КОД БЕЗОПАСНОСТИ

Аппаратно-программный комплекс шифрования

Континент
Версия 3.7

Руководство администратора

Аудит

RU.88338853.501430.006 96 3 1

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

Оглавление

Список сокращений

БД	База данных
БРП	База решающих правил
ДА	Детектор (компьютерных) атак
ЕКН	Единый ключевой носитель
КК	Криптокоммутатор
КШ	Криптографический шлюз
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
ППЖ	Программа просмотра журналов
ППО	Программа просмотра отчетов
ПУ	Программа управления
СД	Сервер доступа
ЦУС	Центр управления сетью криптографических шлюзов
ЭЗ	Программно-аппаратный комплекс "Соболь"

Введение

Данный документ предназначен для администраторов изделия "Аппаратно-программный комплекс шифрования «Континент». Версия 3.7" RU.88338853.501430.006 (далее — комплекс). В документе содержатся сведения, необходимые для настройки компонентов комплекса и работы с программой просмотра журналов. Кроме того, описывается работа, связанная с получением отчетов о состоянии комплекса.

Приступая к изучению данного руководства, необходимо предварительно ознакомиться с [**1**] и [**5**].

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-495-982-30-20 или по электронной почте support@securitycode.ru. Страница службы технической поддержки на сайте компании "Код Безопасности": http://www.securitycode.ru/products/technical-support/.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Задачи аудита

Под аудитом подразумевается контроль состояния защищенности и работоспособности комплекса. Оценка функционирования комплекса осуществляется посредством анализа произошедших событий, зарегистрированных в журналах КШ, ДА, КК, ЦУС и СД. 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).

Возможность просмотра содержимого журналов определяется правами учетных записей пользователей на доступ к базе данных, в которой хранятся журналы. Для выполнения других действий с журналами эти пользователи должны быть наделены правами на администрирование комплекса. Чтобы предоставить необходимые права, пользователю должна быть 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.

Подробные сведения об управлении учетными записями, а также о распределении прав для учетных записей содержатся в [**1**].

Журналы регистрации событий

События, происходящие при функционировании компонентов комплекса, регистрируются в журналах в виде отдельных записей. Записи о событиях содержат подробную информацию для анализа произошедших событий.

Перечень регистрационных журналов комплекса представлен в таблице ниже.

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 и 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 и криптографического шлюза, и детектора атак, и криптокоммутатора, и ЦУС.

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

Из базы данных записи журналов могут быть загружены для просмотра администратором (аудитором). Загрузка записей осуществляется в программе просмотра журналов комплекса.

Очистка журналов может выполняться в следующих режимах:

- автоматический;
- ручной.

Автоматическая очистка выполняется по расписанию, сформированному для агента ЦУС и СД средствами программы управления комплексом. Ручная очистка выполняется администратором из программы просмотра журналов.

Системный журнал

В системном журнале регистрируются события, связанные с работой подсистем КШ, ДА, КК и ЦУС, а также события, регистрируемые ПАК "Соболь". Для каждого зарегистрированного события сохраняются время регистрации, название события, категория и ряд дополнительных параметров.

Ниже представлены описания категорий регистрируемых событий и перечень полей системных журналов КШ, ДА, КК и ЦУС.

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
Журнал Соболя	КШ, ДА, КК	События, зарегистрированные ПАК "Соболь"
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 КШ , ДА , КК
Безопасность виртуального коммутатора	КК	События, связанные с работой криптокоммутатора в режиме безопасности

Табл.3 Перечень 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
Дата/Время на КШ	Дата и время регистрации события в часовом поясе криптошлюза, ДА, КК
Категория события	Наименование категории события
Событие	Наименование события
Описание	Детальное описание события

Журнал НСД

В журнале НСД хранятся записи о зарегистрированных событиях, свидетельствующих о возможных угрозах безопасности. Каждая запись содержит информацию о количестве зарегистрированных событий в течение одной минуты, а также ряде дополнительных параметров.

Ниже представлено описание подсистем — источников событий, а также перечень полей журнала НСД.

Табл.4 Подсистемы, регистрирующие события НСД

Подсистема		Журнал	Название события	Описание
	ЦУС	ЦУС	Неверная имитовставка от КШ, ДА, КК	IP-адрес или диапазон адресов источника
			Неверная имитовставка от ПУ	IP-адрес или диапазон адресов источника
			Неверный номер входящего пакета	IP-адрес или диапазон адресов источника
			Неудачная попытка соединения с ЦУС	Адрес источника; имя учетной записи, под которой было выполнено обращение к ЦУС
	Управление КШ, ДА, КК	КШ, ДА, КК	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
			Нет ключа для шифрования пакета	IP-адрес источника
			Нет ключа для расшифрования пакета	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	Нет	Диапазон адресов отброшенных пакетов
	Сигнатурный/эвристический анализатор	ДА	Сигнатурный/эвристический анализатор	Описание атаки
	Безопасность виртуального коммутатора	КК	Возникновение небезопасного MAC-адреса на интерфейсе	MAC-адрес, имя интерфейса
			Переполнение таблицы MAC-адресов	MAC-адрес последнего пакета за минуту

Табл.5 Перечень 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
Дата/Время на КШ, ДА, КК	Дата и время регистрации события в часовом поясе криптошлюза, или ДА, или КК
Название подсистемы	Название подсистемы, зарегистрировавшей событие
Количество событий	Количество зафиксированных событий НСД этого типа в течение 1 мин.
Описание	Детальное описание произошедшего события

Журнал сетевого трафика

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

Примечание. При интенсивном трафике журнал может периодически переполняться с последующей автоматической очисткой, и, как следствие, часть информации будет утеряна. Переполнение журналов может происходить как на КШ (криптокоммутаторе), так и на ЦУС. Используйте 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 (криптокоммутатора). См. [1].

Описание используемых пиктографических обозначений и перечень полей журнала сетевого трафика представлены в таблицах ниже.

Табл.6 Пиктографические обозначения

Пиктографическое обозначение	Описание
	Входящий IP-пакет
	Исходящий IP-пакет
	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 Перечень 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 КШ, КК	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, примененное к IP-пакету

Журнал приложения

В журнале приложения фиксируются события, связанные с работой агента ЦУС и СД . Сохраняются следующие сведения: о загрузке журналов, об очистке журналов, о командах на немедленную очистку журналов, поступающих из ППЖ. Туда же помещаются сообщения о возникающих при работе агента проблемах (потеря соединения с СУБД, потеря соединения с ЦУС и т. п.).

Ниже приведен перечень полей журнала приложения.

Табл.9 Перечень полей журнала приложения

Поле	Описание
Дата/Время	Дата и время регистрации события
Подсистема	Название компонента, выполнившего действие (агент или программа просмотра журналов)
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 таблице ниже представлен перечень полей журнала сервера доступа.

Табл.10 Перечень полей журнала сервера доступа

Поле	Описание
Дата/Время	Дата и время регистрации события

Поле	Описание
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

Настройка параметров хранения и передачи журналов

События, происходящие на криптографических шлюзах/детекторах атак/криптокоммутаторах, 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. Каждый криптографический шлюз/детектор атак/криптокоммутатор локально хранит записи журналов до момента их передачи центру управления сетью. При наличии связи с ЦУС отправка содержимого журналов осуществляется по мере регистрации событий. После передачи записи удаляются из локальных журналов КШ/ДА/КК. Если связь с ЦУС отсутствует, записи накапливаются в локальных журналах криптографических шлюзов/детекторов атак/криптокоммутаторов.

