.

4. В группе полей "Регистрировать в журнале сетевого трафика пакеты" укажите IP-пакеты, сведения о которых следует сохранять в журналах регистрации. Для этого отметьте соответствующие поля выключателей этой группы.

5. В группе параметров "Уровень детализации" установите отметку в поле "Укажите уворень детализации сведений, регистрируемых в журналах", затем в раскрывающемся списке выберите уровень событий.

   Будут регистрироваться события с уровнем равным или выше указанного.

6. Нажмите кнопку "ОК" или "Применить".

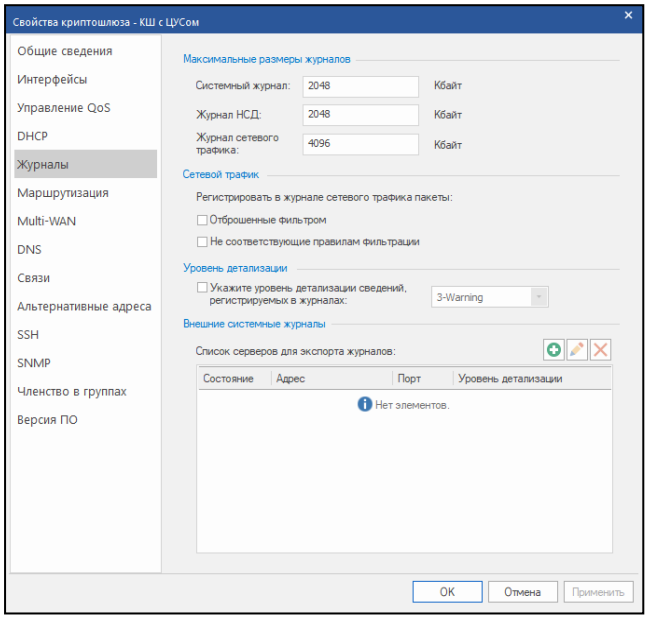
Настройка параметров хранения внешних системных журналов

В комплексе предусмотрена возможность хранения журналов во внешних хранилищах.

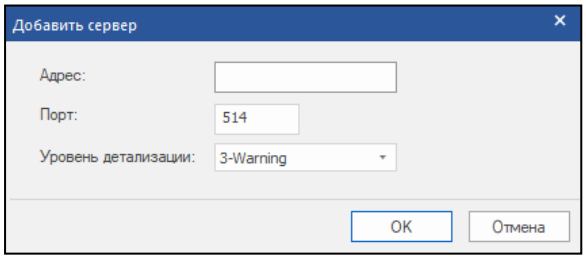
Внимание!
В syslog передается полный список событий, связанных с функционированием механизма усиленной фильтрации, в том числе информация о всех принятых и отброшенных сессиях.

Для настройки параметров внешнего хранения журналов:

1. В контекстном меню КШ выберите пункт "Свойства".
2. В окне свойств КШ выберите пункт "Журналы".



3. В группе параметров "Внешние системные журналы" нажмите кнопку .
   На экране появится окно свойств сервера.



4. Установите значения следующих параметров:
   - Адрес — IP-адрес syslog-сервера;

   Внимание!
   Для выгрузки событий на syslog-сервер в защищаемой сети по VPN необходимо добавить маршрут к syslog-серверу через внутренний интерфейс КШ.

   - Порт — номер порта, по которому происходит подключение к syslog-серверу;
   - Уровень детализации — в раскрывающемся списке выберите уровень детализации сведений, регистрируемых в журналах.