На ЦУС выделен специальный буфер для временного хранения принятых записей журналов. Аналогично локальным журналам КШ/ДА/КК 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 администратора (аудитора).

Для обеспечения сохранности записей журналов и их своевременного получения администратор может централизованно настраивать следующие параметры:

- параметры локальных журналов КШ/ДА/КК;
- параметры буфера журналов ЦУС;
- расписание передачи журналов в базу данных;
- параметры очистки базы данных от устаревших записей журналов.

Настройку параметров хранения и передачи журналов выполняют в программе управления ЦУС. Подробные сведения о работе с программой см. [**1**].

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.

Параметры локальных журналов

При настройке параметров локальных журналов КШ/ДА/КК определяется максимальный размер журналов и осуществляется выбор регистрируемых IP-пакетов.

Для настройки параметров хранения журналов:

1. В программе управления ЦУС вызовите контекстное меню нужного устройства (КШ/ДА/КК) и активируйте команду "Свойства".

   На экране появится диалоговое окно "Свойства...".

2. Перейдите к вкладке "Журналы".

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

   Суммарный размер пространства, отводящегося для хранения журналов, не может превышать 32 Мб. Это конструктивное ограничение введено для поддержки высокого быстродействия системы.

Примечание. 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 КШ/ДА/КК.

Необходимо учитывать, что журналы хранятся на КШ/ДА/КК непродолжительное время, а затем передаются на ЦУС. Поэтому переполнение журналов на КШ/ДА/КК обычно происходит при отсутствии связи КШ/ДА/КК 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.

Примечание. Переданные получателям IP-пакеты регистрируются в журнале сетевого трафика. Сведения о IP-пакетах, отброшенных фильтром или не соответствующих ни одному правилу, — в журнале НСД и в журнале сетевого трафика.

Если включить регистрацию пропущенных пакетов (поле "Переданные получателям"), то журнал при интенсивном трафике будет периодически переполняться с последующей частичной потерей данных. Чтобы этого не произошло, рекомендуется осуществлять выборочную регистрацию пропущенных пакетов с помощью правил фильтрации.

5. Нажмите кнопку "OK" или "Применить".

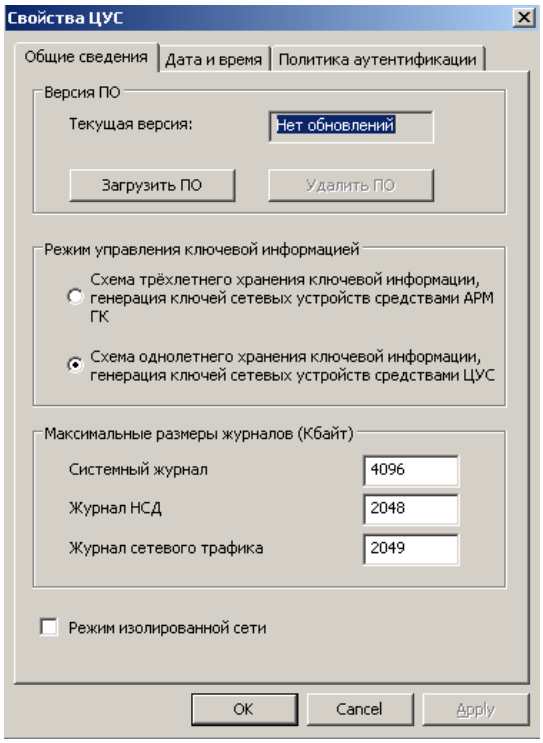
Параметры буфера журналов ЦУС

При настройке параметров буфера журналов, принятых от КШ /ДА /КК , определяется максимальный размер для хранения журналов.

Для настройки параметров хранения журналов:

1. В программе управления ЦУС активируйте в меню "ЦУС" команду "Свойства".

   На экране появится диалог "Свойства ЦУС".



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

Суммарный размер пространства, отводящегося для хранения журналов, не может превышать 32 Мб. Это конструктивное ограничение введено для поддержки высокого быстродействия системы.

Примечание. 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 ЦУС.

3. Нажмите кнопку "ОК" или "Применить".

Конфигурирование базы данных журналов

Агент в соответствии с расписанием сохраняет регистрационные журналы в базе данных. Администраторы комплекса получают доступ к содержимому журналов с помощью программы просмотра журналов.

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.

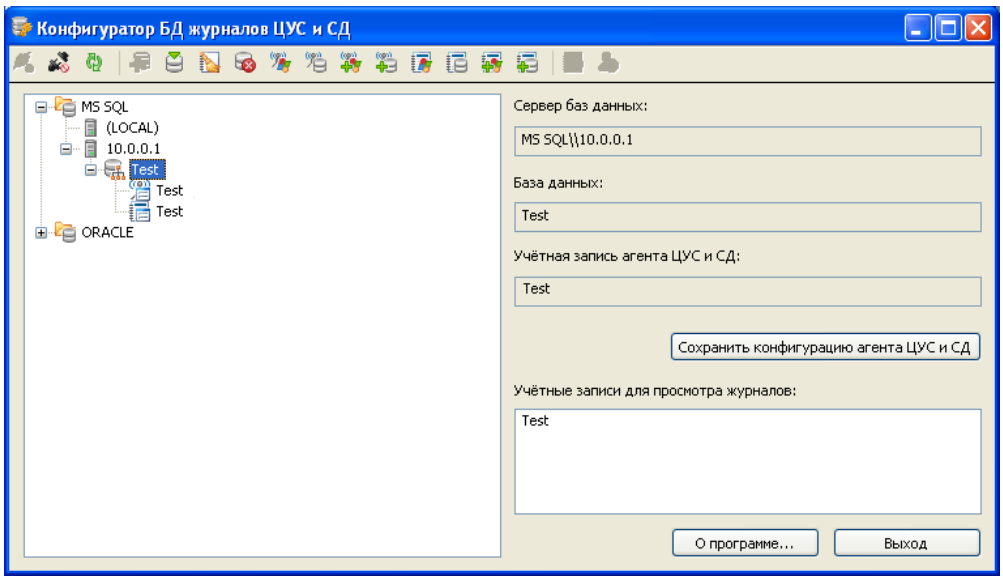
Запуск конфигуратора

Для запуска конфигуратора:

- Нажмите кнопку "Пуск" и выберите в главном меню Windows команду "Программы\ Код Безопасности\ Континент 3.7\ Конфигуратор БД журналов ЦУС и СД".

  На экране появится окно конфигуратора (см. стр.**17**).

Интерфейс конфигуратора



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

Управление объектами осуществляют с помощью команд контекстного меню и кнопок на панели инструментов (см. таблицу ниже).

Табл.11 Команды управления объектами

Кнопка	Команда	Описание
	Подключиться к серверу СУБД...	Запускает процедуру подключения конфигуратора к серверу БД с правами администратора
	Отключить соединение	Отключает соединение с выбранным сервером БД

Кнопка	Команда	Описание
	Обновить	Обновляет в иерархическом списке отображаемые сведения о выбранном объекте
	Создать базу данных...	Запускает процедуру создания базы данных
	Выбрать	Отображает в правой части окна настройки агента, необходимые для подключения к выбранной в иерархическом списке базе данных
	Очистить журналы ЦУС	Выполняет очистку выбранной базы данных
	Удалить	Удаляет выбранную базу данных
	Назначить учетную запись для агента > Пользователь Windows...	Запускает стандартную процедуру выбора зарегистрированной учетной записи Windows для доступа агента к базе данных
	Назначить учетную запись для агента > Пользователь СУБД...	Запускает процедуру выбора зарегистрированной учетной записи СУБД для доступа агента к базе данных
	Назначить учетную запись для агента > Создать нового пользователя Windows...	Запускает стандартную процедуру создания новой учетной записи Windows для доступа агента к базе данных
	Назначить учетную запись для агента > Создать нового пользователя СУБД...	Запускает процедуру создания новой учетной записи СУБД для доступа агента к базе данных
	Назначить учетную запись для ППЖ > Пользователь Windows...	Запускает стандартную процедуру выбора зарегистрированной учетной записи Windows для доступа пользователя программы просмотра журналов к базе данных
	Назначить учетную запись для ППЖ > Пользователь СУБД...	Запускает процедуру выбора зарегистрированной учетной записи СУБД для доступа пользователя программы просмотра журналов к базе данных
	Назначить учетную запись для ППЖ > Создать нового пользователя Windows...	Запускает стандартную процедуру создания новой учетной записи Windows для доступа пользователя программы просмотра журналов к базе данных
	Назначить учетную запись для ППЖ > Создать нового пользователя СУБД...	Запускает процедуру создания новой учетной записи СУБД для доступа пользователя программы просмотра журналов к базе данных
	Отменить доступ пользователя к журналам ЦУС	Отменяет доступ выбранного пользователя к базе данных без удаления учетной записи
	Удалить пользователя СУБД	Удаляет учетную запись выбранного пользователя из СУБД

Подключение конфигуратора к серверу БД

Для подключения к серверу БД:

1. Вызовите на экран окно конфигуратора (см. стр.**17**).
2. В иерархическом списке объектов выберите нужный объект (см. стр.**17**).
3. Вызовите контекстное меню элемента и активируйте команду "Подключиться к серверу СУБД...".

   На экране появится диалог "Подключение к серверу БД...".
4. Заполните поля диалога и нажмите кнопку "ОК".

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

Настройка параметров подключения агента к СУБД

Для настройки параметров подключения:

1. Вызовите на экран окно конфигуратора (см. стр.**17**).
2. В иерархическом списке объектов выберите нужный сервер БД (см. стр.**17**).
3. С помощью команд контекстного меню и кнопок панели инструментов выполните следующие действия:
   - Выберите/создайте базу данных для хранения журналов.

     Примечание. При создании новой базы данных на диске резервируется 4 ГБ дискового пространства.

   - Выберите/создайте учетную запись, под которой агент будет обращаться к базе данных.

     Внимание! Для доступа агента к базе данных под учетной записью пользователя Windows данный пользователь должен входить в группу локальных администраторов.

     Примечание. При выборе/создании новой учетной записи доступ предыдущей учетной записи к БД автоматически отменяется.

   Описание команд см. в Табл.11.
4. Активируйте в контекстном меню нужной базы данных команду "Выбрать" для отображения в правой части окна настроек агента, необходимых для подключения к этой базе данных.
5. Нажмите кнопку "Сохранить конфигурацию агента ЦУС и СД", расположенную в правой части главного окна конфигуратора.

   На экране появится запрос пароля учетной записи агента.
6. Введите пароль и нажмите кнопку "ОК".

   На экране появится сообщение о сохранении конфигурации.
7. Нажмите кнопку "ОК" для закрытия окна сообщения.

   Сведения, необходимые агенту для подключения к БД, будут внесены в реестр компьютера.

Обеспечение доступа администраторов комплекса к БД журналов

Для обеспечения доступа администраторов комплекса к БД:

1. Вызовите на экран окно конфигуратора (см. стр.**17**).
2. В иерархическом списке объектов выберите нужную базу данных (см. стр.**17**).
3. С помощью команд контекстного меню и кнопок панели инструментов сформируйте перечень учетных записей, под которыми администраторы комплекса будут обращаться к базе данных (см. Табл.11).

Настройка агента

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.

Кроме того, требуется создать единый ключевой носитель (ЕКН) для подключения агента к ЦУС и СД.

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

Управление единым ключевым носителем

Агент забирает 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 создания ключевого носителя для агента ЦУС и СД.

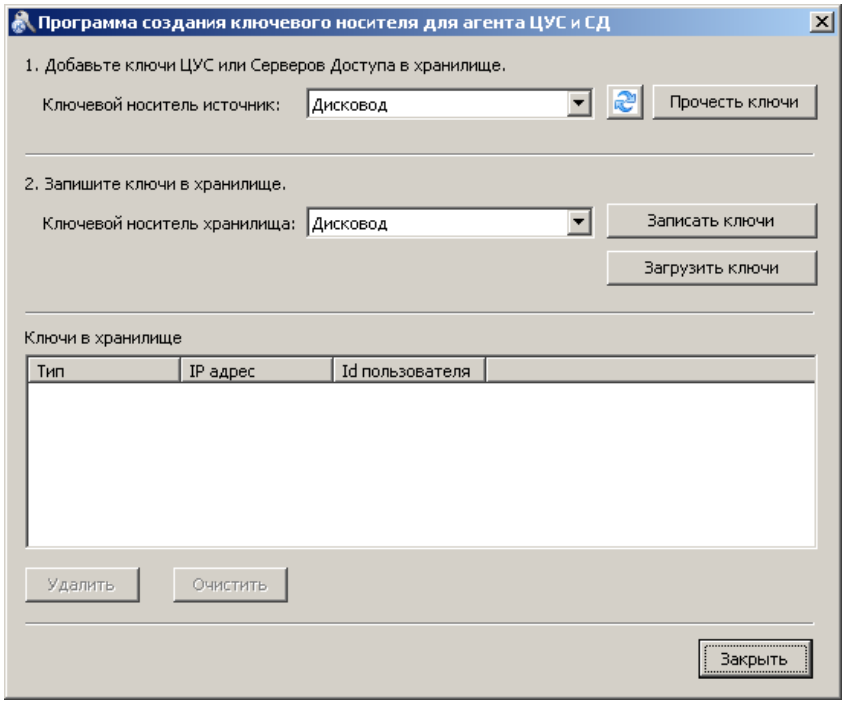
IP-адреса и ключи записываются в специальное хранилище (контейнер). На период работы программы на компьютере создается временное хранилище. Затем это хранилище записывают на носитель. При закрытии программы временное хранилище удаляется.

Запуск программы создания ключевого носителя

Для запуска программы:

1. Выполните одно из следующих действий:
   - Нажмите кнопку "Пуск" на панели задач и в главном меню Windows активируйте команду "Программы (Все программы)/ Код Безопасности/ Континент 3.7/ Программа создания ключевого носителя для агента ЦУС и СД".
   - В программе управления ЦУС активируйте в меню "ЦУС" команду "Создание ключевого носителя агента…".

   На экране появится главное окно программы.



Создание и обновление ЕКН выполняют в данном окне.

Создание единого ключевого носителя

Для создания ЕКН:

1. Вызовите на экран окно программы создания ключевого носителя (см. стр.**20**).
2. Сформируйте содержимое ЕКН. 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.
3. Сохраните сформированный перечень ключей на ЕКН. Для этого:
   - Подключите ЕКН к считывателю.
   - В поле "Ключевой носитель хранилища" укажите нужный считыватель и нажмите кнопку "Записать ключи".
   - Дождитесь сообщения о завершении создания хранилища и нажмите кнопку "ОК".