Сбор данных для SIEM-систем

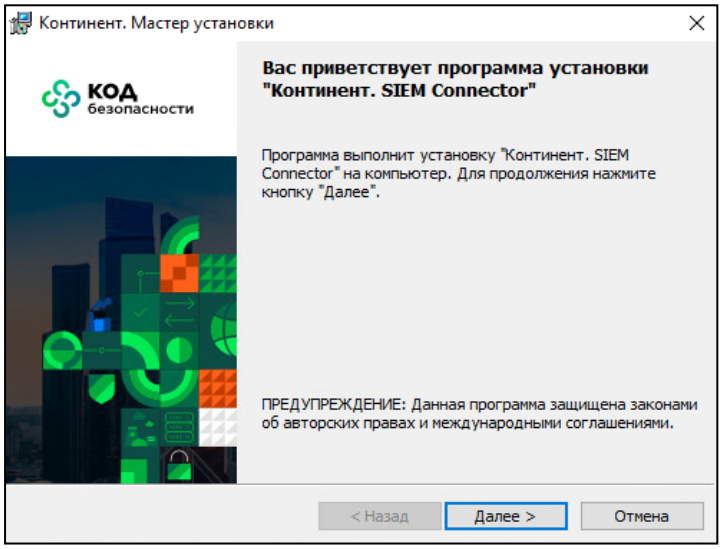
Сбор данных для SIEM-систем в среде АПКШ "Континент" осуществляется с помощью программы SIEM Connector. SIEM Connector собирает журналы из ПУ ЦУС и формирует из них файл с расширением .xml, который хранится на жестком диске компьютера.

Установка программы SIEM Connector

Для установки программы:

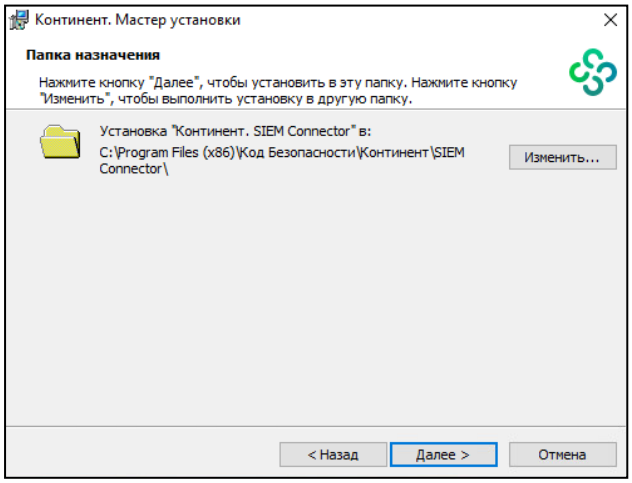
1. Войдите в систему с правами администратора компьютера.
2. Поместите установочный диск в устройство чтения компакт-дисков и запустите на исполнение файл setup.exe, находящийся в каталоге с дистрибутивом комплекса. При необходимости разрешите приложению вносить изменения на компьютере.
3. Перед процедурой установки программы выполните установку компонентов, необходимых для его корректной работы.

   На экране появится окно приветствия.



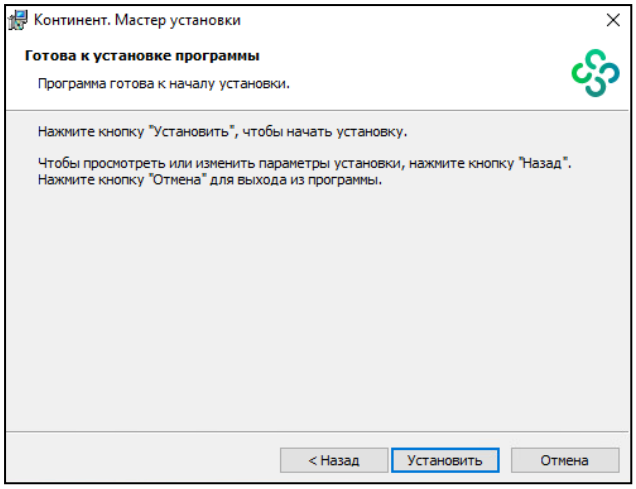
4. Нажмите кнопку "Далее >" для продолжения установки.

   Окно примет следующий вид:



5. Выберите папку назначения и нажмите кнопку "Далее >".