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.**20**).
2. Загрузите содержимое ЕКН во временное хранилище на компьютере. Для этого:
   - Подключите ЕКН к считывателю.

- В поле "Ключевой носитель хранилища" укажите нужный считыватель и нажмите кнопку "Загрузить ключи".

В поле "Ключи в хранилище" отобразится перечень записанных ключей.

3. При необходимости 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.
5. Сохраните обновленный перечень ключей на ЕКН. Для этого:
   - Подключите ЕКН к считывателю (если ЕКН был извлечен из считывателя).
   - В поле "Ключевой носитель хранилища" укажите нужный считыватель и нажмите кнопку "Записать ключи".
   - В появившемся запросе подтвердите перезапись имеющегося хранилища.
   - Дождитесь сообщения о завершении создания хранилища и нажмите кнопку "ОК".

Просмотр содержимого единого ключевого носителя

Для просмотра содержимого ЕКН:

1. Вставьте носитель с ЕКН.
2. Вызовите на экран окно Программы создания ключевого носителя (см. стр.**20**).
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.

Локальное управление агентом

Запуск агента

Запуск программы управления агентом осуществляется автоматически при включении и перезагрузке компьютера, на котором агент установлен. При этом, если на компьютере включен контроль учетных записей Windows, программа запускается в режиме ограниченной функциональности. В этом случае агент может быть запущен только вручную с предварительным перезапуском программы управления агентом (см. ниже).

Запуск программы управления агентом на компьютере под управлением ОС Windows Vista и выше необходимо выполнять под учетной записью, наделенной правами локального администратора.

Внимание! Запуск агента возможен только при предъявлении единого ключевого носителя (ЕКН) и пароля, заданного в настройках агента (см. стр.**24**).

Процедура запуска агента при первом включении описана в [**1**].

Для автоматического запуска агента:

- Включите питание компьютера, 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 "Программа управления агентом ЦУС и СД", отображающая состояние связи между агентом и ЦУС.

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

Если агент был остановлен, запуск агента можно осуществить вручную.

Внимание! Ручной запуск агента должен выполняться от имени локального администратора.

Для запуска агента вручную:

1. Предъявите ЕКН.
2. Вызовите контекстное меню пиктограммы "Программа управления агентом ЦУС и СД" и активируйте команду "Запустить агент".

   При успешном чтении ключевой информации агент будет запущен. Если носитель испорчен или не содержит административного ключа, см. выше примечание к автоматическому запуску агента.

Запуск агента при включенном контроле учетных записей

Для запуска агента:

1. Закройте программу управления агентом. Для этого вызовите контекстное меню пиктограммы программы управления агентом ЦУС и СД и выберите команду "Выход".

   Программа управления агентом будет закрыта и пиктограмма будет удалена.
2. Запустите программу управления от имени администратора. Для этого нажмите кнопку "Пуск", в главном меню Windows выберите команду "Все программы> Код Безопасности> Континент 3.7> Программа управления агентом ЦУС и СД", вызовите контекстное меню и выберите команду "Запустить от имени администратора".

   Программа управления агентом ЦУС и СД будет запущена и в правом углу панели задач появится пиктограмма программы управления агентом ЦУС и СД.
3. Запустите агент вручную (см. выше).

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 КШ/ДА/КК. Используемые для этой цели пиктографические изображения, а также сведения о командах контекстного меню данной пиктограммы представлены в таблицах ниже.

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.12 Пиктографические обозначения состояний агента

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

Табл.13 Команды контекстного меню программы управления агентом

Название команды	Описание
Запустить агент	Осуществляет запуск агента
Остановить агент	Осуществляет остановку агента
Параметры агента…	Открывает диалог программы управления агентом, предназначенный для просмотра и настройки параметров агента
Отключить уведомления об ошибках	Отключает/включает вывод всплывающих сообщений об ошибках в работе 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. **Внимание!** При удалении пиктограммы агент не выключается!

Настройка агента

Настройка агента предусматривает:

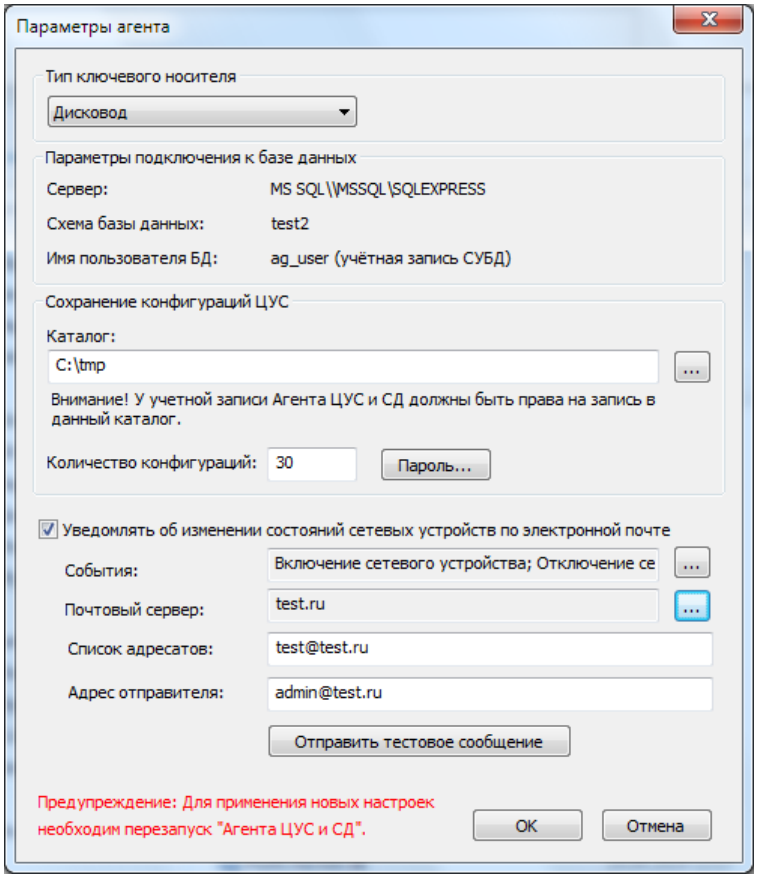
- выбор типа ЕКН;
- просмотр параметров соединения с базой данных для хранения журналов;
- выбор папки архива;
- настройку рассылки уведомлений по электронной почте.

Определение параметров работы агента выполняют в окне настройки.

Вызов окна настройки

Для вызова окна настройки агента:

1. Активируйте команду "Параметры агента…" в контекстном меню пиктограммы агента, расположенной в системной области панели задач. На экране появится диалог для настройки агента.



Просмотр параметров соединения с базой данных и настройку параметров работы агента выполняют в этом окне.

2. Для сохранения изменений нажмите кнопку "OK".
3. Для применения новых настроек остановите агент и заново вручную запустите его (см.стр.**26** и стр.**22**).

Выбор типа ЕКН

Для выбора типа ЕКН:

- В поле "Тип ключевого носителя" выберите в раскрывающемся списке нужное значение и нажмите кнопку "OK".

Выбор папки архива

В эту папку агент автоматически сохраняет зашифрованную резервную копию конфигурации ЦУС в соответствии с заданным расписанием. Имя файла резервной копии Save_at_yy_mm_dd_yy-hh_mm.dat. В папке 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. Имейте в виду, что в MS Windows имя папки Documents может отображаться как Shared documents.

Для выбора папки архива:

- В группе полей "Сохранение конфигураций ЦУС" укажите нужные значения параметров и нажмите кнопку "OK".

Каталог	Полное имя папки архива. Для выбора папки в стандартном диалоге нажмите кнопку "..."
Количество конфигураций	Максимальное количество хранимых резервных копий

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

Настройка рассылки

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 устройства кластера;
- Включение основного устройства кластера;
- Изменение состояния ключей сетевого устройства;
- Задание находится в очереди более указанного времени.

Внимание! На почтовом сервере, через который будут рассылаться уведомления, должен быть включен один из следующих типов аутентификации:

- Anonymous access;
- Basic authentication.

Для настройки рассылки:

- Установите отметку в поле "Уведомлять об изменении состояний сетевых устройств по электронной почте", укажите нужные значения параметров и нажмите кнопку "ОК".

События	Перечень событий, требующих уведомлений. Для выбора из списка нажмите кнопку "..." справа от поля. В открывшемся диалоге укажите также период проверки состояния КШ/ДА/КК
Почтовый сервер	Сетевое имя или IP-адрес почтового сервера, через который будут рассылаться уведомления. Для ввода данных нажмите кнопку "..." справа от поля. В открывшемся диалоге 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

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

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 ЦУС и СД" и активируйте команду "Остановить агент".

  Агент будет остановлен.

Для остановки агента из консоли "Службы":

1. Нажмите кнопку Пуск, активируйте в главном меню Windows команду "Настройка\ Панель управления" и откройте окно элемента "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".

Управление агентом с помощью программы управления ЦУС

Настройка параметров соединения с агентом

Для настройки параметров соединения с агентом:

1. Активируйте в меню "ЦУС" команду "Параметры соединения с агентом ЦУС и СД…". На экране появится одноименный диалог.
2. Заполните поля данного диалога и нажмите кнопку "ОК":

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 600 сек.)

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

Вызов окна настройки агента

Определение параметров работы агента выполняют в окне настройки.

Внимание! 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:

- Активируйте в программе управления ЦУС в меню "ЦУС" команду "Настройка агента…".

  На экране появится диалог "Настройка агента ЦУС и СД".

  Настройку параметров работы агента выполняют в этом окне.

Настройка расписания автоматической передачи журналов в базу данных

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

Примечание. По команде администратора (аудитора) может осуществляться внеочередная передача журналов криптографических шлюзов (см. стр. 29).

Для настройки расписания передачи журналов:

1. Вызовите на экран диалоговое окно "Настройка агента ЦУС и СД" (см. стр. 27).
2. Перейдите к вкладке "Получение журналов".
3. 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".

Настройка параметров автоматической очистки журналов в базе данных

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

Примечание. По команде администратора (аудитора) может осуществляться внеочередное удаление записей — см.стр.39.

Для настройки параметров очистки журналов:

1. Вызовите на экран диалоговое окно "Настройка агента ЦУС и СД" (см. стр.27).
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".

Настройка расписания автоматического копирования конфигурации ЦУС

Предусмотрена возможность сохранения конфигурации ЦУС в файл. Резервная копия позволяет быстро восстановить работу сети при выходе из строя штатного ЦУС. Агент сохраняет резервную копию конфигурации ЦУС в соответствии с заданным расписанием в папку, которую можно указать средствами локального управления агентом (см. стр. **25**) . По умолчанию это папка %PUBLIC% \Documents\Continent3\<имя_ базы данных>. В папке одновременно хранится указанное количество резервных копий. При сохранении очередной копии сверх указанного количества самая старая копия удаляется.

Для настройки расписания автоматического сохранения:

1. Вызовите на экран диалоговое окно "Настройка агента ЦУС и СД" (см. стр.**27**).
2. Перейдите к вкладке "Сохранение конфигурации ЦУС".
3. 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".

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

Внеочередная передача журналов в базу данных

Автоматическая передача регистрационных журналов в базу данных осуществляется агентом в соответствии с заданным расписанием (описание процедуры настройки расписания см.стр.**27**). При необходимости администратор (аудитор) может выполнить внеочередной запуск процесса передачи журналов. Запуск осуществляется в программе управления ЦУС.

Для запуска передачи журналов:

- В главном меню ПУ ЦУС активируйте команду "Объекты > Сбор журналов".

  На экране появится сообщение об отправке команды на исполнение. Через некоторое время, необходимое для передачи журналов в базу данных, полученные записи могут быть загружены в программу просмотра журналов.

Работа с программой просмотра журналов

Программа просмотра журналов комплекса устанавливается на АРМ администратора (аудитора) по умолчанию вместе с ПУ ЦУС или ПУ СД.

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 необходимо предъявить ключ и указать пароль администратора комплекса.

Запуск программы просмотра журналов

Предусмотрено несколько способов запуска программы просмотра журналов. Независимо от выбранного способа при первом запуске программы необходимо настроить параметры соединения с ЦУС. Такими параметрами являются:

- 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. Нажмите кнопку "Пуск" и выберите в главном меню Windows команду "Программы\ Код Безопасности\ Континент 3.7\ Программа просмотра журналов ЦУС и СД".

   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. [**1**].
2. В программе управления ЦУС откройте меню "Объекты" и активируйте команду "Просмотр журналов".

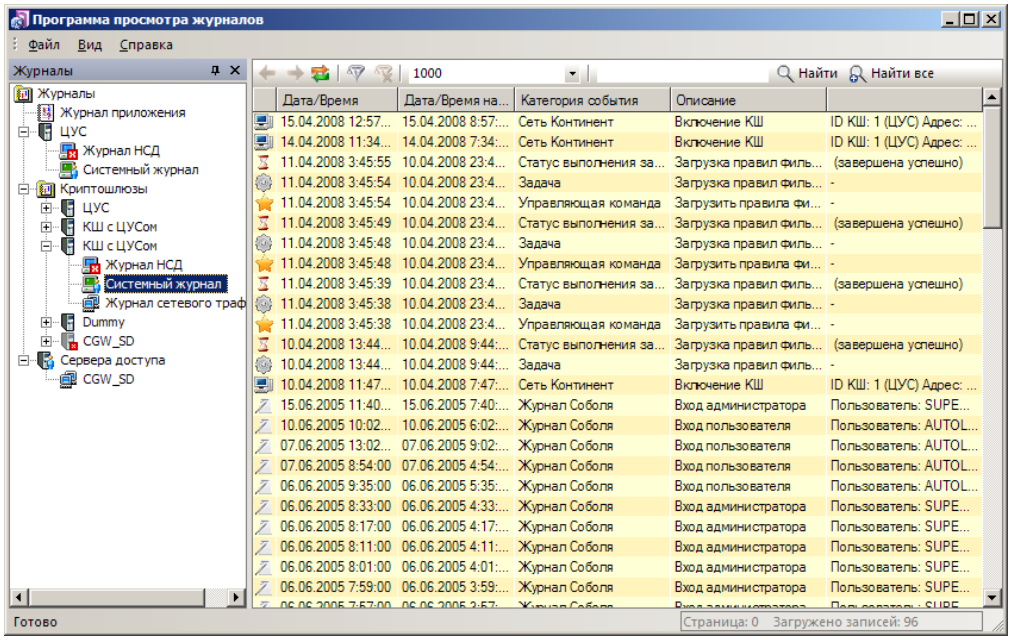
   На экране появится окно ввода пароля администратора.
3. Введите пароль администратора комплекса и нажмите кнопку "ОК".

   На экране появится окно программы просмотра журналов.