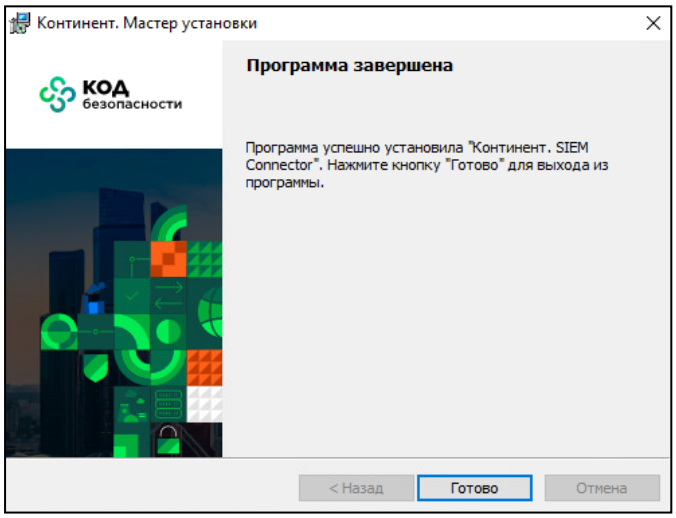
   На экране появится диалог "Установка".



6. Нажмите кнопку "Установить".

   Программа установки приступит к копированию файлов в указанную папку. Сообщения, появляющиеся на экране, отображают этапы процесса установки.

   По окончании процесса копирования на экране появится заключительное окно мастера установки.



7. Нажмите кнопку "Готово".

   На экране появится сообщение о необходимости перезагрузки компьютера.

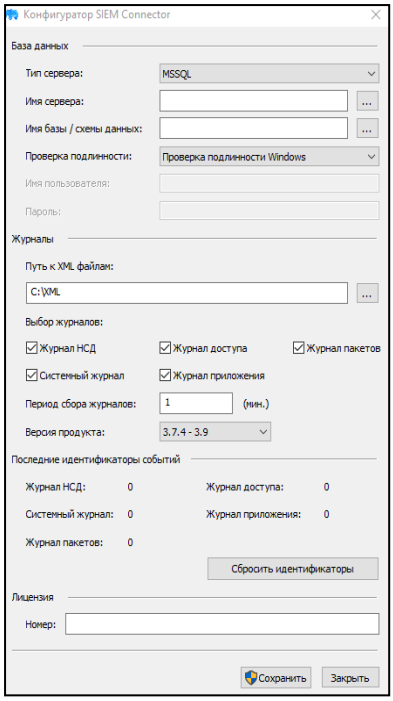
8. Подтвердите перезагрузку компьютера.

Настройка программы SIEM Connector

Для настройки программы:

1. В меню "Пуск" запустите от имени администратора программу SIEM Connector.

   На экране появится следующее окно:



2. В поле "Имя сервера" укажите сервер, на котором хранится база данных ППЖ.
3. В поле "Имя базы / схемы данных" укажите базу данных, в которой хранятся журналы ЦУС.
4. В поле "Путь к XML файлам" выберите адрес папки, в которой будут сохраняться файлы журналов в .xml формате.
5. В полях "Выбор журналов" проставьте отметку напротив журналов, копии которых требуется перевести в формат .xml.
6. В поле "Период сбора журналов" укажите период в минутах. Через указанные промежутки времени программа будет проверять журналы на наличие обновлений и сохранять файл только с новыми событиями.

   Примечание.
   Если необходимо сохранить файл со всеми событиями в БД, нажмите кнопку "Сбросить идентификаторы". При смене БД или схемы БД значения в группе параметров "Последние идентификаторы событий" будут обнулены автоматически.

7. В поле "Лицензия" введите номер, полученный от поставщика.
8. Нажмите кнопку "Сохранить".

   Программа SIEM Connector будет работать в фоновом режиме.