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 этих параметров. Для работы с записями журналов выполните настройку параметров (см. стр.33).

Интерфейс программы просмотра журналов

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.14 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
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 СД, 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

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 Аетевых устройств.

Для включения или отключения отображения удаленных устройств:

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

Очистка иерархического списка от удаленных сетевых устройств

Удаленные сетевые устройства 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. Вызовите контекстное меню элемента и активируйте команду "Очистка несуществующих КШ".

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

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

Отображение времени регистрации событий в часовом поясе сетевого устройства

По умолчанию таблицы с записями журналов (кроме таблицы журнала приложения) содержат колонку "Дата/Время на КШ/ДА/КК". 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 КШ" (установленная отметка рядом с командой означает, что колонка "Дата/Время на КШ/ДА/КК" 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:

- В меню "Вид" активируйте команду "Строка статуса".

Для включения или отключения окна структуры журналов:

- В меню "Вид/Панели инструментов" активируйте команду "Журналы".

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

Обновление отображаемой информации

Для обновления отображаемой информации:

- Вызовите контекстное меню корневого элемента иерархического списка и активируйте команду "Обновить" или нажмите клавишу <F5>.

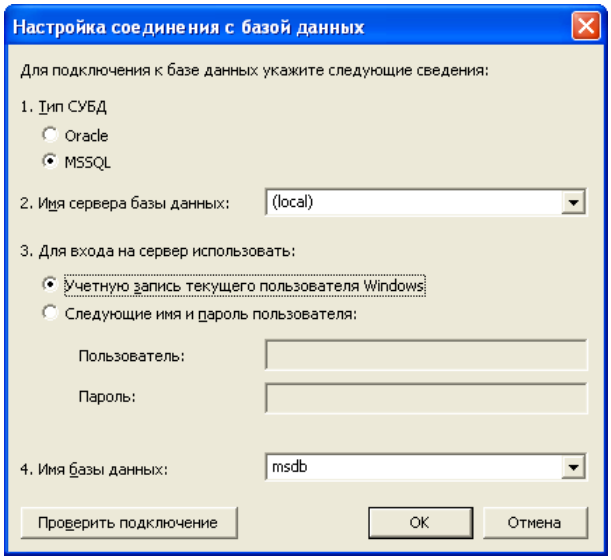
Настройка параметров соединения с базой данных

Для подключения программы просмотра журналов к базе данных необходимо настроить параметры соединения. Если при установке ППЖ эти параметры не были определены, то при первом запуске программы просмотра журналов на экране автоматически появляется диалог настройки. В дальнейшем параметры можно изменить.

Для настройки параметров соединения с базой данных:

1. В меню "Файл" активируйте команду "Параметры соединения с БД...".

   На экране появится диалог настройки параметров соединения:



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

   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 текущего пользователя Windows";
   - чтобы идентификация осуществлялась от имени пользователя СУБД, установите отметку в поле "Следующие 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.17).

5. В поле "Имя базы данных" выберите имя используемой схемы (базы данных).
6. Нажмите кнопку "OK".

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

Управление подключением программы к базе данных

При запуске программа устанавливает соединение с базой данных. В процессе работы пользователь может, не выходя из программы, разрывать соединение и

устанавливать заново.

Для отключения соединения:

- В меню "Файл" активируйте команду "Отключение" (команда доступна, если установлено соединение с базой данных).

Для подключения к базе данных:

- В меню "Файл" активируйте команду "Соединение с БД" (команда доступна, если соединение с базой данных не установлено).

Загрузка записей журналов

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

Выбор журнала

Для выбора 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:

- В поле "Количество одновременно загружаемых записей" на панели инструментов выберите в раскрывающемся списке нужное значение (по умолчанию 500).

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 "Обновление информации" ().

  Программа выполнит новую загрузку содержимого журнала.

Фильтрация записей

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

Программа позволяет выполнять фильтрацию записей следующих журналов:

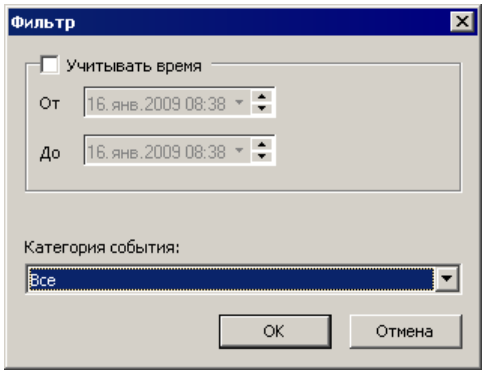
- системный журнал;
- журнал НСД;
- журнал сервера доступа;
- журнал сетевого трафика.

Фильтрация записей системного журнала

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

Для настройки параметров фильтрации:

1. Выберите нужный журнал (см.стр.**34**).
2. После загрузки записей нажмите кнопку "Включение фильтрации" ( ).
   На экране появится диалог настройки параметров фильтрации.



3. Фильтрация записей может осуществляться по времени регистрации событий, если указаны границы интервала времени. Чтобы задать границы интервала, установите отметку в поле "Учитывать время" и измените содержимое полей даты и времени. Фильтру будут удовлетворять записи, которые были зарегистрированы в указанном интервале времени.

   Примечание. Для изменения содержимого поля даты или времени введите новое значение с клавиатуры или воспользуйтесь кнопками в правой части поля. Способы редактирования значений аналогичны стандартным способам, принятым в ОС Windows.

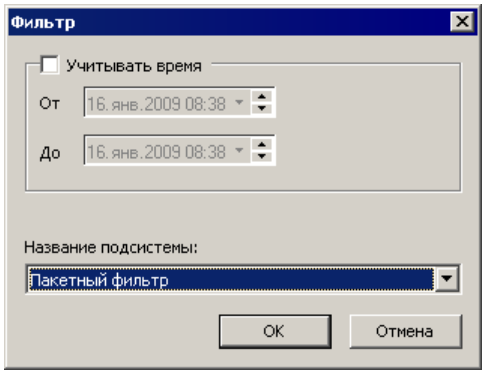
4. В раскрывающемся списке поля "Категория события" выберите название категории событий (для системного журнала). Фильтру будут удовлетворять записи о событиях, хранящие указанное название в соответствующем поле.
5. Нажмите кнопку "ОК".
   В области отображения записей останутся записи, удовлетворяющие заданным условиям отбора.

Фильтрация записей журнала НСД

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

Для настройки параметров фильтрации:

1. Выберите нужный журнал (см.стр.**34**).
2. После загрузки записей нажмите кнопку "Включение фильтрации" ( ).
   На экране появится диалог настройки параметров фильтрации.



3. Фильтрация записей может осуществляться по времени регистрации событий, если указаны границы интервала времени. Чтобы задать границы интервала, установите отметку в поле "Учитывать время" и измените содер-

жимое полей даты и времени. Фильтру будут удовлетворять записи, которые были зарегистрированы в указанном интервале времени.

Примечание. Для изменения содержимого поля даты или времени введите новое значение с клавиатуры или воспользуйтесь кнопками в правой части поля. Способы редактирования значений аналогичны стандартным способам, принятым в ОС Windows.

4. В раскрывающемся списке поля "Название подсистемы" выберите название подсистемы. Фильтру будут удовлетворять записи о событиях, хранящие указанное название в соответствующем поле.
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:

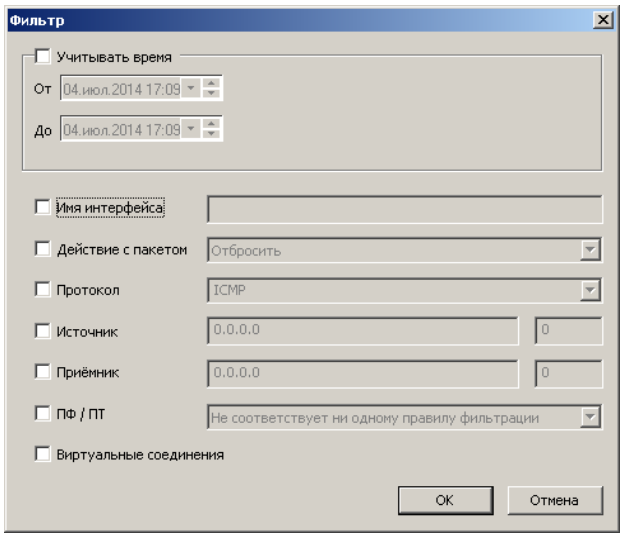
- вручную — пользователь осуществляет настройку параметров фильтрации самостоятельно;
- автоматически — параметры фильтрации задаются программой и обеспечивают вывод сведений, относящихся к выбранной записи журнала НСД. Данный способ фильтрации применяется в тех случаях, когда требуется отобразить сведения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

Для настройки параметров фильтрации вручную:

1. Выберите нужный журнал (см.стр.34).

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

   На экране появится диалог настройки параметров фильтрации:



2. Фильтрация записей осуществляется по заданным значениям параметров. Отметьте нужные 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.**11**)
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 установке виртуальных соединений

3. Нажмите кнопку "ОК".

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

Для автоматической настройки параметров фильтрации:

1. Выберите нужный журнал (см.стр.**34**).
2. Выберите нужную запись о событии.

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

3. Вызовите контекстное меню записи и активируйте команду "Просмотр данных пакета".

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

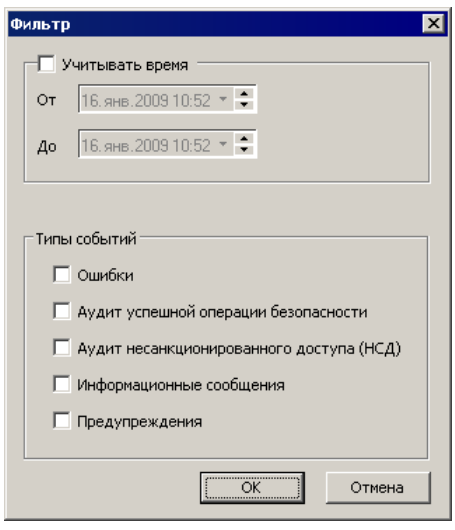
Фильтрация записей журнала сервера доступа

Настройку и применение параметров фильтрации журнала сервера доступа выполняют после выбора журнала.

Для настройки параметров фильтрации:

1. Выберите нужный журнал (см.стр.**34**).
2. После загрузки записей нажмите кнопку "Включение фильтрации" ( ).

   На экране появится диалог настройки параметров фильтрации:



3. Фильтрация записей может осуществляться по времени регистрации событий, если указаны границы интервала времени. Чтобы задать границы интервала, установите отметку в поле "Учитывать время" и измените содержимое полей даты и времени. Фильтру будут удовлетворять записи, которые были зарегистрированы в указанном интервале времени.

   Примечание. Для изменения содержимого поля даты или времени введите новое значение с клавиатуры или воспользуйтесь кнопками в правой части поля. Способы редактирования значений аналогичны стандартным способам, принятым в ОС Windows.

4. В группе полей "Типы событий" отметьте нужные типы. Фильтру будут удовлетворять записи о событиях, хранящие указанные значения в соответствующем поле.
5. Нажмите кнопку "ОК".

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

Отключение режима фильтрации журнала

При включенном режиме фильтрации записей выбранного журнала кнопка "Включение фильтрации" () 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 "Отключение фильтрации" (). 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 нужный журнал (см. стр.**34**).
2. В поле "Найти" на панели инструментов введите текст, который требуется найти.
3. Нажмите одну из следующих кнопок:
   - кнопку "Найти" — для поиска очередного вхождения указанного текста;
   - кнопку "Найти все" — 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 КШ";
   - 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.**28**).

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 КШ/ДА/КК и ЦУС:

1. Выполните одно из следующих действий:
   - Вызовите контекстное меню корневого элемента "Журналы" иерархического списка и активируйте команду "Очистка всех журналов".
   - Вызовите контекстное меню нужного устройства или ЦУС и активируйте команду "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.**38**)
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;
- детекторы 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 обмена", 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.

Передача сведений в СОПКА

Для передачи сведений в СОПКА предварительно необходимо выполнить следующее:

1. Установить и настроить защищенный канал между локальными сетями АПКШ "Континент" и СОПКА.

   Для реализации защищенного канала используют решение "абонентский пункт — сервер доступа". Установку и настройку соединения абонентского пункта с сервером доступа выполняют в соответствии с описанием, приведенным в эксплуатационной документации на абонентский пункт. Для получения значений параметров настройки необходимо обратиться в службу технической поддержки ООО "Код Безопасности".

2. Настроить параметры работы клиента (см. далее).

Настройка параметров клиента СОПКА

Для настройки параметров:

1. Раскройте в иерархическом списке объектов узел "Детекторы атак", вызовите контекстное меню любого из детекторов атак и выберите пункт "Экспорт журналов на внешний сервер (СОПКА)".

   На экране появится диалог "Клиент СОПКА".

2. Перейдите на вкладку "Настройки" и укажите нужные значения параметров.

Параметр	Описание
Адрес сервера	IP-адрес или DNS веб-сервера, расположенного в локальной сети СОПКА
Порт	Используемый порт веб-сервера

3. Если в качестве защищенного канала используется вариант TLS-клиент — TLS-сервер, установите отметку в поле "Использовать TLS-клиент" и укажите параметры:

Параметр	Описание
Адрес	IP-адрес компьютера с установленным TLS-клиентом
Порт TLS-клиента	Используемый порт TLS-клиента

4. Нажмите кнопку "Сохранить".

Примечание. Значения остальных параметров на вкладке "Настройки" заполняются автоматически.

Отправка сведений

Для отправки сведений:

1. В зависимости от используемого защищенного соединения установите соединение с сервером доступа или с TLS-сервером.

   Примечание. При первом соединении с TLS-сервером необходимо указать сертификат, предъявить ключи и ввести пароль.

2. Вызовите контекстное меню узла "Детекторы атак" и выберите пункт "Экспорт журналов на внешний сервер (СОПКА)".

   На экране появится диалог "Клиент СОПКА" с открытой вкладкой "Отчет".

   По умолчанию временной интервал, за который будут отправлены сведения, составляет неделю.

3. Выберите из раскрывающегося списка детектор атак.

   Начнется подсчет количества записей за указанный временной интервал и результат отобразится в нижней части диалога.

4. Если необходимо изменить временной интервал, введите новые значения.

   Начнется пересчет количества записей.

   Внимание! Пересчет количества записей происходит после каждого изменения значений в полях "Детектор атак" и "Временной диапазон".

5. Нажмите кнопку "Отправить".

   Начнется передача сведений веб-серверу.

   Дождитесь сообщения об успешной отправке сведений.

Работа с программой просмотра отчетов

Отчеты ЦУС

Предусмотрена возможность получения отчетов, содержащих сведения о криптографических шлюзах/детекторах атак/криптокоммутаторах комплекса. Перечень доступных отчетов зависит от роли администратора.