Приложение

Перечень регистрируемых событий

Табл.17 Перечень событий ЦУС и КШ

Название зарегистрированного события	Описание произошедшего события/причина	Действия пользователя
ID не зарегистрирован в ЭЗ. Событие ПАК "Соболь"	При входе в систему был предъявлен идентификатор, не принадлежащий ни одному из пользователей, зарегистрированных на данном КШ. При входе администратора был указан неверный пароль	Повторить вход в систему с правильным идентификатором и паролем
Конфликт IP-адресов (IP-адрес, MAC-адрес)	Сетевым объектам назначены одинаковые IP-адреса	Использовать в сети только уникальные IP-адреса
Неверная имитовставка от КШ. НСД от ЦУС	Неверный ключ связи с ЦУС	Убедиться, что на КШ загружены правильные ключи. При необходимости создать и загрузить новый ключ КШ
Неверная имитовставка от ПУ. НСД от ЦУС	Результат проверки целостности служебного пакета отрицательный. Пакет отброшен. Неверный ключ администратора или пароль	Убедиться, что используются правильные ключи и пароль. При необходимости создать новые ключи администратора
Неверная имитовставка. НСД от системы управления КШ	Результат проверки целостности служебного пакета отрицательный. Пакет отброшен. Неверный ключ связи с ЦУС	Убедиться, что на КШ загружены правильные ключи. При необходимости создать и загрузить новый ключ КШ
Неверная имитовставка. НСД от шифратора	Результат проверки целостности пакета отрицательный. Пакет отброшен. Возможные причины: • Пакет перехвачен и изменен нарушителем. • Неверные ключи парной связи	Руководствоваться положениями политики безопасности предприятия. Пересоздать парную связь между КШ
Неверный номер входящего пакета. НСД от системы управления КШ	Нарушен порядок следования служебных пакетов. Пакет отброшен. Возможные причины: • Пакет перехвачен и повторно переслан нарушителем. • Промежуточное оборудование переставляет местами зашифрованные пакеты. • Неверный идентификатор сессии	Руководствоваться положениями политики безопасности предприятия. Устранить возможные неполадки на промежуточном оборудовании. Перезагрузить КШ
Неверный номер входящего пакета. НСД от ЦУС	Нарушен порядок следования служебных пакетов. Пакет отброшен. Возможные причины: • пакет перехвачен и повторно переслан нарушителем; • промежуточное оборудование переставляет местами зашифрованные пакеты; • неверный идентификатор сессии	Руководствоваться положениями политики безопасности предприятия. Устранить возможные неполадки на промежуточном оборудовании. Перезагрузить КШ
Неправильный номер пакета. НСД от шифратора	Нарушен порядок следования пакетов. Пакет отброшен. Возможные причины: • пакет перехвачен и повторно переслан нарушителем; • промежуточное оборудование переставляет местами зашифрованные пакеты	Руководствоваться положениями политики безопасности предприятия. Устранить возможные неполадки на промежуточном оборудовании

Название зарегистрированного события	Описание произошедшего события/причина	Действия пользователя
Неправильный пароль. Событие ПАК "Соболь"	При входе в систему был указан неверный пароль. Ранее дважды была выполнена смена аутентификатора средствами других комплексов "Соболь" и при этом пользователь ни разу не выполнил вход в систему на данном компьютере	Повторить вход в систему с правильным идентификатором и паролем
Ошибка при контроле целостности. Событие ПАК "Соболь"	Обнаружено несовпадение эталонного значения контрольной суммы и ее текущего значения для одного из проверяемых объектов. На диске отсутствуют файлы шаблонов КЦ	Переустановить ПО АПКШ "Континент" на криптошлюз
Пользователь блокирован. Событие ПАК "Соболь"	Пользователь, вход которого в систему блокирован, осуществил попытку входа	Разблокировать пользователя, повторить попытку входа
Превышено число попыток входа. Событие ПАК "Соболь"	Количество неудачных попыток входа данного пользователя в систему превысило установленное ограничение	Войти в меню ПАК "Соболь". Разблокировать учетную запись пользователя. Сменить пароль пользователя
Назначение комплекта ключей для КШ	Для КШ назначен комплект ключей	Получить от администратора ключевой носитель с назначенным комплектом для последующей загрузки ключа на КШ
Удаление назначенного для КШ комплекта ключей	Из БД ЦУС удален назначенный для КШ комплект ключей	Загрузка ключей, входящих в состав удаленного комплекта, невозможна
Активация ключа на ЦУС	На ЦУС выполнена загрузка и активация ключа	Информационное сообщение
Переход на резервный ключ КШ	На КШ выполнен переход на резервный ключ	Информационное сообщение
Изменение схемы хранения ключевой информации	В ПУ ЦУС переключен режим управления ключами (с однолетней схемы хранения на трехлетнюю или наоборот)	В зависимости от установленного режима блокируется или активируется выполнение определенных операций с ключами
На КШ загружен неизвестный ключ	На КШ загружен ключ, не входящий в состав назначенных для данного КШ комплектов	Загрузить на КШ ключ из назначенного комплекта