Табл.15 Отчеты ЦУС

Наименование отчета	Содержание	Доступ
Версии КШ/ДА/КК	Список всех устройств комплекса и их версии	Все администраторы
Состояние КШ	Для каждого КШ отображаются: • имя; • описание; • признак связи с другими сетями; • признак мягкого режима; • признак ввода в эксплуатацию; • наличие сервера доступа; • признак кластера; • наличие НСД; • время загрузки главного ключа; • время смены ключа связи с ЦУС	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; • режим работы; • признак ввода в эксплуатацию; • признак кластера; • наличие НСД; • расположение; • режим работы 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

Наименование отчета	Содержание	Доступ
Конфигурации криптокоммутаторов	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
Распределение комплектов ключей КШ	Для каждого устройства приводится список назначенных ему комплектов ключей. Для каждого ключа в комплекте приводится следующая информация: • номер комплекта; • номер ключа; • статус (загружен на устройство/не загружен); • дата создания; • дата окончания срока хранения; • серийный номер ключевого носителя (ТОКЕН_КШ), на котором хранится ключ	Все администраторы. Только для трехлетней схемы хранения ключей
Наличие связей между КШ	Перечень криптографических шлюзов, которые должны устанавливать защищенные соединения, и характеристики этих соединений	Все администраторы
Наличие связей между КК	Перечень криптокоммутаторов, 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
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

Наименование отчета	Содержание	Доступ
Правила фильтрации по прикладному протоколу	Список правил фильтрации ЦУС с регулярными выражениями. Правила приводятся в порядке обработки	Кроме администратора ключей

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

Программа поставляется как компонент "Отчеты", входящий в состав общего дистрибутива Подсистемы управления. Установка Подсистемы управления представлена в [**1**].

После установки программы просмотра отчетов в главном меню Windows добавляется команда "Все программы\ Код Безопасности\ Континент 3.7 \ Программа просмотра отчетов ЦУС", предназначенная для вызова программы.

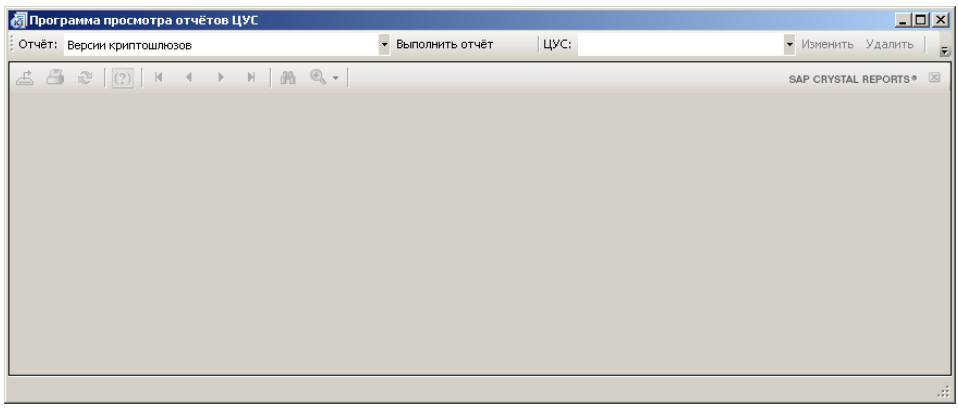
Формирование отчета осуществляется на основании запроса, отправляемого из ППО в ЦУС. Для соединения с ЦУС необходимо указать параметры соединения и предъявить ключ администратора комплекса. Перечень доступных отчетов зависит от роли администратора. Сформированный отчет отображается в формате Crystal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

Запуск программы просмотра отчетов

Для запуска программы:

- Нажмите кнопку "Пуск" и выберите в главном меню Windows команду "Все программы\ Код Безопасности\ Континент 3.7 \ Программа просмотра отчетов ЦУС".

  На экране появится главное окно программы.



Интерфейс программы просмотра отчетов

Окно программы состоит из трех панелей и области отображения отчета.

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;
- кнопка "О программе".

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

- — экспортировать отчет;
- — распечатать отчет;
- — обновить на сервере;
- — показать/скрыть панель параметров;
- — перелистывание по страницам отчета;
- — найти текст;
- — масштаб;
- — закрыть текущий вид.

На нижней панели отображается название сформированного отчета.

Примечание. Нижняя панель доступна 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 "Закрыть текущий вид".

Настройка параметров соединения с ЦУС

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

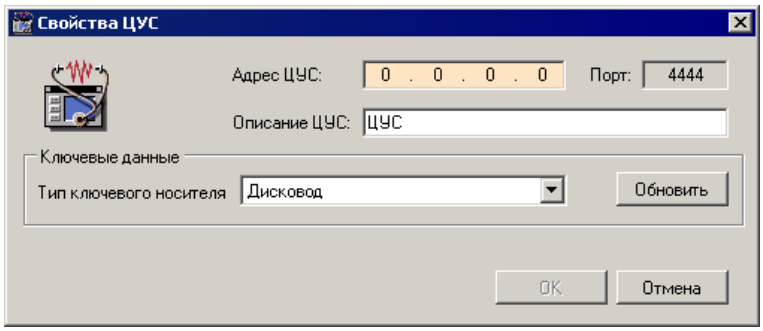
- IP-адрес ЦУС;
- тип ключевого носителя пользователя, используемого для связи с ЦУС.

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. Раскройте список выбора ЦУС и выберите в нем "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. Раскройте список выбора ЦУС, выберите соединение, у которого требуется изменить параметры, и нажмите кнопку "Изменить", расположенную справа от списка выбора.

   Появится диалог настройки соединения.
2. Введите необходимые изменения и нажмите кнопку "ОК".

Для удаления соединения из списка:

1. Раскройте список выбора ЦУС.
2. Выберите соединение и нажмите кнопку "Удалить", расположенную справа от списка выбора.

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;
- Adobe Acrobat;
- Microsoft Excel;
- Microsoft Excel Data Only;
- Microsoft Word;
- Rich Text Format.

Для вывода отчета на печать и сохранения используйте соответственно кнопки "Распечатать отчет" и "Экспортировать отчет", расположенные на средней панели окна программы.

Приложение

Перечень регистрируемых событий

Табл.16 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

Название зарегистрированного события	**Описание произошедшего события/причина**	**Действия пользователя**
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
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

Название зарегистрированного события	Описание произошедшего события/причина	Действия пользователя
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.17 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
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

Название зарегистрированного события	**Описание произошедшего события/причина**	**Действия 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 сертификаци
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

Название зарегистрированного события	Описание произошедшего события/причина	Действия пользователя
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
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.18 Перечень событий детектора атак

Событие
Обнаружена атака. Описание атаки
Изменение режима работы детектора атак
Изменение значения параметра детектора атак
Изменение правила ДА
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". Руководство администратора. Централизованное управление комплексом
2.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Локальное управление сетевыми устройствами
3.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аудит
4.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Аутентификация пользователя
5.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Сервер доступа
6.	Аппаратно-программный комплекс шифрования "Континент". Руководство пользователя. Программа мониторинга КШ
7.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Тестирование каналов связи
8.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Обновление программного обеспечения
9.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Автоматизированное рабочее место генерации ключей
10.	Аппаратно-программный комплекс шифрования "Континент". Руководство администратора. Система обнаружения вторжений

Примечание. Набор документов, входящих в комплект поставки, может отличаться от указанного списка.