Табл.18 Перечень событий сервера доступа

Название зарегистрированного события	Описание произошедшего события/причина	Действия пользователя
Создан ключевой носитель	На КШ с СД средствами локального управления создан ключевой носитель администратора	Информационное сообщение
Установлена временная зона	На КШ с СД задан часовой пояс	Информационное сообщение
Добавлена лицензия	На СД средствами локального управления добавлена лицензия на подключение АП	Информационное сообщение
Удалена лицензия	На СД средствами локального управления удалена лицензия на подключение АП	Информационное сообщение
Восстановлена БД	На СД средствами локального управления восстановлена база данных	Информационное сообщение
EAP: неправильный ID пакета (получен N вместо M) –отброшен bp [0]	Нарушена очередность получения пакетов. Возможные причины: • Медленный канал. • Сбои в работе сетевого оборудования. • Действия злоумышленника	Дополнительная информация для службы техподдержки. При неудачной попытке подключения повторить попытку

Название зарегистрированного события	Описание произошедшего события/причина	Действия пользователя
АП не подает признаков жизни	Клиент отключен по тайм-ауту	1) Убедиться в корректности настроек СД и данных клиента. 2) Произвести повторную попытку подключения к СД
В базе сервера доступа не установлены лицензии	Отсутствуют зарегистрированные лицензии в базе данных СД	Добавить серийный номер лицензии в подразделе "Лицензии" раздела "Настройки сервера"
Вход пользователя в неразрешенное время	Отказ в подключении АП. Попытка подключиться к серверу в запрещенное время	Повторить попытку подключения в разрешенный период времени. Изменить расписание работы пользователя
Вход пользователя заблокирован	Отказ в подключении АП. Учетная запись пользователя заблокирована	1) В свойствах пользователя выключить опцию "Отключена". 2) Повторить попытку подключения
Заблокирована нелицензионная учетная запись	Предупреждающее сообщение	Дополнительная информация для службы техподдержки
Завершилось время работы АП	Разрыв соединения по установленному расписанию (закончился период времени, в течение которого абоненту разрешено работать с СД)	Повторить попытку подключения в разрешенный период времени. Изменить расписание работы пользователя
Запрос АП отклонен: сервер заблокирован	Отказ в подключении АП. Сертификат клиента не прошел проверку	Убедиться, что сервер доступа не заблокирован. В противном случае разблокировать его командой ПУ СД и повторить попытку подключения
Защищенная сеть установлена в списке открытых сетей	Предупреждающее сообщение	Дополнительная информация для службы техподдержки
Испорченный архив БД	Ошибка при попытке восстановить БД СД из файла с архивом	Убедиться в правильности выбранного файла архива (*.asb)
Ключ ПУ СД не задан: чтение сохраненного в БД ключа	Предупреждающее сообщение	Дополнительная информация для службы техподдержки
Лицензия с введенным серийным номером уже существует	Введенный номер лицензии уже зарегистрирован в базе данных СД	Добавить корректный номер лицензии
Многократный вход пользователя запрещен	Отказ в подключении АП при попытке подключения под одной учетной записью более чем с одного компьютера. Включен режим запрета множественных подключений	Для разрешения множественных подключений нужно в свойствах данной учетной записи включить режим "разрешить множественные подключения"
Не найден CRL-файл (результат авторизации АП)	Список отозванных сертификатов по указанному в сертификате адресу отсутствует	Указать правильный путь к списку отозванных сертификатов для внешнего Центра сертификации. Создать правило фильтрации, обеспечивающее доступ СД к Центру сертификации
Не установлен пул динамических адресов	Ошибка при запуске СД. Не задан пул IP-адресов в настройках сервера	Заполнить поле "Пул адресов" (адрес/маска) в разделе "Настройки сервера"

Название зарегистрированного события	Описание произошедшего события/причина	Действия пользователя
Не установлены лицензии: окончился срок действия лицензии	Предупреждающее сообщение	Дополнительная информация для службы техподдержки
Неверная имитовставка	Ошибка ПУ СД. Возможные причины: • Неправильный ключ. • Неправильный пароль администратора ПУ	Убедиться, что используются верные ключи. При необходимости пересоздать новые ключи администратора ПУ СД
Неизвестный клиент	Отказ в подключении АП. В БД не найден сертификат пользователя, с которым была проведена попытка подключения к СД	Зарегистрировать сертификат пользователя в БД СД
Некорректный сертификат АП	Отказ в подключении АП. Сертификат не прошел проверку по одной из причин: сертификат отозван, сертификат просрочен, срок действия сертификата еще не наступил, не найден корневой сертификат, слишком длинная цепочка сертификатов, неправильное назначение сертификата	Зарегистрировать действительный сертификат пользователя в БД СД
Некорректный сертификат сервера	При получении цепочки сертификатов было выявлено, что сертификат СД некорректен	Создать новый сертификат СД
Нет свободных IP-адресов	Исчерпан лимит выданных IP-адресов из пула адресов	Расширить диапазон выдаваемых IP-адресов в настройках сервера доступа
Отключение заблокированных пользователей	Заблокированные пользователи были отключены	Дополнительная информация для службы техподдержки
Ошибка аутентификации АП	Ошибка аутентификации клиента	Дополнительная информация для службы техподдержки. Произвести повторную попытку подключения к СД
Ошибка получения диапазона адресов для сервера	Ошибка при запуске СД. Не задан пул IP-адресов в настройках сервера	Заполнить поле "Пул адресов" (адрес/маска) в разделе "Настройки сервера"
Ошибка получения номера порта для связи с АП	Ошибка может возникнуть при открытии БД	Изменить значение номера порта для связи с АП на корректный. Сохранить изменения в БД
Ошибка получения параметров сервера	Ошибка прочтения порта из базы данных СД	Переинициализировать СД
Ошибка при получении TZ (Time Zone – временная зона)	Предупреждающее сообщение. Эта ошибка может возникнуть при старте СД в случае наличия проблем с БД СД	Дополнительная информация для службы техподдержки
Ошибка сохранения ключа ПУ СД в архиве	Ошибка сохранения ключа ПУ СД в архиве	Дополнительная информация для службы техподдержки
Ошибка удаления связанного сертификата	Ошибка при удалении корневого сертификата. Ошибка возникает в процессе удаления объектов, связанных с корневым сертификатом	Дополнительная информация для службы техподдержки
Ошибка чтения списка корневых сертификатов	Предупреждающее сообщение	Дополнительная информация для службы техподдержки
Превышено максимальное количество запросов на подключение	Ошибка при попытке подключения клиента	Дополнительная информация для службы техподдержки
Превышено максимальное количество соединений	Ошибка аудита	Дополнительная информация для службы техподдержки

Название зарегистрированного события	Описание произошедшего события/причина	Действия пользователя
Соединение не инициализировано	Отказ в подключении АП	Дополнительная информация для службы техподдержки
Сохранение изменений невозможно, так как основной сервер доступа отключен или неактивен	Ошибка в работе кластера КШ. Была произведена попытка выполнить команду СД, когда основной КШ был недоступен или неактивен	Повторить команду СД после подключения основного КШ

Табл.19 Перечень событий КШ и КК

Название зарегистрированного события	Описание произошедшего события/причина	Действия пользователя
Парная связь заблокирована	Истек срок действия ключа VPN	Проверьте сроки действия сертификатов и межсетевых ключей. Обновите ключи парной связи

Табл.20 Перечень событий детектора атак

Событие
Обнаружена атака. Описание атаки
Изменение режима работы детектора атак
Изменение значения параметра детектора атак
Изменение правила детектора атак
Подключение правила к детектору атак
Загрузка обновлений БРП
Добавление правила детектора атак
Удаление правила детектора атак
Изменение параметров агента обновлений БРП
Изменение режима работы эвристик
Импорт сертификата обновлений БРП
Удаление сертификата обновлений БРП

Документация

1. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Ввод в эксплуатацию.
2. Аппаратно-программный комплекс шифрования "Континент". Версия 3.9. Руководство администратора. Управление комплексом.